ISSN 2074-7128 (print), ISSN 2074-7136 (on-line)

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
(IT Security)

Периодический рецензируемый научный журнал «Безопасность информационных технологий», освещающий широкий спектр проблем обеспечения информационной безопасности, в том числе технологические, организационно-правовые и образовательные аспекты.

Журнал зарегистрирован в Государственном комитете Российской Федерации по печати. Свидетельство № 017789.
Издается с 1994 г.

С момента основания и до настоящего времени учредителем журнала является федеральное государственное автономное образовательное учреждение высшего образования Национальный исследовательский ядерный университет «МИФИ» (НИЯУ МИФИ).

С 2007 г. и по настоящее время журнал входит в Перечень ВАК ведущих рецензируемых научных журналов и изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени доктора и кандидата наук по отраслям науки и группе специальностей научных работников 05.13.00 – информатика, вычислительная техника и управление, по которой журнал входит в этот перечень.

Основные тематические направления журнала:

- *Концептуальные основы обеспечения информационной безопасности автоматизированных систем;*
- *Методические подходы к анализу и оценке рисков информационной безопасности, технологии поиска уязвимостей в программном обеспечении;*
- *Оценка уровня защищенности автоматизированных систем;*
- *Программно-технические способы и средства обеспечения информационной безопасности.*

Журналом приветствуются статьи на русском и английском языках.

IT Security (Russia)

IT Security is a periodic peer-reviewed scientific journal publishing papers on a wide range of information security topics, including technological, organizational, legal and educational problems.

Since its establishment in 1994 (registration certificate No. 017789 by the State Committee for Press of the Russian Federation), the journal has been publishing by the Federal Autonomous Educational Institution of Higher Education National Research Nuclear University, a.k.a. "MEPhI" (Moscow Engineering Physics Institute).

Papers in Russian and English are equally welcome.

Focus topics:

- *Fundamentals of information security of automated systems;*
- *Methodology of assessing the information security risks;*
- *Technology of detecting software vulnerabilities;*
- *Evaluation of the security level of automated systems;*
- *Soft- and hardware means of ensuring information security.*

СОДЕРЖАНИЕ

CONTENT

Виктор А. Шурыгин[1], Игорь М. Ядыкин[2]
Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, Москва, 115409, Россия
[1]e-mail: vic-54@mail.ru, https://orcid.org/0000-0003-2739-9560
[2]e-mail: IMYadykin@mephi.ru, https://orcid.org/0000-0003-3952-5288

УНИВЕРСАЛЬНОЕ КОДИРОВАНИЕ ТРОЙКАМИ ДЛЯ СЖАТИЯ И ЗАЩИТЫ ДВОИЧНЫХ ДАННЫХ

DOI: http://dx.doi.org/10.26583/bit.2021.1.01

Аннотация. Статья посвящена актуальной проблеме сжатия обрабатываемых и передаваемых данных, хранения и защиты данных. Приводится анализ и особенности методов сжатия данных. Рассмотрен метод универсального кодирования тройками двоичных наборов (КТ). Метод предназначен для сжатия двоичных данных без потерь в условиях неизвестной статистики источника сообщений. Метод основан на разбиении исходной последовательности двоичных данных на блоки разрядностью *n*. Каждому блоку на основании анализа содержимого *n*–блока ставится в соответствие три параметра: количество единиц в блоке, сумма номеров позиций единиц, номер данной конкретной комбинации в соответствующем префиксном классе. Рассмотрены подходы к снижению трудоемкости процедур вычисления параметров КТ. Приводится табличный алгоритм вычисления коэффициентов и алгоритм заполнения строк таблиц с применением рекуррентного соотношения для элементов множеств, оценка объемов памяти для хранения таблиц и способы сокращения емкости памяти. Рассмотрена зависимость разрядности кодовых слов КТ от разрядности *n*-блоков. Анализируются подходы и особенности применения кодировании тройками для защиты информации.

Ключевые слова: сжатие данных, кодирование, хранение данных, защита данных, рекуррентное отношение, сжатие без потерь.

Для цитирования: ШУРЫГИН, Виктор А.; ЯДЫКИН, Игорь М. УНИВЕРСАЛЬНОЕ КОДИРОВАНИЕ ТРОЙКАМИ ДЛЯ СЖАТИЯ И ЗАЩИТЫ ДВОИЧНЫХ ДАННЫХ. Безопасность информационных технологий, [S.l.], v. 28, n. 1, p. 6–18, jan. 2021. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1315>. Дата доступа: 14 jan. 2021. DOI: http://dx.doi.org/10.26583/bit.2021.1.01

Victor A. Shurygin[1], Igor M. Yadykin[2]
National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Kashirskoe shosse, 31, Moscow, 115409, Russia
[1]e-mail: vic-54@mail.ru, https://orcid.org/ 0000-0003-2739-9560
[2]e-mail: IMYadykin@mephi.ru, https://orcid.org/0000-0003-3952-5288

Universal triple encoding for compression and protecting binary data

DOI: http://dx.doi.org/10.26583/bit.2021.1.01

Abstract. The paper is devoted to the actual problem of compression of processed and transmitted data, as well as of the data storage and protection. The analysis and features of data compression methods are presented. The method of universal coding by triples of binary sets (CT) is considered. The method is intended for lossless compression of binary data under conditions of unknown message source statistics. The method is based on dividing the original sequence of binary data into blocks of length *n*. Based on the analysis of the contents of the n–block, three parameters are assigned to each block: the number of units in the block, the sum of the unit position numbers, and the number of this particular combination in the corresponding prefix class. Approaches to reducing the complexity of procedures for calculating the parameters of CT are considered. A tabular algorithm for calculating coefficients and an algorithm for filling table rows using a recursive relation for elements of sets and an estimate of the amount of memory for storing tables as well as the ways to reduce the memory capacity are presented. The dependence of the

bit width of the QT codewords on the bit width of *n*-blocks is considered. The approaches and features of the use of coding by triplets for information protection are analyzed.
Keywords: data compression, encoding, data storage, data protection, recurrence relation, lossless compression.
For citation: SHURYGIN, Victor A.; YADYKIN, Igor M. Universal triple encoding for compression and protecting binary data. IT Security (Russia), [S.l.], v. 28, n. 1, p. 6–18, jan. 2021. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1315>. Date accessed: 14 jan. 2021. DOI: http://dx.doi.org/10.26583/bit.2021.1.01

Введение

В настоящее время наблюдается лавинообразный рост объемов передаваемых, хранимых и обрабатываемых двоичных данных. Фактически не осталось областей интеллектуальной деятельности человека, где это не ощущалось бы. Это эксперименты в ядерной физике, космических исследованиях, ИТ областях и пр. Особенно следует отметить специфику бортовых применений, где идет постоянная борьба за каждый грамм, миллиметр, литр. Для экономии объемов памяти и более эффективного использования информационных каналов используется сжатие данных. Но и здесь возникают специфические проблемы. Дополнительные трудности определяются, тем, что, как правило, статистика по данным исследуемых объектов неизвестна или известна неполностью. Понятно, что здесь невозможно «в лоб» применить принцип – более вероятному сообщению ставим в соответствие более короткое кодовое слово и за счет этого выигрываем в объеме. Особенно остро эти проблемы дают себя знать в случае необходимости использования квазиобратимого сжатия, или сжатия без потерь. В силу этого появились различные подходы к устранению статистической избыточности из потока сообщений.

1. Краткий обзор методов сжатия

В [1] авторами приведена классификация подходов к методам сжатия информации. Все методы делятся на две большие группы – сжатие допускающее потерю части информации и сжатие без потерь. Например, при передаче аудиофайлов можно «угрубить» – допустить ухудшение качества звука незаметное подавляющему большинству людей из-за их антропологических свойств и за счет этого существенно уменьшить нагрузку на каналы передачи данных и сэкономить память [2–3]. Однако методы сжатия с потерями обладают недостатками: применима не для всех случаев графической информации, например, при исследовании медицинских снимков потери могут быть недоступны глазу, но могут быть доступны для анализатора, второй недостаток – накопление погрешности при повторной компрессии и декомпрессии [4–6].

Кодирование без потерь может применяться для сжатия любой информации, поскольку обеспечивает точное восстановление данных после кодирования и декодирования.[3] Сжатие без потерь основано на простом принципе преобразования данных из одной группы символов в другую, более компактную. Когда потери недопустимы, единственно возможный подход – из последовательности символов удаляется статистическая избыточность и объем сообщения приближается к энтропии.

Если статистика известна, например, вероятность появления единиц в бинарной последовательности значительно меньше, чем нулей, то более вероятным сообщениям ставим в соответствие более короткие кодовые слова – удаляем из потока длинные последовательности одинаковых символов и т.д. Здесь можно отметить адресно-позиционное кодирование (АПК) [7], кодирование длин серий (КДС) [7–8], коды

Хаффмана [7, 9], на основе которых строятся архиваторы [2, 8, 10], исключение избыточных нулевых групп [11, 12] и т.д.

В 1967 г. Б.М. Фитингофом, на основе работ А.Н. Колмогорова, была рассмотрена возможность создания кодов устраняющих статистическую избыточность из потока символов без знания статистики источника их порождающего [13–15]. В [13] было строго математически доказана обоснованность такого подхода.

Данное направление получило название – универсальное кодирование. Суть в том, что исходная последовательность разбивается на блоки длиной n, затем применяется кодирование, и статистическая избыточность в потоке стремится к нулю при стремлении n к бесконечности. В работах [2, 6, 13] были рассмотрены различные аспекты такого подхода. Следует отметить основную трудность, препятствующую практическому применению универсального кодирования – это высокая трудоемкость.

В теории информации трудоемкость оценивалась двумя параметрами – время и объем памяти, требуемые для реализации кодирования. Б.М. Фитингоф определил рост объема памяти с ростом n, как экспоненту. В то время это было немыслимо. Появились работы направленные на уменьшение объема памяти за счет построения алгоритмов нумерации элементов кодирования, т.е. уход от табличной реализации [16]. Понятно, что это вело к резкому росту времени реализации кодирования.

В настоящее время состояние элементной базы кардинально изменилось, что делает возможным перейти к реальной реализации универсального кодирования. Одному из возможных методов кодирования и его реализации посвящена эта статья.

2. Метод кодирования тройками

В [17] описан разработанный авторами метод универсального кодирования тройками. В данном методе входные двоичные последовательности размерности N разбиваются на двоичные блоки длиной n бит (n–блоки) (где $n< N$), для каждого n–блока вычисляются три параметра. При этом если разрядность параметров меньше чем 2^n, то осуществляется сжатие данных.

На рис. 1 для n=5 приведены возможные двоичные числа разрядностью n бит, всего 2^n=32 элементов, расположенные в порядке возрастания. Для множества N введем два подмножества M_k и L_S:

– M_k элементами подмножества являются все элементы множества N, содержащие k единиц $(0 \le k \le n)$.

– L_S элементами подмножества являются все элементы множества N, сумма номеров позиций единиц которых равна S $(0 \le S \le n(n+1)/2)$.

На рис. 1 показаны подмножества M_k и L_S для n=5. Цифрами 1, …, 5 заданы номера бит (разрядов) в n–блоке.

Введем подмножество $R_{k,\,S}$, как пересечение подмножеств M_k и L_S. Обозначим $r(n,\,k,\,s)$ – количество элементов множества $R_{k,\,S}$. Поставим в соответствие каждому элементу подмножества $R_{k,\,S}$ номер $b(n,\,k,\,s)$, причем $0 \le b(n,\,k,\,s) \le r(n,\,k,\,s) - 1$.

Авторами в [18] проведено исследование эффективности универсального кодирования в зависимости от длины n–блока. Получены зависимости избыточности кодирования и коэффициента сжатия от длины n–блока.

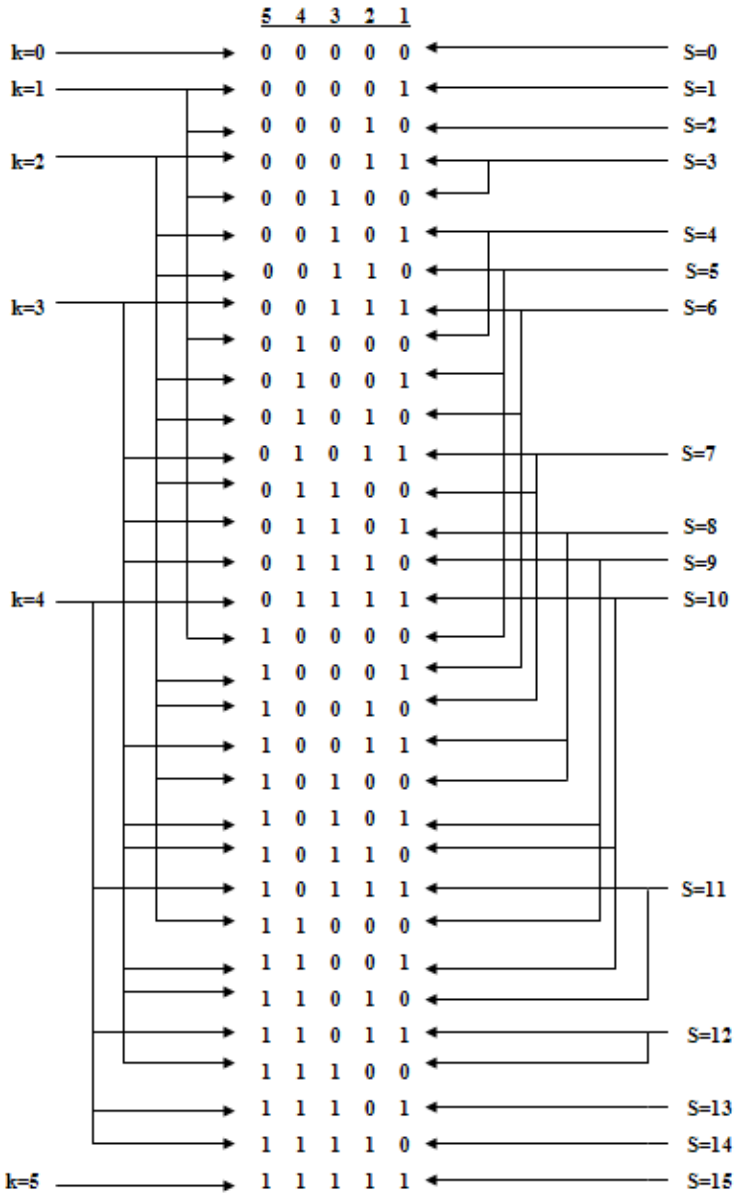


Рис. 1. Элементы множества N для n=5
(Fig. 1. Elements of the set N for n = 5)

Определим кодовое слово w соответствующее n–блоку, как упорядоченную тройку двоичных наборов $(k, s, b(n, k, s))$. Разрядность кодового слова w (в битах) будет равна:

$$Z =]log_2 (n+1)[+]log_2 (n (n+1)/2)+1[+]log_2 r(n, k, s)[, \quad (1)$$

где] [большее целое; первое слагаемое количество разрядов для задания максимального числа единиц в n–блоке; второе слагаемое – для задания максимального числа суммы всех номеров позиций в n–блоке; третье слагаемое – для задания максимального числа параметра $r(n, k, s)$ пересечения подмножеств M_k и L_s.

Введем подмножество W, элементами которого являются все кодовые слова w. Из формирования подмножества W следует, что W – префиксное множество, а, следовательно, между n-блоками и кодовыми словами w существует взаимно однозначное соответствие.

Кодирование n-блоков двоичных наборов (k, s, $b(n, k, s)$) авторами в [17] названо как **кодирование тройками (КТ).**

В литературе по комбинаторике [19–21] не было выявлено соотношений для вычисления значений коэффициентов $r(n, k, s)$. В [17] авторами были сформулированы и доказаны теоремы для вычисления коэффициентов r (n, k, s) и выведено рекуррентное соотношение:

$$r(n, k, s) = r(n–1, k, s)+ r(n–1, k–1, s–n). \quad (2)$$

Далее для определения номера $b(n, k, s)$ соответствующего каждому элементу подмножества $R_{k,S}$ был разработан алгоритм нумерации.

В n–блоке фиксируем номер k–ой единицы i_k. При этом остальные номера от 1 до (i_k–1) будут размещаться в (i_k–1) разрядной сетке и количество всех возможных комбинаций k номеров с суммой s, будет равно $r(i_k–1, k, s)$. Аналогично можно получить значения для всех номеров до i_1 включительно. В результате для каждого i_j получено соответствующее значение $r((i_j–1), j, (s – i_k – i_{k-1} –…– i_{j+1}))$. На основании исследований и доказательств получено соотношение для вычисления номера:

$$b(n, k, s)=r((i_k –1), k, (i_k + i_{k-1}+...+ i_1)) + r((i_{k-1} –1), (k\text{-}1), (i_{k-1} + i_{k-2} ...+i_1))+ ... +$$

$$+ r((i_2 – 1), 2, (i_2 + i_1)) = (\sum_{j=2}^{k} r((i_j – 1)), j, (\sum_{m=1}^{j} i_m)). \quad (3)$$

При этом любой номер b (n, k, s), вычисленный по формуле (3) удовлетворяет неравенству: $0 \le b(n, k, s) \le r(n, k, s) – 1$.

3. Табличный алгоритм вычисления коэффициентов

Трудоемкость определения коэффициентов КТ определяется вычислением $r(n, k, s)$. На рис. 2а приведена полная таблица 1 значений коэффициентов $r(n, k, s)$ для n=7. Например, коэффициенту $r(7, 2, 8)=3$ при двух единицах $k=2$ и сумме позиций единиц $s=8$ соответствует три следующих последовательности в n–блоке ($n=7$) – 0010100, 0100010, 1000001. При $k=1$ для каждого значения s (от 1 до 7) соответствует только по одной последовательности содержащей одну единицу. При $k=7$ возможна только одна последовательность в n–блоке ($n=7$) содержащая все единицы 1111111, при этом единицам соответствует сумма всех позиций в n–блоке ($n=7$) – $s=28$.

Оценим объем таблицы. Таблица (рис. 1b) содержит k строк ($0 \le k \le$ n+1) и s столбцов ($0 \le s \le$ (n*(n+1)/2 + 1)). Общее количество ячеек памяти для элементов таблицы составляет V:

$$V = (n+1) (n (n+1)/2 + 1)) = n (n+1)^2/2 + n + 1 \quad (4)$$

Их таблицы видно, что первая строка $k=1$ симметрична шестой строке $k=6$, вторая строка $k=1$ симметрична пятой строке $k=5$, третья строка $k=3$ симметрична четвертой строке $k=4$, при сдвигах в столбцах соответственно на 20, 12 и 4 позиции.

Из анализа коэффициентов $r(n, k, s)$ было выявлено, что коэффициенты обладают свойством симметрии – для любых значений n, k, s выполняются условия:

$$r(n, k, s) = r(n, (n\text{-}k), (n\text{-}(n+1))/2 – s)), \quad (5)$$

$$r(n, k, s) = r(n, k, (k\ (n+1)) – s)). \quad (6)$$

k \ S	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
0	1																												
1		1	1	1	1	1	1	1																				
2				1	1	2	2	3	3	3	2	2	1	1															
3							1	1	2	3	4	4	5	4	4	3	2	1	1										
4											1	1	2	3	4	4	5	4	4	3	2	1	1						
5																1	1	2	2	3	3	3	2	2	1	1			
6																						1	1	1	1	1	1	1	
7																													1

a)

k \ S	0	1	2	3	4	5	6	7	8	9	10	11	12
0	1												
1		1	1	1	1								
2				1	1	2	2	3	3				
3							1	1	2	3	4	4	5

b)

k \ S	1	2	3	4	5	6	7
1	1	1	1	1			
2	1	1	2	2	3	3	
3	1	1	2	3	4	4	5

c)

Рис. 2. Таблицы коэффициентов r(n, k, s) при n=7
а) полная таблица, в) симметричная таблица, с) минимальная таблица
(Fig. 2. Tables of coefficients r(n, k, s) for n = 7
a) complete table, b) symmetric table, c) minimal table)

В соответствии с соотношениями (5), (6) полная таблица (рис. 2a) может быть преобразована к виду таблицы с учетом симметрии коэффициентов (рис. 2b). При этом при обращении к таблице для определения коэффициентов *r*, для произвольных *k* и *s*, проводится сравнение с соответствующими максимальными значениями:

$$k_{макс} =]n/2[, \qquad s_{макс} =](k_{макс}\ (n+1))/2[\qquad (7)$$

Если *k* и *s* будут меньше или равны, то непосредственно обращаемся к таблице. Если больше, то преобразуем по соотношениям (5) и (6) и затем обращаемся к таблице.

Для таблицы с учетом симметрии (рис. 2b) общее количество ячеек памяти составляет:

$$V = ([n/2]+1)\ ([([n/2]\ (n+1))/2] + 1 \qquad (8)$$

Для нечетных *n* соотношение (8) преобразуется к виду:

$$V = ((n+1)\ (n^2+3))/8$$

Для четных *n* делящихся на 4 соотношение (8) преобразуется к виду:

$$V = ((n+1)\ (n^2+n+4))/8$$

Для четных *n* не делящихся на 4 соотношение (8) преобразуется к виду:

$$V = ((n+1)\ (n^2+n+2))/8$$

Из проведенных преобразований следует, что объем таблицы с учетом симметрии (рис. 2b) сокращается более чем в 4 раза по сравнению с объемом (4) для полной таблицы (рис. 2a).

В таблице с учетом симметрии (рис. 2б) можно заметить «пустые» клетки соответствующие таким значениям k и s для которых отсутствуют двоичные комбинации в n–блоках. Например, невозможно в 7 разрядах так расположить 2 единицы (k=2), чтобы сумма их позиций s была равна 2 или более 15 и т.п. Другие «пустые» клетки, например, k=2 и s=9 или k=1 и s=5 (в таблице заштрихованы) возникают за счет того, что перед обращением к таблице коэффициентов, сначала осуществляется преобразование k и s в соответствии с (5) и (6). Таким образом, к ячейкам памяти, соответствующим «пустым» клеткам, никогда не будет обращения и их можно исключить.

Для построения таблицы без «пустых» клеток определим максимальное и минимальное значения для суммы позиций s:

$$s_{\text{мин}}(\text{k}) = \text{k}\ (\text{k}+1)/2, \qquad s_{\text{макс}} = (\text{k}\ \text{n}) - (\text{k}(\text{k}+1)/2). \tag{9}$$

Перейдем от собственного значения s к его номеру:

$$s1 = s - (k\ (k+1))/2 + 1. \tag{10}$$

Минимальная таблица, после преобразования количества позиций s в номер $s1$ по соотношению (9), приведена на рис. 2c. Нулевая строка соответствующая k=0 и нулевой столбец s=0 исключены, так как данный коэффициент может быть определен на этапе предварительной оценки. Оценим количество ячеек памяти, требуемое для минимальной таблицы. Определим объем V как сумму ненулевых квадратов каждой строки:

$$V = \sum_{k=1}^{n/2} \ ](k\ n - k^2 + 1)/2[.$$

Рассмотрим случай n – четное. Выполнив несложные преобразования, с учетом арифметической прогрессии, получаем соотношение для объема:

$$V = n^3/21 + n^2/16 + n/3 + u/4,$$

где u=0, если n делится на 4, или u=1, если n не делится на 4.

Если n – нечетное, то:

$$V = n^3/24 + 11/24\ n - 1/2.$$

Таким образом, объем минимальной таблицы (рис. 2c) уменьшается в три раза по сравнению с таблицей с учетом симметрии (рис. 2b) или более чем в 12 раз сокращается полная таблица коэффициентов (рис. 2a).

Разрядность q ячеек памяти для записи коэффициентов r в соответствии с (7) определяется следующим соотношением:

$$q =]\ log_2\ (r\ (n,\ ]n/2[,\ ](\ (]n/2[)\ (n+1)\ )/2[)\ +1)[.$$

Проведенный анализ соотношения (8) и проведенные вычисления показали линейную зависимость q от n. В результате для разрядности q получено следующее соотношение:

$$q = n - (2\ log_2\ n - 2).$$

Таким образом, суммарный объем памяти в битах составит V*q.

4. Алгоритм заполнения таблиц

Алгоритм заполнения таблиц основан на последовательном применении для вычисления коэффициентов $r(n, k, s)$ рекуррентного соотношения (2) [22]. В соответствии с преобразованием сумм позиций s в номер $s1$ по соотношению (10), под таблицу отводится объем памяти $V*q$. При этом таблицу можно представить как двумерный массив, который обозначим как A.

Определим значения коэффициентов для простейших случаев. Например, для n=2 A(1,1)=1, A(1,2)=1, A(2,1)=1, остальные значения A принимают нулевые значения. На основании применения соотношения (2) легко определить значения A для n=3 и т.д. Схема перехода для расчета коэффициентов при переходе от размерности (n–1) к размерности n приведена на рис. 3. Вычисления проводятся построчно. Очередная строка из массива A заносится во временный одномерный массив Y, а на ее место заносится строка из временного одномерного массива X. Затем, в соответствии с (2) суммируем элементы $A(k,s1)+Y(s1–n)$ и заносим результат в массив X по адресу $s1$. Далее, если перебрали не все значения $s1$, то увеличиваем $s1$ на 1 и вновь суммируем, если все, то строку k заносим в массив Y, а на ее место заносим строку из массива X и т.д.

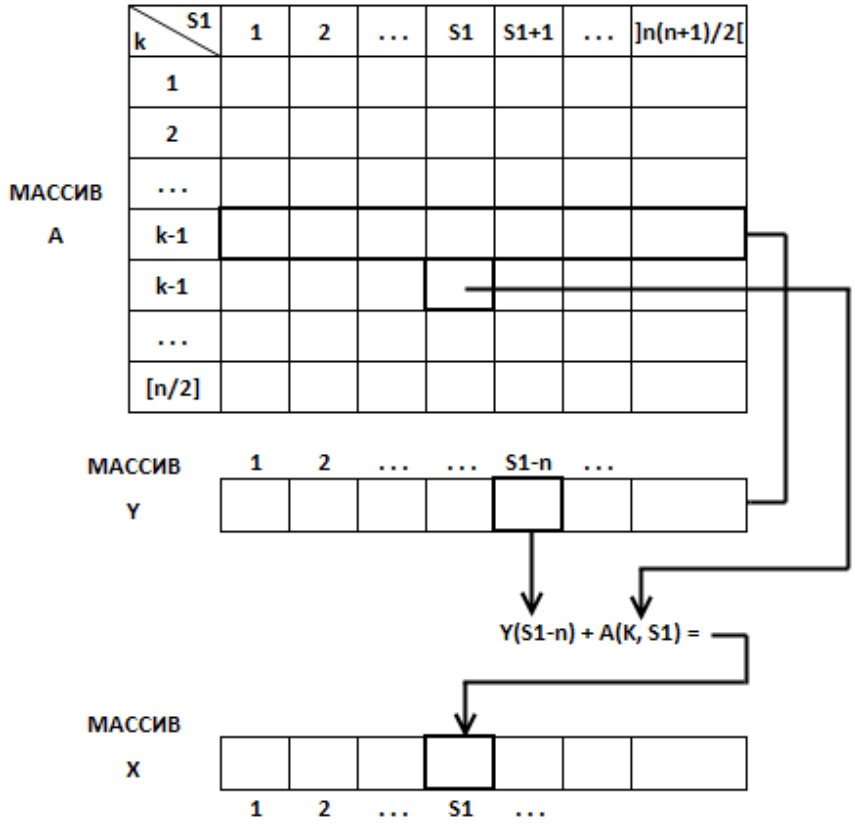


Рис. 3. Схема перехода от размерности (n-1) к размерности n
(Fig. 3. Scheme of transition from dimension (n-1) to dimension n)

На рис. 4 приведен алгоритм заполнения таблицы коэффициентов $r(n, k, s)$. Исходными параметрами являются:

N – текущее значение длины n–блока,

NK – конечное значение длины n–блока,

K1 – максимальное значение k.

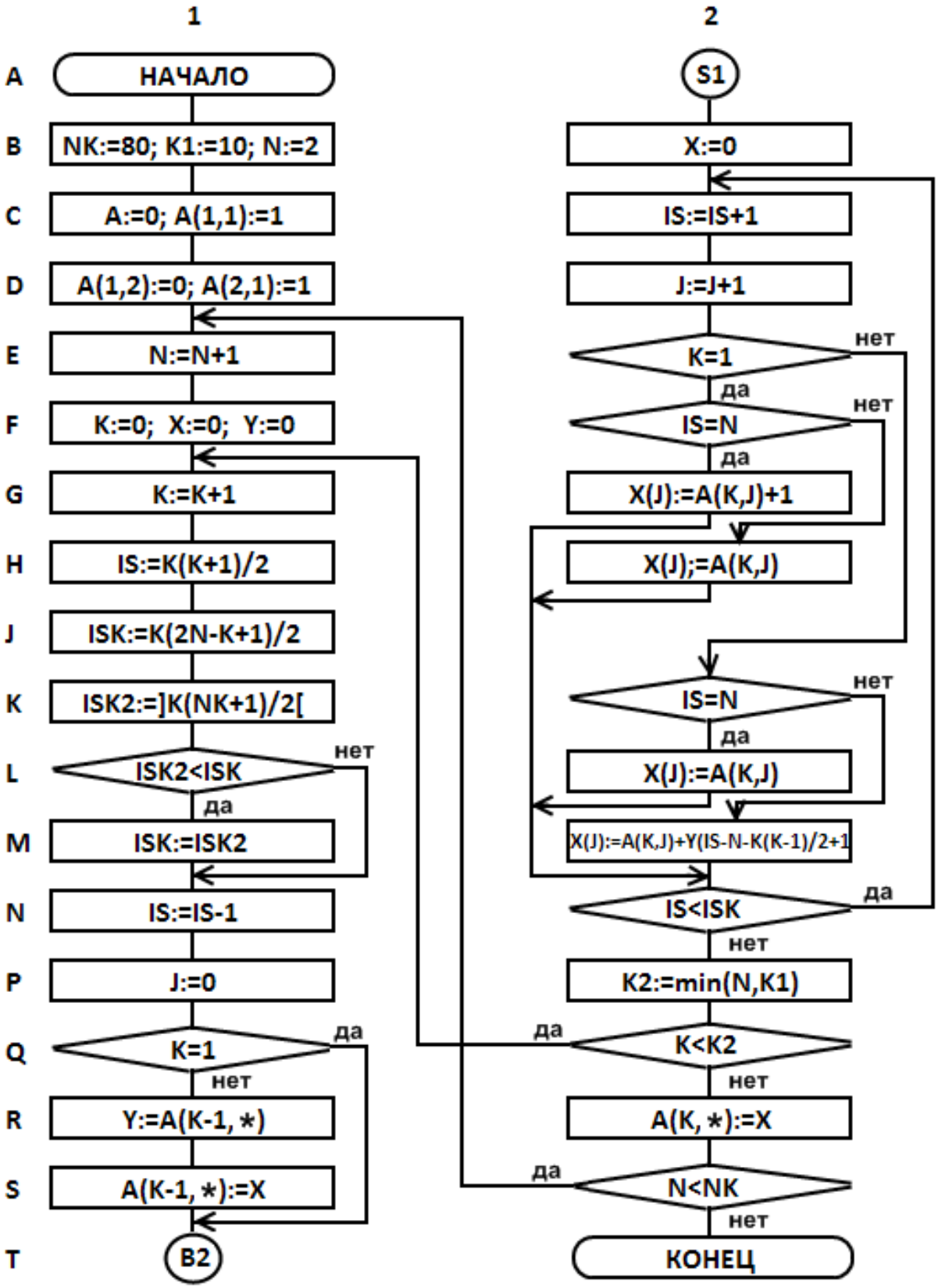


Рис. 4. Алгоритм заполнения таблицы коэффициентов r(n, k, s)
(Fig. 4. Algorithm for filling the coefficient table r(n, k, s)

В алгоритме введены следующие обозначения:
A – двумерный массив коэффициентов,
X и Y – одномерные временные массивы,
K – текущая строка массива A,
IS – текущее минимальное значение *s*,
ISK – текущее максимальное значение *s*,
J – счетная переменная,
K2 –временная переменная.

В начале работы вводятся исходные параметры и задаются начальные значения массивов A=0, X=0, Y=0, начальных коэффициентов A(1,1)=1, A(1,2)=1, A(2,1)=1, переменной K=0.

В блоках алгоритма H1, J1 определяются минимальное IS и максимальное ISK значения сумм позиций *s*. В блоках E2, F2, …, M2 записаны логические условия, при которых второе слагаемое в соотношении (2) принимает значение равное нулю, единице или берется из массива Y.

После завершения работы алгоритма в массиве A будут записаны значения коэффициентов $r(n, k, s)$ соответствующих длине *n*–блока равной NK.

5. Применение кодирования тройками для защиты информации

Универсальное кодирование тройками двоичных наборов (КТ) одновременно с сжатием данных можно использовать для защиты информации.

Алгоритм кодирования опубликован и общеизвестен. Но для того, чтобы правильно декодировать последовательность кодовых слов, ***необходимо знать следующее*** (по сути, совокупность этих сведений является ключом):

1. **Длину исходного блока *n***, т.е. количество двоичных символов в блоках, на которые разбивается исходная двоичная последовательность.

Это основной параметр, без знания которого провести декодирование невозможно. Знание *n* является необходимым, но недостаточным условием для правильной расшифровки, поскольку необходимо знать и другие параметры рассмотренные ниже.

2. **Обычное кодирование или модифицированное.**

В случае обычного кодирования количество разрядов, отводимое в кодовом слове на сумму позиций единиц, постоянно и рассчитано на максимальное возможное значение суммы для данной длины исходного блока – второе слагаемое в формуле (1). При модифицированном кодировании количество разрядов, отводимое на сумму позиций единиц в исходном блоке, становится переменным и зависит от количества единиц в блоке. В этом случае разрядность кодового слова *w* (в битах) будет равна:

$$Z =]log_2 (n+1)[\; + \;]log_2 (k\,(n-k)+1[\; + \;]log_2 r(n, k, s)[.$$

С точки зрения эффективности сжатия данных модифицированное кодирование всегда предпочтительней, но для защиты информации вполне можно использовать и обычное. Без знания, какое кодирование использовано, расшифровка невозможна, даже если известна исходная длина блока.

3. **Применение процедуры адаптации.**

В случае использования адаптации, кодирование применяется для значений *k* меньших или равных k_{max}, а для больших k_{max} *n*–блок передается без кодирования, с соответствующим «флагом» в формате кодового слова *w*. Возможен, также вариант адаптации, когда кодирование применяется и для *k* больших или равных $(n–k_{max})$ с учетом

свойств симметрии кодирования, формулы (5), (6), т.е. сжатие для k такое же, как для (n–k).

4. **Применение инверсии.**

Как отмечено выше кодирование обладает свойством симметрии. Поэтому можно кодировать не двоичный n–блок, а его инверсию. При этом вводится соответствующий «флаг» в формате кодового слова w.

5. **Место расположения «флагов» в кодовом слове.**

Для усложнения кодирования можно размещать «флаги» инверсии и адаптации не в начале кодового слова, а в произвольных разрядах. При этом позиции «флагов» должны быть в пределах минимально возможной длины кодового слова w. Также возможны варианты, когда адаптация и инверсия не применяется или применяется что-то одно.

Следует отметить, что полный перебор в данном случае не поможет, как из-за огромного количества различных вариантов возможных соотношений перечисленных пяти типов параметров ключа, так и из-за того, что просто не с чем сравнивать.

Таким образом, можно утверждать, что кодирование тройками (КТ) не только устраняет статистическую избыточность, но защитит информацию.

Заключение

В ходе данного исследования проведен анализ и ключевые особенности методов сжатия. Описан метод универсального кодирования тройками двоичных наборов для сжатия без потерь в условиях неизвестной статистики источника сообщений. Для формирования коэффициентов кодирования применяется детектирование позиций единиц в n–блоках входной бинарной последовательности. Проведена оценка разрядности кодовых слов при адаптации кодирования к количеству единиц в n–блоках.

Получены соотношения для вычисления коэффициентов кодового слова. Разработан табличный подход для хранения коэффициентов, приводятся варианты формирования таблиц, проведена оценка требуемых объемов памяти для хранения таблиц и показаны подходы для сокращения емкости памяти в 12 раз без потери точности коэффициентов. Разработана методика обработки рекуррентных соотношений для вычисления коэффициентов, обладающая неэкспотенциальной трудоемкостью. Предложен и апробирован алгоритм для заполнения таблиц коэффициентов кодовых слов n–блоков.

Разработаны подходы для защиты данных одновременно с их сжатием без потерь. Для защиты информации предложено пять типов параметров ключей, совокупность которых обладает множеством вариантов при их применении.

СПИСОК ЛИТЕРАТУРЫ:

1. Vavrenyuk A.B., Klarin A.P., Makarov V.V., Shurygin V.A. Data compression methods. Journal of Theoretical and Applied Information Technology. 2015. V. 80 (No 2). P. 423–438. ISSN 1992-8645. E- ISSN 1817-3195. URL: http://www.jatit.org/volumes/Vol80No2/2Vol80No2.pdf. (дата обращения: 05.12.2020).
2. Wayner P. Compression algorithms for real programmers. // Morgan Kaufman, 1999. – 252 p. ISBN: 9780127887746.
3. Уэлстид С. Фракталы и вейвлеты для сжатия изображений в действии. / Пер. с англ. М. Триумф, 2003. – 319 с. ISBN 5-89392-079-1.
4. Д. Сэломон. Сжатие данных, изображения и звука. М.: Техносфера, 2006. – 368 с. ISBN 5-94836-027-X, 0-387-95260-8.
5. Ковалгин Ю.А., Вологдин Э.И. Цифровое кодирование звуковых сигналов //М.: Корона-Принт, 2004. – 240 с. ISBN: 978-5-7931-0290–2.
6. Salomon D. Data compression: The complete reference. // Springer, 2006. – 1118 p. ISBN: 1-84628-602-6 (978-1-84628-602-5).

7. Соловьев В.Ф. Рациональное кодирование при передаче сообщений. М.: Энергия, Серия: Библиотека по автоматике, вып. 411, 1970. – 64 с.
8. William A. Pearlman, Amir Said. Digital signal compression: Principles and practice // Cambridge University Press, 2011. – 420 p. ISBN: 10-0521805031, 0521899826. URL: https://books.google.ru/books?id=s3H8s8rdsHkC&printsec=frontcover&dq=inauthor:%22William+A.+Pearlman%22&hl=ru&sa=X&ved=2ahUKEwitn7HD3_DtAhUI-yoKHXmfAtoQ6AEwAnoECAEQAg#v=onepage&q&f=false (дата обращения: 05.12.2020).
9. Khalid Sayood. Introduction to data compression (4th Edition)// Printbook, 2012. – 768 p. ISBN: 1849690308.
10. Ватолин Д., Ратушняк А., Смирнов М., Юкин В. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео. М.: Диалог-МИФИ, 2002. – 384 с. ISBN 5-86404-170-X.
11. Новиков Г.Г., Шурыгин В.А., Ядыкин И.М. Устройство для упаковки данных. Патент RU 2701711 C1. Заявка RU 2019100240, 09.01.2019. Опубликовано 30.09.2019. Бюл. №28. МПК H03M 7/30.
12. Новиков Г.Г., Ядыкин И.М. Устройство для распаковки данных. Патент RU 2729509 C1. Заявка RU 2019143298, 23.12.2019. Опубликовано 07.08.2020. Бюл. №28. МПК H03M 7/30.
13. Фитингоф Б.М. Сжатие дискретной информации. Проблемы передачи информации. Т 3. Вып. 3. 1967. С. 28–36. URL: http://www.mathnet.ru/php/archive.phtml?jrnid=ppi&option_lang=rus&paperid=1909&wshow=paper (дата обращения: 05.12.2020).
14. Колмогоров А.Н. Три подхода к определению понятия «количество информации». Проблемы передачи информации. Т 1. Вып. 1. 1965. С. 3–11. URL: http://www.mathnet.ru/php/archive.phtml?jrnid=ppi&option_lang=rus&paperid=68&wshow=paper (дата обращения: 05.12.2020).
15. Успенский В.А., Вьюгин В.В. Становление алгоритмической теории информации в России. Информационные процессы. Т. 10, № 2, 2010. С. 145–158. URL: http:// www.jip/ru/2010/145-158-2010/pdf (дата обращения: 05.12.2020).
16. Штарьков Ю.М. Универсальное кодирование. Теория и алгоритмы. М.: Физматлит, 2013 – 280 с. ISBN: 9785922115179.
17. Александрович А.Е., Шурыгин В.А., Ядыкин И.М. Метод универсального кодирования двоичных данных. Вопросы радиоэлектроники, серия Электронная вычислительная техника, вып. 2, М.: 2011, С. 94–115.
18. Кларин А.П., Шурыгин В.А. Исследование эффективности универсального кодирования в зависимости от длины блока. / Проблемы передачи информации, 1984. № 2. С. 105–110. URL: http://www.mathnet.ru/php/archive.phtml?jrnid=ppi&option_lang=rus&paperid=1136&wshow=paper (дата обращения: 05.12.2020).
19. Виленкин Н.Я., Виленкин А.Н., Виленкин П.А. Комбинаторика. – М.: ФИМА, МЦНМО, 2006. – 400 с. ISBN 5-89492-014-0 («ФИМА»), ISBN5-94057-230-8 (МЦНМО). URL: https://fileskachat.com/download/31544_4f4851eee87775966184b8ca8056bd02.html (дата обращения: 10.12.2020).
20. Справочник по специальным функциям. Под ред. Абрамовица М. и Стиган И. //Пер. с англ. М.: Наука, 1979. – 835 с.
21. Андерсон, Джеймс А. Дискретная математика и комбинаторика. //Пер. с англ. М.: Диалектика / Вильямс, 2020. – 960 с. URL: https://fb2lib.ru/nauchnaya/diskretnaya-matematika-i-kombinatorika/ (дата обращения: 10.12.2020).
22. Швец А.Н. Perl. Примеры программ. URL: http://mech.math.msu.su/~shvetz/54/inf/perl-problems/index.xhtml (дата обращения: 10.12.2020).

REFERENCES:

[1] Vavrenyuk A.B., Klarin A.P., Makarov V.V., Shurygin V.A. Data compression methods. Journal of Theoretical and Applied Information Technology. 2015. V. 80 (no 2). P. 423–438. ISSN 1992-8645. E- ISSN 1817-3195. URL:http://www.jatit.org/volumes/Vol80No2/2Vol80No2.pdf (accessed: 05.12.2020).
[2] Wayner P. Compression algorithms for real programmers. Morgan Kaufman, 1999. – 252 p. ISBN: 9780127887746.
[3] Welstead S. Fractals and wavelets for image compression in action. M.: Triumph, 2003. – 319 p. ISBN 5-89392-079-1 (in Russian).
[4] Salomon D. Compression of data, image and sound. M.: Technosfera, 2006. – 368 p. ISBN 5-94836-027-X, 0-387-95260-8 (in Russian).
[5] Kovalgin Yu.A., Vologdin E.I. Digital coding of audio signal. M.: Korona-Print, 2004. – 240 p. ISBN: 978-5-7931-0290-2 (in Russian).

[6] Salomon D. Data compression: The complete reference. Springer, 2006. – 1118 p. ISBN: 1-84628-602-6 (978-1-84628-602-5.
[7] Solovyev V.F. Efficient coding at transmission of messages. M.: Energy. Series: Library for Automation, issue 411, 1970. – 64 p. (in Russian).
[8] William A. Pearlman, Amir Said. Digital signal compression: Principles and practice. Cambridge University Press, 2011. – 420 p. ISBN: 10- 0521805031, 0521899826. URL:https://books.google.ru/books?id=s3H8s8rdsHkC&printsec=frontcover&dq=inauthor:%22William+A.+Pearlman%22&hl=ru&sa=X&ved=2ahUKEwitn7HD3_DtAhUI-yoKHXmfAtoQ6AEwAnoECAEQAg#v=onepage&q&f=false (accessed: 10.12.2020).
[9] Khalid Sayood. Introduction to data compression (4th Edition). Printbook, 2012. – 768 p. ISBN: 1849690308.
[10] Vatolin D., Ratushniak A., Smirnov M., Yukin V. Data compression methods. Design of archivers, compression of images and video. M.: Dialog-MEPhI, 2002. – 384 p. ISBN 5-86404-170-X (in Russian).
[11] Novikov G.G., Shurygin V.A., Yadykin I.M. Device for packing data. Patent RU 2701711 C1. Application RU 2019100240, 09.01.2019. Published 30.09.2019, bull. no. 28. IPC H03M 7/30 (in Russian).
[12] Novikov G.G., Yadykin I.M. Device for unpacking data. Patent RU 2729509 C1. Application RU 2019143298 23.12.2019. Published 07.08.2020, bull. no. 22. IPC H03M 7/30 (in Russian).
[13] Fitingof B.M. Compression of discrete information. Problemy Peredachi Informatsii. V. 3. no. 3. 1967. P. 28–36. URL: http://www.mathnet.ru/php/archive.phtml?jrnid=ppi&option_lang=rus&paperid=1909&wshow=paper. (accessed: 05.12.2020) (in Russian).
[14] Kolmogorov A.N. Three approaches to the definition of «Information amount». Problems of information transmission. Vol. 1, no 1. 1965. P. 3–11. URL: http://www.mathnet.ru/php/archive.phtml?jrnid=ppi&option_lang=rus&paperid=68&wshow=paper (accessed: 05.12.2020) (in Russian).
[15] Uspensky V.A., Vyugin V.V. Formation of algorithmic information theory in Russia. Information processes. V. 10, no. 2, 2010. P. 145–158. URL: http:// www.jip/ru/2010/145-158-2010/pdf (дата обращения: 5.12.2020) (accessed: 10.12.2020) (in Russian).
[16] Shtarkov Yu.M. Universal coding. Theory and algorithms. M.: Fizmatlit, 2013. – 280 p. ISBN: 9785922115179 (in Russian).
[17] Aleksandrovich A.E., Shurygin V.A., Yadykin I.M. A method of universal data coding. Questions of radio electronics, a series of Electronic computers. V. 2, 2011. P. 94–115. (in Russian).
[18] Klarin A.P., Shurygin V.A. Analysis of Efficiency of Universal Coding as a Function of the Block Length. Problemy Peredachi Informatsii. V. 20, no. 2. 1984. P. 105–110. URL: http://www.mathnet.ru/php/archive.phtml?jrnid=ppi&option_lang=rus&paperid=1136&wshow=paper (accessed: 05.12.2020) (in Russian).
[19] Vilenkin N.Ya., Vilenkin A.N., Vilenkin P.A. Combinatorics. M.: FIMA, MTsNMO, 2006. ISBN 5-89492-014-0 («FIMA»), ISBN5-94057-230-8 (MTsNMO). URL: https://fileskachat.com/download/31544_4f4851eee87775966184b8ca8056bd02.html (accessed: 10.12.2020) (in Russian).
[20] Abramowitz M., Stegun I.A. Handbook of Mathematical Functions. M.: Nauka, 1979. – 835 p. (in Russian).
[21] Anderson James A. Discrete mathematics and combinatorics. M.: Vil'jams, 2006. – P. 960. URL: https://fb2lib.ru/nauchnaya/diskretnaya-matematika-i-kombinatorika/ (accessed: 10.12.2020) (in Russian).
[22] Shvets A.N. Perl. Sample programs. URL: http://mech.math.msu.su/~shvetz/54/inf/perl-problems/index.xhtml (accessed: 10.12.2020) (in Russian).

Поступила в редакцию – 16 ноября 2020 г. Окончательный вариант – 14 января 2021 г.
Received – November 16, 2020. The final version – January 14, 2021.

Владимир Л. Евсеев[1], Виталий Г. Иваненко[2]
[1]Финансовый университет при Правительстве Российской Федерации (Финансовый университет), Ленинградский пр–т, 49, Москва, 125993, Россия
[2]Национальный исследовательский ядерный университет «МИФИ», Каширское ш., 31, Москва, 115409, Россия
[1]e-mail: VLEvseev@fa.ru, https://orcid.org/0000-0003-3283-3106
[2]e-mail: VGIvanenko@mephi.ru, https://orcid.org/0000-0003-0823-5501

АНАЛИЗ СТРУКТУРЫ ПОСТРОЕНИЯ И ОСНОВНЫХ ТАКТИКО-ТЕХНИЧЕСКИХ ХАРАКТЕРИСТИК АВТОМАТИЗИРОВАННЫХ СИСТЕМ ОХРАНЫ СТАЦИОНАРНЫХ УДАЛЕННЫХ ОБЪЕКТОВ ПОВЫШЕННОЙ ЗАЩИЩЕННОСТИ

DOI: http://dx.doi.org/10.26583/bit.2021.1.02

Аннотация. Для формализации математической постановки задачи исследования по обоснованию программ модернизации автоматизированных систем охраны был проанализирован их состав, структура построения и основные тактико-технические характеристики. Современные системы охраны стационарных удаленных объектов повышенной защищенности представляют собой сложные автоматизированные системы, включающие в свой состав несколько функционально завершенных и объединенных в единый комплекс подсистем и дежурные силы охраны. Анализ структурной схемы типовых автоматизированных систем охраны стационарных удаленных объектов повышенной защищенности показал, что в общем случае применительно к рассматриваемой задаче существующих систем охраны целесообразно использовать декомпозицию на подсистемы, как способ метода системного анализа. С помощью подсистем автоматизированных систем охраны формируются периметровая и локальные зоны охраны. Каждая из подсистем и входящие в нее составные части в процессе функционирования выполняют одну или несколько функций, возлагаемых на систему охраны в целом. Результаты анализа показывают, что существующие автоматизированные системы охраны не в полной мере соответствуют требованиям руководящих документов, указывая, таким образом, на возможные направления их модернизации, включая применение технических средств обнаружения, работающих на различных физических принципах действия, телевизионных средств наблюдения и средств проноса (провоза) запрещенных материалов. Причем, принципиально возможна частичная модернизация в виде замены одного из двух технических средств обнаружения на более совершенные. Результаты исследования показали, что основными характеристиками автоматизированных систем охраны, определяющими их качество, являются интегральные показатели: эффективности; надежности; устойчивости функционирования; стоимости создания и эксплуатации автоматизированных систем охраны. Объединение нескольких интегральных показателей в один комплексный показатель было осуществлено с помощью процедур их специальной логико-весовой обработки, предусматриваемых в методе расстановки приоритетов. С учетом проведенного анализа состава, структуры построения и основных тактико-технических характеристик автоматизированных систем охраны, в дальнейшем может быть сформулирована математическая постановка задачи исследования.

Ключевые слова: автоматизированная система охраны, структурная схема, объекты повышенной защищенности, декомпозиция на подсистемы, периметровая и локальные зоны охраны, показатель эффективности, показатель надежность, показатель устойчивости функционирования, показатель стоимости жизненного цикла.

Для цитирования: ЕВСЕЕВ, Владимир Л.; ИВАНЕНКО, Виталий Г. АНАЛИЗ СТРУКТУРЫ ПОСТРОЕНИЯ И ОСНОВНЫХ ТАКТИКО-ТЕХНИЧЕСКИХ ХАРАКТЕРИСТИК АВТОМАТИЗИРОВАННЫХ СИСТЕМ ОХРАНЫ СТАЦИОНАРНЫХ УДАЛЕННЫХ ОБЪЕКТОВ ПОВЫШЕННОЙ ЗАЩИЩЕННОСТИ. Безопасность информационных технологий, [S.l.], v. 28, n. 1, p. 19–28, jan. 2021. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1316>. Дата доступа: 14 jan. 2021. DOI: http://dx.doi.org/10.26583/bit.2021.1.02

Vladimir L. Evseev[1], Vitaliy G. Ivanenko[2]
[1]Financial University under the Government of the Russian Federation (Financial University), Leningradskiy Prospekt, 49, Moscow, 125993, Russia
[2]National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Kashirskoe shosse, 31, Moscow, 115409, Russia
[1]e-mail: VLEvseev@fa.ru, https://orcid.org/0000–0003-3283-3106
[2]e-mail: VGIvanenko@mephi.ru, https://orcid.org/0000-0003-0823-5501

Analysis of the structure of construction and the main tactical and technical characteristics of automated security systems for stationary remote objects of increased security

DOI: http://dx.doi.org/10.26583/bit.2021.1.02

Abstract. In order to formalize the mathematical formulation of the research problem on the justification of programs for the modernization of automated security systems, their composition, structure, and main tactical and technical characteristics were analyzed. Modern security systems for stationary remote objects of increased security are complex automated systems that include several subsystems functionally completed and integrated into a single complex and security forces on duty. Analysis of the structural diagram of typical automated security systems for stationary remote objects of increased security showed that in the general case applied to the considered task of existing security systems, it is advisable to use a decomposition into subsystems as a method of the system analysis. By using the subsystems of automated security systems, perimeter and local security zones are formed. Each of the subsystems and its constituent parts in the process of functioning perform one or more functions assigned to the security system as a whole. The results of the analysis show that the existing automated security systems do not fully comply with the requirements of the guidance documents, thus indicating possible directions for their modernization, including the use of technical detection equipment operating on different physical principles of operation, television surveillance equipment and means of transport (transportation) prohibited materials. Moreover, partial modernization is possible in the form of replacing one of the two technical means of detection with more advanced ones. The results of the study showed that the main characteristics of automated security systems that determine their quality are integral indicators: efficiency; reliability; stability of functioning; the cost of creating and operating automated security systems. The combination of several integral indicators into one complex indicator was carried out using the procedures for their special logical-weight processing foreseen by the prioritization method. Taking into account the analysis of the composition, structure of construction and the main tactical and technical characteristics of automated security systems, a mathematical formulation of the research problem can be formulated in further studies.

Keywords: automated security system, structural diagram, objects of increased security, decomposition into subsystems, perimeter and local protection zones, efficiency indicator, reliability indicator, operational stability indicator, life cycle cost indicator.
For citation: EVSEEV, Vladimir L.; IVANENKO, Vitaliy G. Analysis of the structure of construction and the main tactical and technical characteristics of automated security systems for stationary remote objects of increased security. IT Security (Russia), [S.l.], v. 28, n. 1, p. 19–28, jan. 2021. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1316>. Date accessed: 14 jan. 2021. DOI: http://dx.doi.org/10.26583/bit.2021.1.02.

Введение

Современный терроризм – серьезный вызов национальной безопасности России [1]. Как угроза национальной безопасности терроризм охватывает своим деструктивным воздействием все основные сферы общественной жизни страны. Непосредственные насильственные посягательства на жизнь, здоровье и имущество граждан, а также на материальные объекты различного назначения не только влекут за собой тяжкий ущерб для безопасности населения и экономики страны, но и одновременно подрывают устойчивость политической системы общества, стабильность государства, веру граждан в

свое государство, способствуют подрыву авторитета власти среди населения. Организаторы террористических акций стремятся посеять страх среди населения, нанести экономический ущерб государству. При определенных условиях акции террористов могут привести к возникновению крупномасштабных экологических, либо экономических катастроф и массовой гибели людей. Не случайно, что в последнее время значительно возросло число угроз взрывов объектов атомной энергетики, транспорта, экологически опасных производств.

Требования ФЗ-187 «О безопасности критической информационной инфраструктуры Российской Федерации», обязывают организации обеспечить комплексную защиту критической информационной инфраструктуры (КИИ). Учитывая важность исполнения этого закона и активную позицию регулятора, предусмотрено проведение плановых проверок ФСТЭК России после трех лет со дня предоставления сведений об объекте КИИ и внеплановых проверок в случае возникновения инцидента информационной безопасности. Кроме того, вводится уголовная ответственность за нарушение правил эксплуатации значимых объектов КИИ [2].

Одним из направлений защиты объектов информатизации от несанкционированного доступа к ним и, в частности, к информации, является обеспечение их физической защиты. Автоматизированные системы охраны (АСО) создаются с целью предотвращения несанкционированного проникновения на территорию и в помещения объекта информатизации посторонних лиц, обслуживающего персонала и пользователей. Для формализации математической постановки задачи исследований по обоснованию программ модернизации АСО требуется проанализировать их состав, структуру построения и основные тактико-технические характеристики.

1. Состав и структура автоматизированных систем охраны

Современные системы охраны стационарных удаленных объектов повышенной защищенности, отнесенных к КИИ, представляют собой сложные автоматизированные системы, включающие в свой состав, в соответствии с принятой в России концепцией, несколько функционально завершенных и объединенных в единый комплекс подсистем и дежурные силы охраны (дежурная смена охраны и обороны – караул (ДСОО-К)) [3–4].

Анализ структурной схемы типовых АСО стационарных удаленных объектов повышенной защищенности (рис. 1) показывает, что в общем случае применительно к рассматриваемой задаче существующие системы охраны предпочтительно декомпозировать на подсистемы, к которым относятся [5, 6]:

- подсистема технических средств обнаружения (ТСО), содержащая периметровые ТСО на рубежах охраны и средства охранной сигнализации;
- подсистема технических средств воздействия (ТСВ), включающая электризуемое заграждение (ЭЗ), башенно-пулеметную установку (БПУ) и инженерные заграждения (ИЗ);
- технические средства контроля зоны въездных ворот ($ТСО_В$);
- аппаратура управления и контроля системы (АУ);
- аппаратура (оборудование) электропитания (АЭП), содержащая преобразовательные устройства, токораспределительные устройства, источники резервного питания (аккумуляторные батареи);
- средства контроля и управления доступом на объект (СКУД);
- технические системы обеспечения жизнедеятельности ДСОО-К в караульном помещении (СКП);
- кабельная сеть системы на объекте.

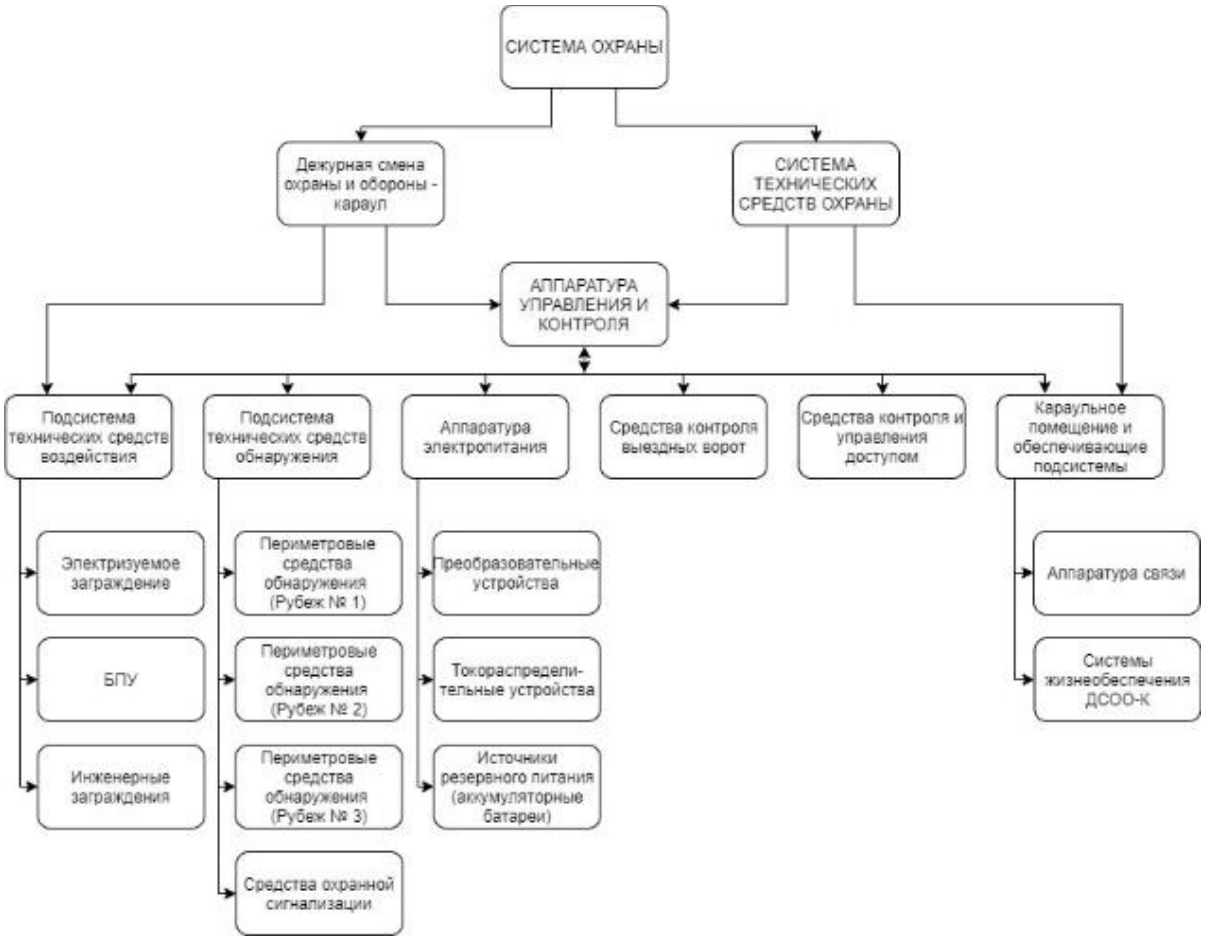


Рис. 1. Типовая структурная схема АСО стационарных удаленных объектов повышенной защищенности
(Fig.1. Typical scheme of the structure of an Automated Security System for stationary remote objects of increased security)

С помощью перечисленных составных частей формируются периметровая и локальные зоны охраны. Периметровая зона в виде замкнутого участка определенной ширины располагается вдоль внешней границы охраняемой территории, а локальные зоны – вокруг наиболее значимых элементов охраняемого объекта (зданий, сооружений, агрегатов).

Каждая из подсистем и входящие в нее составные части в процессе функционирования выполняют одну или несколько функций, возлагаемых на систему охраны в целом. Структуры построения существующих АСО в зависимости от типа стационарных удаленных объектов отличаются друг от друга составом средств и отдельных функциональных подсистем [7].

Примерный состав оборудования систем охраны I, II и III-го типов и АСО объекта с большим периметром (ОБП) приведен в табл. 1 [3].

Подсистема ТСО предназначена для обнаружения нарушителей при их попытках проникнуть на охраняемую территорию объекта, в периметровую и локальные зоны охраны, а также в здания и специальные сооружения.

Для АСО I и II-го типов характерным является то, что они не соответствуют требованиям в части оснащения рубежей охраны ТСО, работающих на различных физических принципах [3].

Таблица 1. Составные части подсистем АСО основных стационарных объектов

Тип АСО	СОСТАВНЫЕ ЧАСТИ ПОДСИСТЕМ АСО								
	ТСО		АУ	АЭП	ЭЗ	БПУ	$ТСО_В$	СКУД	СКП
	два рубежа	три рубежа							
I, II	+	–	+	+	+	+	–	–	+
III	–	+	+	+	+	+	–	–	+
ОБП	–	+	+	+	+	–	+	+	+

Подсистема технических средств воздействия (ТСВ) предназначена для информирования и предупреждения нарушителей при их попытках проникновения на охраняемый объект, а также сдерживания и поражения обнаруженных нарушителей на территории охраняемого объекта.

Основным назначением СКУД является управление доступом людей и техники на территорию охраняемого объекта, локальные зоны, здания и сооружения. Наряду с этим применяемые в составе СКУД средства контроля выполняют функции обнаружения запрещенных предметов и материалов при их проносе (провозе) через контрольно-пропускной пункт (КПП) [8]. Указанные средства во всех существующих АСО ограничиваются только их размещением в периметровой зоне охраны и отсутствуют в локальных зонах, а также в зданиях и сооружениях.

Аппаратура управления и контроля предназначена для сбора, обработки и отображения информации, поступающей от системы ТСО, формирования и выдачи сигналов «тревоги», команд на задействование ТСВ, автоматического контроля функционирования технических средств охраны, документирования событий (срабатывание средств обнаружения, включение и отключение технических средств воздействия, отказов и т.д.) с выдачей необходимой информации на пульт оператора [6].

Аппаратура электропитания АСО представляет собой совокупность средств, предназначенных для преобразования, распределения и передачи электрической энергии к потребителям от основного источника питания или источника, обеспечивающего гарантированное питание системы в режиме автономии.

Обеспечивающими системами являются системы связи, охранного освещения, вентиляции, водоснабжения, канализации и другие названия обеспечивающие функционирование подсистем и системы охраны в целом, а также несение службы ДСОО-К.

В составе существующих АСО стационарных удаленных объектов повышенной защищенности отсутствуют такие важные подсистемы, как подсистемы телевизионных средств наблюдения.

Анализ состава, структуры и назначения основных подсистем показывает, что существующие АСО стационарных объектов повышенной защищенности относятся к классу сложных человеко-машинных систем, качество функционирования которых в

значительной мере определяется характеристиками применяемых средств охраны, действиями личного состава ДСОО-К в соответствии с установленными порядком и правилами, а также особенностями охраняемого объекта.

Результаты анализа показывают также, что существующие АСО не в полной мере соответствуют требованиям руководящих документов, указывая, таким образом, на возможные направления их модернизации, включая применение ТСО, работающих на различных физических принципах действия, телевизионных средств наблюдения и средств проноса (провоза) запрещенных материалов. Причем, принципиально возможна частичная модернизация в виде замены одного из двух ТСО на более совершенные [8].

2. Основные тактико-технические характеристики АСО

Рассматривая АСО как сложную организационно-техническую систему, воспользуемся определением качества системы охраны [9], под которым понимается совокупность характеристик, определяющих степень пригодности данной системы для выполнения своего назначения. Тактико-технические характеристики АСО, как и любых других систем, определяются их назначением. Учитывая результаты исследований, приведенные в [3, 4, 11, 12], можно заключить, что основными характеристиками АСО, определяющими их качество, являются интегральные показатели:

- показатель эффективности;
- показатель надежности;
- показатель устойчивости функционирования;
- обобщенный показатель стоимости создания и эксплуатации АСО.

Данные характеристики качества АСО являются обобщенными, а их количественные значения зависят от структуры АСО, значений характеристик ее элементов (в том числе частных показателей назначения) и условий функционирования системы.

Важнейшей и наиболее общей характеристикой качества АСО является ее эффективность [10, 11, 13]. Эффективность АСО оценивается при помощи показателя эффективности Φ_0 – количественной меры, характеризующей способность системы выполнять свое назначение. За показатель эффективности системы охраны Φ_0 принимается вероятность выполнения системой своего назначения по предотвращению акций нарушителя (нарушителей) по проникновению к охраняемому объекту (на территорию, в здания, сооружения, агрегаты объекта). Этот показатель как основная числовая характеристика качества АСО, используется для сравнения различных вариантов построения системы на этапах ее создания и модернизации, а также для оценки результатов мероприятий по повышению эффективности системы на этапах ее доработки и эксплуатации. Показатель эффективности является функцией множества параметров системы и ее элементов [12, 13] и может быть представлен в виде функционала

$$\Phi_0 = F\left\| E_{ТСО}, E_{ТСВ}, E_{СКУД}, R_{АУ}, R_{АЭП}, P_{ДСОО-К}, f \right\|, \quad (1)$$

где $E_{ТСО} = R_{ТСО} P_{ТСО}$ – показатель эффективности подсистемы ТСО;
$R_{ТСО}$ – показатель технической надежности подсистемы ТСО;
$P_{ТСО}$ – вероятность обнаружения нарушителей техническими средствами;
$E_{ТСВ} = R_{ТСВ} P_{ТСВ}$ – показатель эффективности подсистемы ТСВ;
$R_{ТСВ}$ – показатель технической надежности подсистемы ТСВ;
$P_{ТСВ}$ – вероятность поражения нарушителей техническими средствами;
$E_{СКУД} = R_{СКУД} P_{СКУД}$ – показатель эффективность СКУД;
$R_{СКУД}$ – показатель технической надежности СКУД;

$P_{СКУД}$ – вероятность правильной идентификации СКУД персонала объекта;

$R_{АУ}$ – показатель технической надежности аппаратуры управления АСО;

$R_{АЭП}$ – показатель технической надежности АЭП системы;

$P_{ДСОО\text{-}К}$ – вероятность действий личного состава ДСОО-К в точном соответствии с инструкциями по несению боевого дежурства с АСО;

f – аргумент, отражающий взаимосвязь подсистем в структуре АСО.

В техническом задании на разработку системы задается значение показателя эффективности для определенного способа проникновения нарушителя на охраняемый объект.

Из выражения (1) следует, что одними из значимых параметров, от которых зависит эффективность АСО, являются показатели технической надежности составных частей, определяющие надежность системы в целом. В свою очередь надежность системы и ее составных частей зависит от совокупности свойств АСО при выполнении ею заданных функций по назначению в определенных условиях эксплуатации. К основным свойствам относятся: сохранение работоспособности, быстрое восстановление после отказа и продолжительность срока службы. За счет реализации этих свойств АСО стационарных объектов атомной промышленности относятся к классу восстанавливаемых и обслуживаемых систем.

С учетом результатов исследований, приведенных в [4, 5], в качестве показателей надежности АСО в работе приняты:

- вероятность безотказной работы системы $R(t)$ (сохранения работоспособного состояния) в течение заданного времени t

$$R(t) = e^{-\frac{t}{T_{ОС}}}, \quad (1)$$

где t – расчетное время;

$T_{ОС}$ – наработка АСО на неисправность;

- наработка на неисправность $T_{ОС}$ (среднее время работы между двумя неисправностями при эксплуатации системы)

$$T_{ОС} = \frac{1}{\Lambda} = \frac{1}{\sum_{i=1}^{M} \lambda_i}, \quad (2)$$

где λ_i – интенсивность неисправностей в i-ой подсистеме;

M – число типов подсистем в составе АСО.

За показатель устойчивости функционирования АСО принята ее наработка на ложную тревогу, определяемая по формуле:

$$T_{ЛТr,h} = \frac{\prod^{h} T_{ЛТl}}{rm^r \tau^{r-1} \sum^{\left(C_h^r\right)_{h-r}} \prod T_{ЛТl}}, \quad (3)$$

где h – количество рубежей обнаружения;

r – количество сигналов, необходимых для срабатывания подсистемы ТСО;

$T_{ЛТl}$ – наработка на ложную тревогу l-го сектора обнаружения;

m – количество секторов обнаружения в h-ом рубеже обнаружения;

C_h^r – число сочетаний из h по r;

$\left(C_h^r\right)$ – число членов суммы;

τ – время обработки информации в логическом устройстве системы охраны.

В качестве обобщенного показателя стоимости АСО принимаются суммарные затраты C на жизненный цикл

$$C = \frac{1}{V_N} C_P + C_{СП} + C_{СМ} + C_Э, \quad (4)$$

где C_P – единовременные затраты на разработку АСО;

$C_{СП}$ – стоимость серийного производства АСО;

$C_{СМ}$ – стоимость строительно-монтажных работ при вводе АСО в эксплуатацию;

$C_Э$ – общие затраты на эксплуатацию системы;

V_N – объем серийного производства АСО.

Эксплуатационные затраты $C_Э$ относятся к числу наиболее значимых показателей, влияющих на поддержание АСО в готовности к применению по назначению, и рассчитываются для определенного периода времени по выражению

$$C_Э = C_{ТО} + C_{ГН} + C_{ЛС} + C_{ЗИП} + C_{УН}, \quad (6)$$

где $C_{ТО}$ – затраты на плановые эксплуатационно-технические мероприятия (приведение в готовность, контроль технического состояния, ТО системы);

$C_{ГН}$ – затраты на обеспечение гарантийного надзора за системой охраны;

$C_{ЛС}$ – стоимость содержания персонала, обслуживающего систему;

$C_{ЗИП}$ – затраты на приобретение, хранение и обслуживание ЗИП;

$C_{УН}$ – затраты на устранение неисправностей и ремонтно-восстановительные работы.

Очевидно, что разработчик системы, осуществляющий ее модернизацию, будет стремиться к достижению наиболее высоких значений рассмотренных выше показателей качества при минимуме затрат. Это предполагает для анализа и оценки возможных вариантов построения модернизируемых АСО использовать обобщенный комплексный показатель. В работе в качестве такого показателя выбран комплексный показатель приоритета η-го варианта построения системы, определяемый функционалом

$$Q_\eta = Q_\eta\left[\Phi_0, T_{ОС}, T_{ЛТ}, \Delta T, C_У, \bar{\mu}_П\right], \quad (7)$$

где $\bar{\mu}_П$ – математическое ожидание вектора стратегий нарушителя, характеризующего его техническую оснащенность и тактику действий;

ΔT – продолжительность эксплуатации АСО после модернизации;

$C_У$ – удельные затраты в предмодернизационный период.

Объединение нескольких интегральных показателей в один комплексный показатель осуществляется с помощью процедур их специальной логико-весовой обработки, предусматриваемых в методе расстановки приоритетов.

Выбранные интегральные характеристики позволяют оценить влияние на качество функционирования АСО не только заложенных в них технических решений, но и проводимых мероприятий по поддержанию систем в готовности к применению, составляющих систему эксплуатации АСО [13, 14].

Кроме того, выбранные показатели обеспечивают возможность учета влияния на качество систем охраны интенсивности возникновения неисправностей в них как в период гарантийной, так и постгарантийной эксплуатации. Как показали исследования [3, 4], для указанных сроков эксплуатации интенсивность неисправностей существенно различается

и по-разному сказывается на величине показателей надежности и эффективности составных частей и системы в целом. В итоге это предполагает корректировку содержания и периодичности мероприятий в системе эксплуатации.

А далее, с учетом проведенного анализа состава, структуры построения и основных тактико-технических характеристик АСО, может быть сформулирована математическая постановка задачи исследований.

Заключение

Для формализации математической постановки задачи исследований по обоснованию программ модернизации АСО был проанализирован их состав, структура построения и основные тактико-технические характеристики, который показал, что существующие АСО не в полной мере соответствуют требованиям руководящих документов, указывая, таким образом, на возможные направления их модернизации, включая применение ТСО, работающих на различных физических принципах действия, телевизионных средств наблюдения и средств проноса (провоза) запрещенных материалов. Причем, принципиально возможна частичная модернизация в виде замены одного из двух ТСО на более совершенные. Было проведено объединение нескольких интегральных показателей в один комплексный показатель с помощью процедур их специальной логико-весовой обработки, предусматриваемых в методе расстановки приоритетов. Выбранные интегральные характеристики позволяют: оценить влияние на качество функционирования АСО не только заложенных в них технических решений, но и проводимых мероприятий по поддержанию систем в готовности к применению, составляющих систему эксплуатации АСО; обеспечить возможность учета влияния на качество систем охраны интенсивности возникновения неисправностей в них как в период гарантийной, так и постгарантийной эксплуатации.

СПИСОК ЛИТЕРАТУРЫ:

1. Сычев Ю.Н. Защита информации и информационная безопасность. Учебное пособие. М.: Инфра-М, 2020. – 201 с.
2. Белоус А.А. Кибербезопасность объектов топливно-энергетического комплекса. Концепции, методы и средства обеспечения. Практическое пособие. М.: Инфра-Инженерия, 2020. – 644 с.
3. Арифуллин, Марат В., Евсеев, Владимир Л. Анализ технического состояния автоматизированных систем охраны и мероприятий по поддержанию их в готовности к применению. Безопасность информационных технологий, [S.l.]. Т. 21, № 2, май 2014. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/211 (дата обращения: 05.12.2020).
4. Иваненко, Виталий Г., Евсеев, Владимир Л. Разработка предложений по совершенствованию системы поддержания автоматизированных систем охраны в готовности к применению в постгарантийный период эксплуатации. Безопасность информационных технологий, [S.l.], Т. 21, № 3. С. 66–70, сен. 2014. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/168 (дата обращения: 05.12.2020).
5. Магауенов Р.Г., Семёнов О.И., Афанасьева Л.Г., Егоров А.Н. Толковый словарь терминов по системам физической защиты /Под ред. Р.Г. Магауенова. М.: Секьюрити Фокус, 2019. – 276 с.
6. Магауенов Р.Г. Системы охранной сигнализации: основы теории и принципы построения: Учебное пособие. М.: Горячая линия – Телеком, 2004. – 367 с.: ил.
7. Физические средства защиты информации. //Национальная библиотека им. Н.Э. Баумана / Bauman national library. URL: https://ru.bmstu.wiki/Физические_средства_защиты_информации (дата обращения: 05.12.2020).
8. Мишин Е.Т., Леонов В.А., Папанин Г.П. Применение технических средств в системах охраны промышленных объектов. М.: Мин. авиа. пром. СССР, 1985. – 100 с.
9. Проников А.С. Параметрическая надежность машин. М.: Изд-во МГТУ им. Н.Э. Баумана, 2002. – 560 с.
10. Мосолов А. С. Оценка эффективности системы безопасности на основе метода Монте-Карло // Системы безопасности. 2014. № 1. С. 74–77. URL: http://secuteck.ru/articles2/science/otsenka-effektivnosti-sistemy-bezopasnosti-na-osnove-metoda-monte-karlo (дата обращения: 05.12.2020).

11. Дурденко, Владимир Андреевич, Рогожин, Александр Александрович, Баторов, Батор Октябрьевич. Моделирование и оценка эффективности интегрированных систем безопасности объектов, подлежащих государственной охране. Вестник Воронежского государственного университета. Серия: Системный анализ и информационные технологии. 2018, № 3. С. 82–92. URL: http://www.vestnik.vsu.ru/pdf/analiz/2018/03/2018-03-10.pdf (дата обращения: 05.12.2020).
12. Мартиросян, Р.М. и др. Автоматизированный охранный комплекс. Электромагнитные волны и электронные системы. 2011. Т. 16, № 2. С. 37–42. URL: https://www.elibrary.ru/item.asp?id=16336165(дата обращения: 05.12.2020)..
13. Костин, В.Н. Проектирование систем физической защиты потенциально опасных объектов на основе развития современных информационных технологий и методов синтеза сложных систем: монография / В.Н. Костин, С.Н. Шевченко, Н.В. Гарнова. Оренбург: ООО ИПК «Университет», 2014. – 202 с.
14. Meyer-Nieberg S., Beyer HG. (2007) Self-Adaptation in Evolutionary Algorithms. In: Lobo F.G., Lima C.F., Michalewicz Z. (eds) Parameter Setting in Evolutionary Algorithms. Studies in Computational Intelligence. V. 54. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-540-69432-8_3.

REFERENCES:

[1] Sychev Yu.N. Information protection and information security. Tutorial. M.: Infra-M, 2020. – 201 p. (in Russian).
[2] Belous A.A. Cybersecurity of objects of the fuel and energy complex. Concepts, methods and means of support. A practical guide. M.: Infra-Engineering, 2020. – 644 p. (in Russian).
[3] Arifullin, Marat V., Yevseyev, Vladimir L. The Analysis of Technical Condition of the Automated Systems of Protection and Actions for Their Maintenance in Readiness for Application. IT Security (Russia), [S.l.]. V. 21, no. 2, may 2014. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/211 (accessed: 05.12.2020) (in Russian).
[4] Ivanenko, Vitaliy G., Evseev, Vladimir L. Development of Offers on Perfection of System of Maintenance of Automated Systems of Protection in Readiness for Use in Post-Warranty Period of Operation. IT Security (Russia), [S.l.]. V. 21, no. 3, sep. 2014. ISSN 2074-7136 URL: https://bit.mephi.ru/index.php/bit/article/view/168 (accessed: 05.12.2020) (in Russian).
[5] Magauenov R.G., Semyonov O.I., Afanasyeva L.G., Egorov A.N. Explanatory dictionary of terms for physical protection systems Ed. R.G. Magauenov M .: Security Focus, 2019. – 276 p. (in Russian).
[6] Magauenov R.G. Burglar alarm systems: the basics of the theory and principles of construction: Textbook. M.: Hot line - Telecom, 2004. – 367 p.: Ill. (in Russian).
[7] Physical means of information protection. National Library. N.E. Bauman. Bauman national library. URL: https://ru.bmstu.wiki/physical_devices_of_information_protection (accessed: 05.12.2020) (in Russian).
[8] Mishin E.T., Leonov V.A., Papanin G.P. The use of technical means in security systems for industrial facilities. M.: Min. air. prom. USSR, 1985. – 100 p. (in Russian).
[9] Pronikov A.S. Parametric reliability of machines. M.: Publishing house of MSTU im. N.E. Bauman, 2002. – 560 p. (in Russian).
[10] Mosolov AS Evaluation of the effectiveness of a security system based on the Monte Carlo method. Security systems. 2014. no. 1. P. 74–77. URL: http://secuteck.ru/articles2/science/otsenka-effektivnosti-sistemy-bezopasnosti-na-osnove-metoda-monte-karlo (accessed: 05.12.2020) (in Russian).
[11] Durdenko, Vladimir Andreevich; Rogozhin, Alexander Alexandrovich; Batorov, Bator Oktyabrievich. Modeling and evaluation of the effectiveness of integrated security systems for objects subject to state protection. Voronezh State University Bulletin. Series: System Analysis and Information Technology. 2018, no. 3. P. 82–92. URL: http://www.vestnik.vsu.ru/pdf/analiz/2018/03/2018-03-10.pdf (accessed: 05.12.2020) (in Russian).
[12] Martirosyan, R.M.; Gulyan, A.G.; Pirumyan, G.A. Automated security complex. Electromagnetic waves and electronic systems. 2011. T. 16, no. 2. P. 37–42. URL: http://www.vestnik.vsu.ru/pdf/analiz/2018/03/2018-03-10.pdf (accessed: 05.12.2020) (in Russian).
[13] Kostin, V.N. Design of physical protection systems for potentially dangerous objects based on the development of modern information technologies and methods of synthesis of complex systems: monograph. V.N. Kostin, S.N. Shevchenko, N.V. Garnov. Orenburg: LLC IPK "University", 2014. – 202 p. (in Russian).
[14] Meyer-Nieberg S., Beyer HG. (2007) Self-Adaptation in Evolutionary Algorithms. In: Lobo F.G., Lima C.F., Michalewicz Z. (eds) Parameter Setting in Evolutionary Algorithms. Studies in Computational Intelligence. V. 54. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-540-69432-8_3.

Поступила в редакцию – 18 ноября 2020 г. Окончательный вариант – 15 января 2021 г.
Received – November 18, 2020. The final version – January 15, 2021.

Ирина Г. Дровникова[1], Елена С. Овчинникова[2], Евгений А. Рогозин[3]
[1-3]Воронежский институт министерства внутренних дел Российской федерации,
пр-т Патриотов, 53, Воронеж, 394065, Россия
[1]e-mail: idrovnikova@vail.ru, https://orcid.org/0000-0001-5265-5875
[2]e-mail: yelena_ovchinnikova1@mail.ru, https://orcid.org/0000-0003-4139-9524
[3]e-mail: evgenirogozin@yandex.ru, https://orcid.org/0000-0002-4455-7535

ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ ДИНАМИКИ РЕАЛИЗАЦИИ СЕТЕВЫХ АТАК В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ОРГАНОВ ВНУТРЕННИХ ДЕЛ В ПРОГРАММНОЙ СРЕДЕ «CPN TOOLS»

DOI: http://dx.doi.org/10.26583/bit.2021.1.03

Аннотация. В статье представлены результаты имитационного моделирования динамики реализации сетевой атаки в ее конфликтном взаимодействии с системой защиты информации от несанкционированного доступа автоматизированной системы в виде количественных значений вероятностно-временных характеристик атаки. Целью имитационного моделирования является выявление возможности использования полученных результатов при расчете вероятности реализации и проведении количественной оценки опасности реализации сетевых атак на информационный ресурс автоматизированных систем, эксплуатируемых в защищенном исполнении на объектах информатизации органов внутренних дел (ОВД). Представлена обобщенная формальная модель функционирования дестабилизирующего воздействия и построена сеть Петри-Маркова, отражающая динамику протекания информационного конфликта с учетом различий возможностей конфликтующих сторон. Разработана имитационная модель, описывающая механизм информационного конфликта «Сетевая атака – система защиты», и проведено имитационное моделирование, используя программную среду «CPN Tools». Результаты имитационного моделирования представлены в виде временной статистики процесса реализации сетевой атаки в динамике конфликтного взаимодействия с системой защиты. Приведены средние времена реализации типовых сетевых атак на информационный ресурс защищенных автоматизированных систем ОВД, полученные путем имитационного моделирования данных атак с помощью сети Петри-Маркова. Приведены перспективы использования полученных результатов для повышения защищенности автоматизированных систем при их разработке и эксплуатации на объектах информатизации ОВД.

Ключевые слова: система защиты информации, несанкционированный доступ, сетевая атака, информационный конфликт, сеть Петри-Маркова, вероятностно-временные характеристики, имитационное моделирование, программная среда «CPN Tools».

Для цитирования: ДРОВНИКОВА, Ирина Г.; ОВЧИННИКОВА, Елена С.; РОГОЗИН, Евгений А. ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ ДИНАМИКИ РЕАЛИЗАЦИИ СЕТЕВЫХ АТАК В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ОРГАНОВ ВНУТРЕННИХ ДЕЛ В ПРОГРАММНОЙ СРЕДЕ «CPN TOOLS». Безопасность информационных технологий, [S.l.], v. 28, n. 1, p. 29–41, jan. 2021. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1318>. Дата доступа: 20 jan. 2021. DOI: http://dx.doi.org/10.26583/bit.2021.1.03.

Irina G. Drovnikova[1], Elena S. Ovchinnikova[2], Evgeni A. Rogozin[3]
[1-3]Voronezh Institute of the Ministry of the Interior,
Prospekt Patriotov, 53, Voronezh, 394065, Russia
[1]e-mail: idrovnikova@vail.ru, https://orcid.org/0000-0001-5265-5875
[2]e-mail: yelena_ovchinnikova1@mail.ru, https://orcid.org/0000-0003-4139-9524
[3]e-mail: evgenirogozin@yandex.ru, https://orcid.org/0000-0002-4455-7535

Simulation of the dynamics of network attacks in automated systems of internal affairs bodies in the "CPN Tools" software environment

DOI: http://dx.doi.org/10.26583/ bit.2021.1.03

Abstract. The paper presents the results of simulation modeling of the dynamics of the implementation of a network attack in its conflict interaction with the information protection system from unauthorized access of an automated system in the form of quantitative values of the probabilistic and time characteristics of the attack. The aim of simulation modeling is to identify the possibility of using the results obtained in calculating the implementation probability and conducting an accurate quantitative assessment of the risk of network attacks on the information resource of automated systems operated in a protected version at the objects of Informatization of internal Affairs bodies. A generalized formal model of the functioning of a destabilizing influence is presented and a Petri-Markov network is constructed that reflects the dynamics of the information conflict, taking into account the differences in the capabilities of the conflicting parties. A simulation model describing the mechanism of information conflict "Network attack – protection system" was developed, and simulation was performed using the "CPN Tools" software environment. The results of simulation modeling are presented in the form of time statistics of the process of implementing a network attack in the dynamics of conflict interaction with the protection system. The average implementation times of typical network attacks on the information resource of protected automated systems of internal Affairs bodies, obtained by simulating these attacks using the Petri-Markov network in the "CPN Tools" software environment, are given. The prospects of using the results obtained to improve the real security of automated systems in their development and operation at the objects of Informatization of internal Affairs bodies are outlined.

Keywords: information protection system, unauthorized access, network attack, information conflict, Petri-Markov network, probabilistic-time characteristics, simulation modeling, "CPN Tools" software environment.

For citation: DROVNIKOVA, Irina G.; OVCHINNIKOVA, Elena S.; ROGOZIN, Evgeni A. Simulation of the dynamics of network attacks in automated systems of internal affairs bodies in the "CPN Tools" software environment. IT Security (Russia), [S.l.], v. 28, n. 1, p. 29–41, jan. 2021. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1318>. Date accessed: 20 jan. 2021. DOI: http://dx.doi.org/10.26583/bit.2021.1.03.

Введение

Процесс функционирования современных автоматизированных систем (АС), эксплуатируемых в защищенном исполнении на объектах информатизации органов внутренних дел (ОВД), характеризуется применением злоумышленниками все более изощренных методов социальной инженерии, OSINT (Open Source INTelligence) поиска, сбора и анализа информации о структуре системы на основе открытых источников, иных разведывательных методов, приводящих к успешной реализации удаленных воздействий (сетевых атак), результатом которой является нанесение ущерба информационному ресурсу АС ОВД (нарушение конфиденциальности, целостности или доступности служебной информации) в соответствии с предметом атаки [1, 2]. Это приводит к необходимости учета возможной опасности реализации сетевых атак на начальных этапах разработки системы[1], что предполагает проведение количественной оценки опасности их реализации [3].

Анализ открытых литературных источников, международных и отраслевых стандартов Российской Федерации, нормативных документов Федеральной службы по техническому и экспертному контролю (ФСТЭК) России и руководящих документов МВД России, посвященных вопросам информационной безопасности (ИБ) АС[2-6] [4–6],

[1]ГОСТ Р 51583-2014. Порядок создания автоматизированных систем в защищенном исполнении.
[2]ISO/IEC 15408-2012. Common Criteria for Information Technology Security Evaluation
[3]ГОСТ 34.601-90. Автоматизированные системы. Стадии создания.
[4]ФСТЭК России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.
[5]ФСТЭК России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного

показал недостаточную проработанность данного вопроса, в частности, исследования сетевых атак в динамическом режиме. Это подтверждает актуальность проблемы имитационного моделирования динамики реализации сетевых атак в защищенных АС на объектах информатизации ОВД с целью исследования вероятностно-временных характеристик (ВВХ), необходимых для проведения количественной оценки опасности их реализации.

1. Постановка задачи

Процесс имитационного моделирования динамики реализации сетевых атак на информационный ресурс АС, эксплуатируемых в защищенном исполнении на объектах информатизации ОВД, включает следующие этапы:

1. На основе вербальной модели процесса функционирования системы защиты информации (СЗИ) от несанкционированного доступа (НСД), в условиях реализации сетевых атак на информационный ресурс защищенных АС ОВД, создание обобщенной формальной модели функционирования дестабилизирующего воздействия в динамике конфликтного взаимодействия с помощью сети Петри-Маркова (СПМ).
2. Построение имитационной модели, описывающей механизм информационного конфликта «Сетевая атака – СЗИ от НСД», используя программную среду «CPN Tools».
3. Осуществление имитационного моделирования и представление его результатов в табличной форме в виде значений ВВХ сетевой атаки в динамике информационного конфликта с СЗИ от НСД.

2. Метод исследования

Реализация сетевых атак на информационный ресурс современных АС ОВД представляет собой сложный динамический процесс, включающий множество взаимовлияющих параллельных процессов. Поэтому предпочтительным инструментом для его моделирования и анализа являются СПМ [7], объединяющие возможности и преимущества двух традиционных подходов к моделированию отказов в сложных системах, основанных на теории сетей Петри и марковских (а в более общем случае полумарковских) процессах [8, 9]. Построение обобщенной динамической модели информационного конфликта «Сетевая атака – СЗИ от НСД» с использованием СПМ, наглядно описывающей все состояния и условия переходов в рассматриваемом конфликте, позволяет исследовать процесс реализации сетевой атаки с определением ее временных и вероятностных характеристик.

Одним из методов определения количественных параметров указанных характеристик служит натурный эксперимент. Преодолеть затруднение, заключающееся в значительном усложнении его практического проведения в случае малого времени реализации сетевой атаки, позволяет использование программной среды имитационного моделирования «CPN Tools» – мощного инструмента моделирования и анализа сетей различного уровня сложности, к которым, несомненно, относятся и СПМ, доступного для ОС семейства Windows и Linux [10]. Имитационное моделирование в «CPN Tools», являясь дискретно-событийным, предполагает мгновенную смену состояний СПМ, что полностью соответствует конечному полумарковскому процессу. Среда «CPN Tools» предоставляет возможность программирования на унифицированном языке моделирования «Unified Modeling Language». Программный продукт «CPN Tools»

доступа к информации.

[6]Об утверждении Концепции обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года: приказ МВД России от 14.03.2012 № 169.

позволяет генерировать, анализировать пространство состояний модели, а также получать отчеты о работе сети в виде невременной и временной статистики [11].

При проведении имитационного моделирования процесса реализации сетевой атаки в динамике ее конфликтного взаимодействия с СЗИ от НСД с помощью СПМ вводятся следующие обозначения для элементов сети: s_i – все возможные состояния (позиции) рассматриваемого процесса, t_j – все возможные переходы между состояниями.

3. Модели и результаты исследования

Для обеспечения успешности реализации сетевой атаки или успешности защиты информационного ресурса АС ОВД необходимо оценить возможности обеих сторон в информационном конфликте «Сетевая атака – СЗИ от НСД».

В научных исследованиях информационного конфликта традиционно принимается допущение, что изначальные возможности конфликтующих сторон равны и конфликтные действия начинаются ими одновременно [12, 13], что в реальной практике эксплуатации защищенных АС ОВД выполняется крайне редко. Также должна быть учтена возможность выигрыша конфликта стороной, изначально не имеющей преимуществ, в результате возможных ошибок противоположной стороны (запаздывания ее действий, либо неадекватной реакции на воздействие). Следовательно, при разработке формальной модели функционирования дестабилизирующего воздействия в динамике конфликтного взаимодействия необходимо учитывать различия начальных и потенциальных возможностей конфликтующих субъектов.

Развитие и исход информационного конфликта «Сетевая атака – СЗИ от НСД» напрямую зависят от значений средних времен обнаружения сетевой атакой системы защиты, обнаружения системой защиты атаки и начала противодействия системы защиты сетевой атаке. Согласно результатам исследований, опубликованным в [1], средние значения указанных времен соответственно равны: $\tau_{\text{об ат}\rightarrow\text{СЗИ}}$ = 40 с, $\tau_{\text{об СЗИ}\rightarrow\text{ат}}$ = 52 с, $\tau_{\text{непр СЗИ}\rightarrow\text{ат}}$ = 1 с.

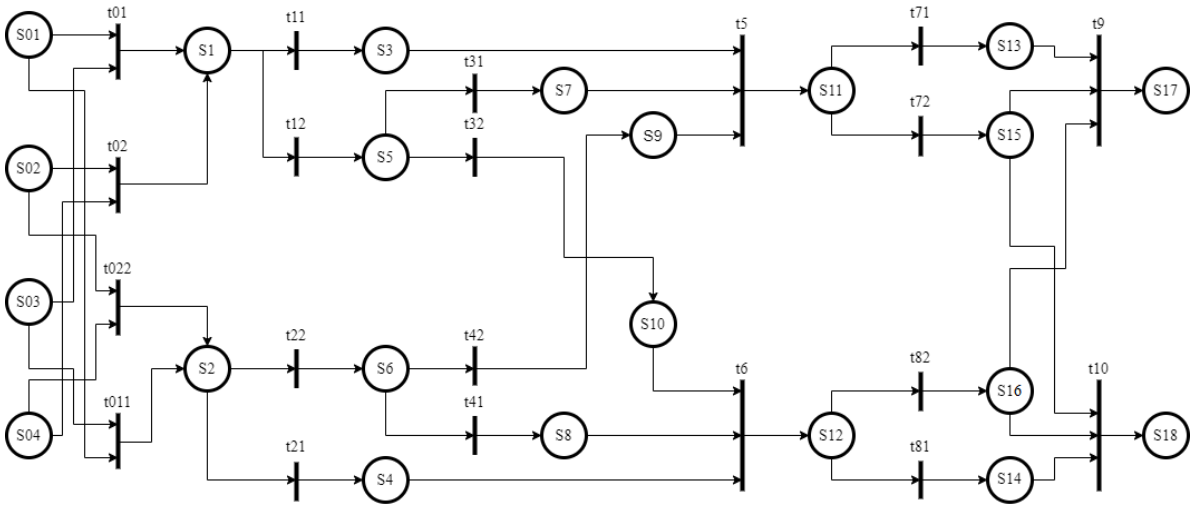
С учетом вышеизложенного для исследования информационного конфликта «Сетевая атака – СЗИ от НСД» в АС ОВД рассмотрим ситуацию, когда ответные действия системы защиты начинаются в процессе реализации сетевой атаки, то есть до наступления момента начала ее действия. В этом случае атака будет реализована, если все действия СЗИ от НСД вплоть до полного устранения эффективности попыток злоумышленника продолжать атаку (запрет обработки сообщений с блокированного адреса) не успеют завершиться к моменту начала действия атаки.

В [14, 15] подробно рассмотрены вербальная, вероятностная и обобщенная графовая модели динамики информационного конфликта «Сетевая атака – Система защиты» в АС ОВД, на основе которых с помощью СПМ построена представленная на рис. 1 обобщенная формальная модель, раскрывающая основные этапы данного конфликта.

Имитационная модель указанной сети, построенная при помощи программного продукта «CPN Tools», приведена на рис. 2.

В качестве начальных возможностей конфликтующих сторон, по которым осуществляется их сравнение в указанных моделях, рассматриваются производительности и объемы памяти сетевой атаки и СЗИ от НСД, определяемые в ходе натурного эксперимента. При этом под производительностью сетевой атаки (СЗИ от НСД) понимается количество выполняемых сетевой атакой (СЗИ от НСД) вредоносных (защитных) функций в единицу времени, а объем памяти сетевой атаки (СЗИ от НСД) представляет собой объем оперативной памяти, отвлекаемой на выполнение вредоносных

(защитных) функций сетевой атакой (СЗИ от НСД) из оперативной памяти АС, используемой для инициирования данной атаки (эксплуатирующей данную систему защиты).



s_{01}, s_{03} – производительность сетевой атаки, СЗИ от НСД задана;
t_{01}, t_{011} – сравнение производительностей сетевой атаки и СЗИ от НСД;
s_{02}, s_{04} – объем памяти сетевой атаки, СЗИ от НСД задан;
t_{02}, t_{022} – сравнение объемов памяти сетевой атаки и СЗИ от НСД;
s_1, s_2 – сетевая атака, СЗИ от НСД изначально имеет преимущество;
t_{11}, t_{21} – усиление изначального преимущества сетевой атакой, СЗИ от НСД;
s_3, s_4 – сетевая атака, СЗИ от НСД усиливает изначально имеющееся преимущество;
t_{12}, t_{22} – получение временного преимущества СЗИ от НСД, сетевой атакой;
s_5, s_6 – СЗИ от НСД противостоит сетевой атаке и получает временное преимущество, сетевая атака противостоит СЗИ от НСД и получает временное преимущество;
t_{31}, t_{41} – возвращение утерянного преимущества сетевой атакой, СЗИ от НСД;
s_7, s_8 – сетевая атака противостоит СЗИ от НСД и возвращает утерянное преимущество, СЗИ от НСД противостоит сетевой атаке и возвращает утерянное преимущество;
t_{32}, t_{42} – усиление временного преимущества СЗИ от НСД, сетевой атакой;
s_9, s_{10} – сетевая атака, СЗИ от НСД усиливает временное преимущество;
t_5, t_6 – усиление имеющегося преимущества сетевой атакой, СЗИ от НСД;
s_{11}, s_{12} – сетевая атака, СЗИ от НСД усиливает имеющееся преимущество;
t_{71}, t_{81} – закрепление преимущества за сетевой атакой, СЗИ от НСД;
s_{13}, s_{14} – преимущество за сетевой атакой, СЗИ от НСД закреплено;
t_{72} – противостояние СЗИ от НСД сетевой атаке;
s_{15} – СЗИ от НСД противостоит сетевой атаке;
t_{82} – проведение «взлома» СЗИ от НСД сетевой атакой;
s_{16} – сетевая атака «взламывает» СЗИ от НСД;
t_9 – преодоление СЗИ от НСД;
s_{17} – финальное состояние: «взлом» СЗИ от НСД, победа сетевой атаки;
t_{10} – блокирование сетевой атаки;
s_{18} – финальное состояние: защита АС ОВД, победа СЗИ от НСД

Рис. 1. СПМ, моделирующая информационный конфликт «Сетевая атака – СЗИ от НСД» (Fig. 1. SPM modeling information conflict "Network attack – SPI from NSD")

Для построения сети и имитации ее функционирования приближенно к реальному взаимодействию сетевой атаки с системой защиты проведем конфигурацию в виде создания сегмента кода на языке UML (рис. 3). Полученная при этом имитационная модель представлена на рис. 4.

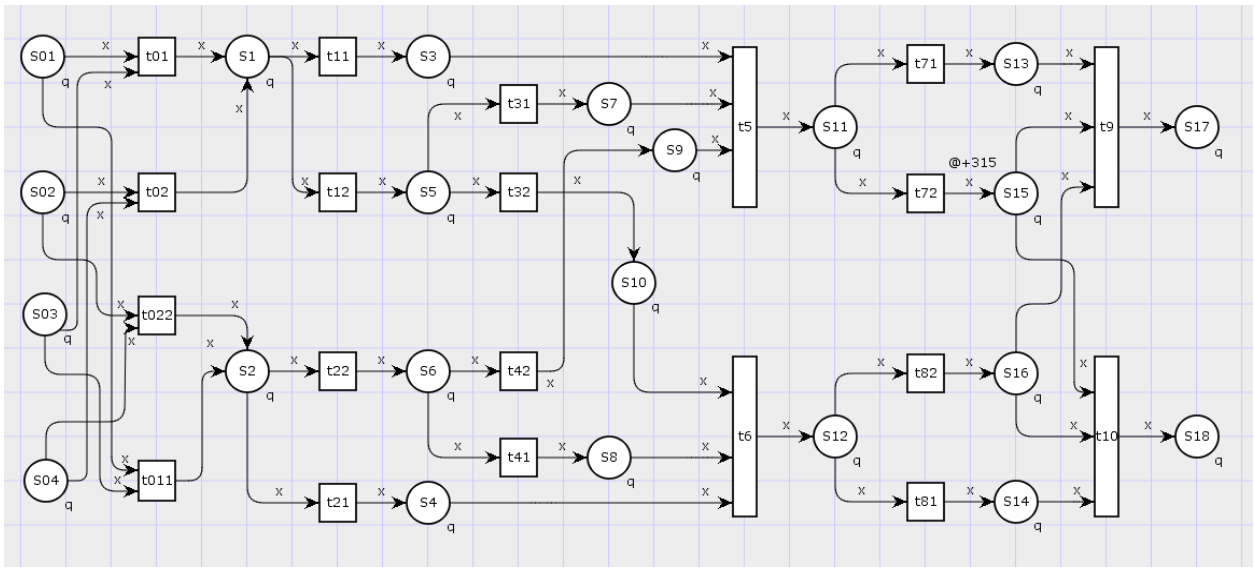


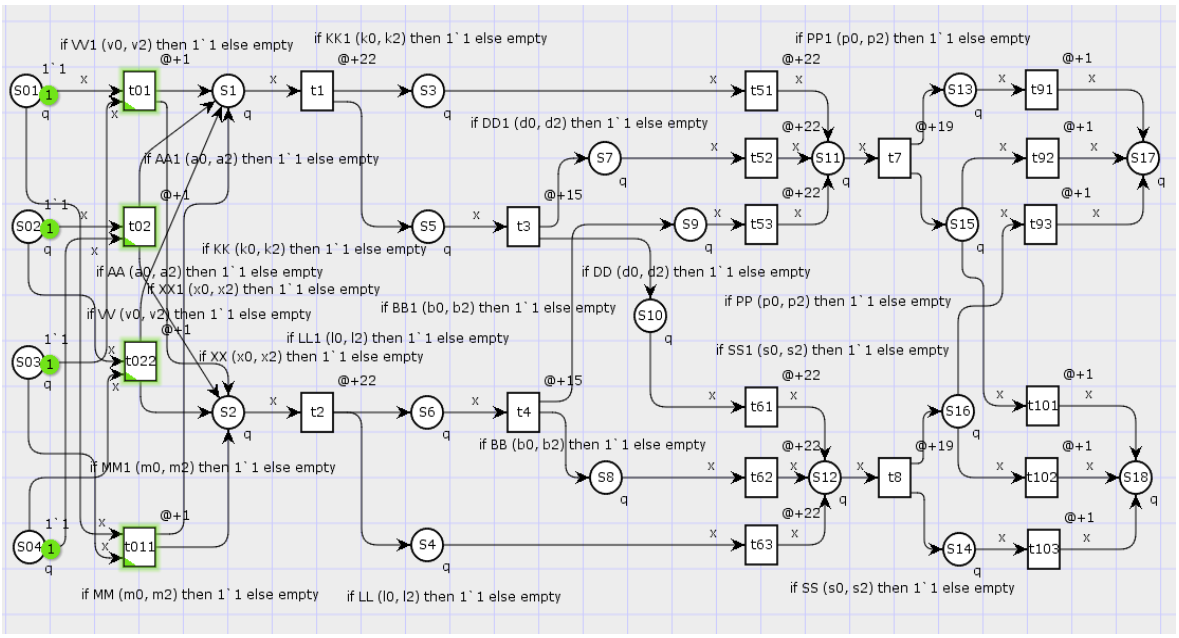
Рис. 2. Имитационная модель информационного конфликта «Сетевая атака – СЗИ от НСД», построенная в программной среде «CPN Tools»
(Fig. 2. Simulation model of information conflict "Network attack – SPI from NSD", built in the software environment "CPN Tools")

```
Declarations
  Standard priorities
  Standard declarations
    colset UNIT
    colset BOOL
    colset INT
    colset q = INT timed;
    var x : INT;
    fun curTime() = IntInf.toInt(!CPN'Time.model_time)
    colset VV = int with 1..100;
    var v0 : VV;
    val v2 = 10;
    fun VV (v0, v2) = (v0 <= v2);
    fun VV1 (v0, v2) = (v0 > v2);
    colset AA = int with 1..100;
    var a0 : AA;
    val  a2 = 10;
    fun AA (a0, a2) = (a0 <= a2);
    fun AA1 (a0, a2) = (a0 > a2);
    colset XX = int with 1..100;
    var x0 : XX;
    val x2 = 10;
    fun XX (x0, x2) = (x0 <= x2);
    fun XX1 (x0, x2) = (x0 > x2);
    colset MM = int with 1..100;
    var m0 : MM;
    val m2 = 10;
```

Рис. 3. Настройка сети, имитирующей информационный конфликт «Сетевая атака – СЗИ от НСД»
(Fig. 3. Setting up a network that simulates an information conflict "Network attack – SPI from NSD")

Поскольку представленная на рис. 1 обобщенная формальная модель имеет нелинейный характер, то для проведения имитационного моделирования информационного конфликта «Сетевая атака – СЗИ от НСД» с получением адекватных характеристик на выходе определим необходимое количество прогонов по СПМ на основе методики, изложенной в [10].

Для проверки адекватности модели осуществим необходимое количество шагов, в результате которых суммарное количество фишек в состояниях s_1 и s_2, s_{11} и s_{12}, s_{17} и s_{18} составит 100: в состояниях s_1 и s_2 – 92 и 8 фишек (рис. 5), в состояниях s_{11} и s_{12} – 94 и 6 фишек (рис. 6), в состояниях s_{17} и s_{18} – 99 и 1 фишка (рис. 7).



t_{01}, t_{011} – сравнение производительностей сетевой атаки и СЗИ от НСД;
t_{02}, t_{022} – сравнение объемов памяти сетевой атаки и СЗИ от НСД;
t_1 – усиление изначального или получение временного преимущества сетевой атакой;
t_2 – усиление изначального или получение временного преимущества СЗИ от НСД;
t_3 – возвращение утерянного или усиление временного преимущества сетевой атакой;
t_4 – возвращение утерянного или усиление временного преимущества СЗИ от НСД;
t_{51}, t_{52} , t_{53} – усиление имеющегося преимущества сетевой атакой;
t_{61}, t_{62}, t_{63} – усиление имеющегося преимущества СЗИ от НСД;
t_7 – закрепление преимущества за сетевой атакой или противостояние СЗИ от НСД сетевой атаке;
t_8 – закрепление преимущества за СЗИ от НСД или проведение «взлома» СЗИ от НСД сетевой атакой;
t_{91}, t_{92}, t_{93} – преодоление СЗИ от НСД;
t_{101}, t_{102}, t_{103} – блокирование сетевой атаки

Рис. 4. Конфигурированная имитационная модель информационного конфликта «Сетевая атака – СЗИ от НСД»
(Fig. 4. Configured simulation model of information conflict "Network attack – SPI from NSD")

Тогда частоту появления фишек в состояниях s_1, s_{11} и s_{17} рассчитаем по формулам:

$$\rho_{s_1 t_{01}} = \frac{46}{100} = 0.46,\ \rho_{s_1 t_{02}} = \frac{46}{100} = 0.46,\ \rho_{s_{11} t_5} = \frac{94}{100} = 0.94,$$

$$\rho_{s_{17} t_9} = \frac{99}{100} = 0.99.$$

Определим необходимое количество прогонов по сети для вероятности появления события с точностью $\varepsilon = 0,01$ и достаточностью D = 0,99 с помощью выражения:

$$N = \frac{\rho(1-\rho)}{\varepsilon^2}\left[\Phi_0^{-1}\frac{D}{2}\right]^2,$$

где Φ_0 – функция Лапласа.

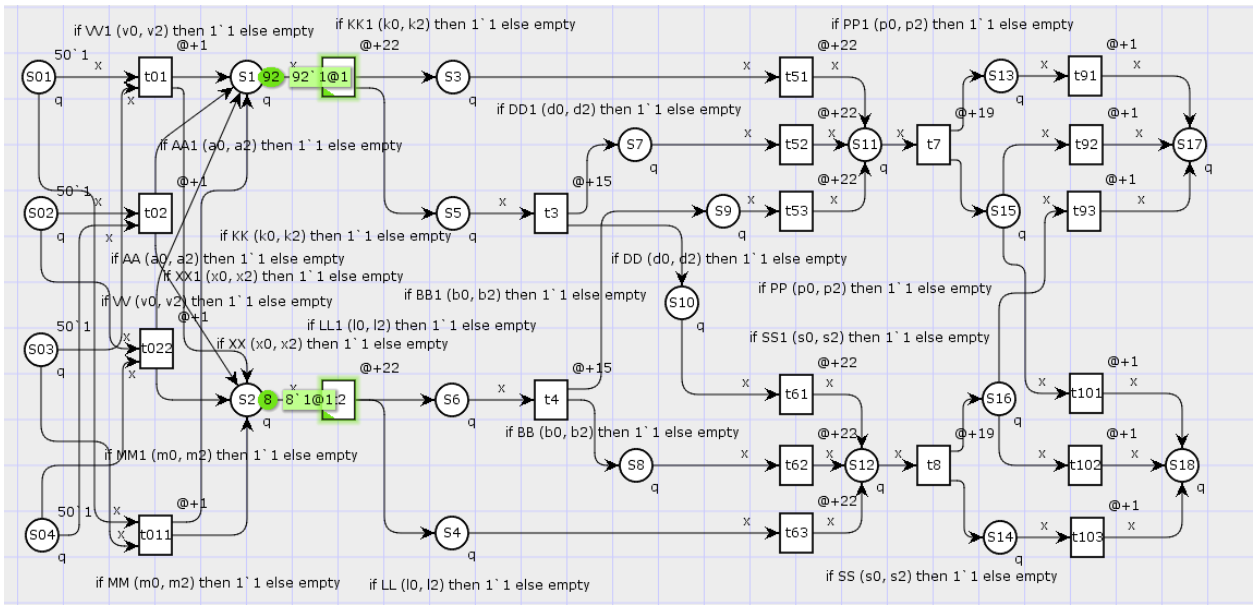


Рис. 5. Прогон модели для определения количества фишек в состояниях s_1 и s_2
(Fig. 5. Run the model to determine the number of chips in states s_1 and s_2)

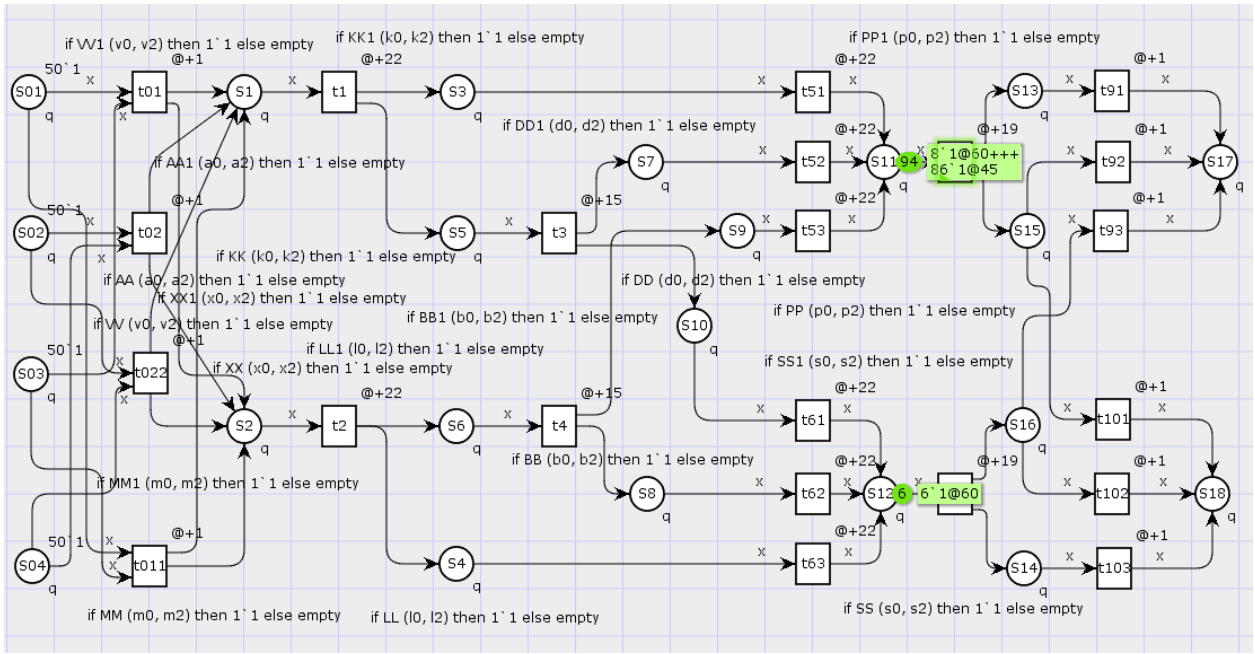


Рис. 6. Прогон модели для определения количества фишек в состояниях s_{11} и s_{12}
(Fig. 6. Run the model to determine the number of chips in states s_{11} and s_{12})

Соответственно, необходимое количество прогонов $N_{s_1t_{01}}$, $N_{s_1t_{02}}$, $N_{s_{11}t_5}$, $N_{s_{17}t_9}$ для данных состояний будет следующим:

$$N_{s_1t_{01}} = \frac{0.46(1-0.46)}{0.01^2} \cdot 2.58^2 = 16534.4976 \approx 16534,$$

$$N_{s_1t_{02}} = \frac{0.46(1-0.46)}{0.01^2} \cdot 2.58^2 = 16534.4976 \approx 16534,$$

$$N_{s_{11}t_5} = \frac{0.94(1-0.94)}{0.01^2} \cdot 2.58^2 = 3754.2096 \approx 3754,$$

$$N_{s_{17}t_9} = \frac{0.99(1-0.99)}{0.01^2} \cdot 2.58^2 = 658.9836 \approx 659.$$

Для определения необходимого количества прогонов по сети выберем максимальное из рассчитанных значений $N \approx 16534$ (рис. 8).

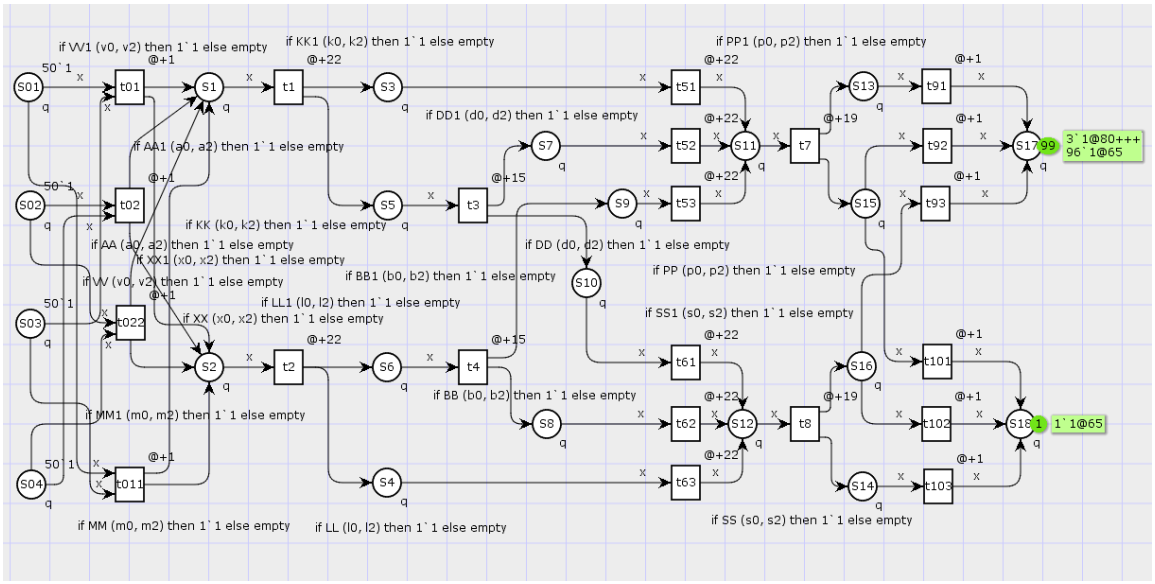


Рис. 7. Прогон модели для определения количества фишек в состояниях s_{17} и s_{18}
(Fig. 7. Run the model to determine the number of chips in states s_{17} and s_{18})

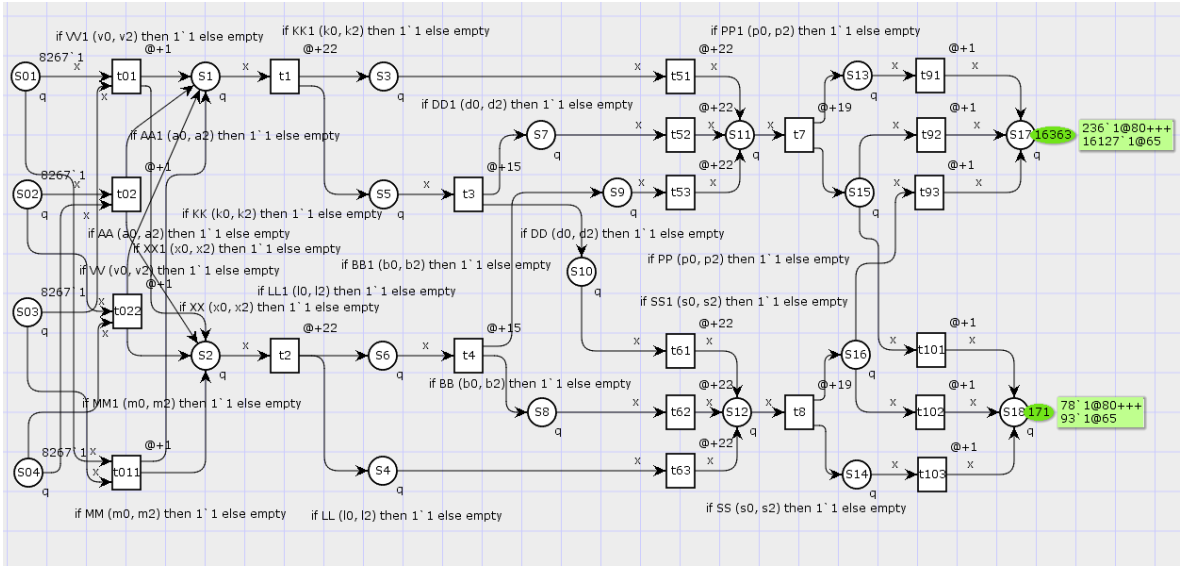


Рис. 8. Имитационная модель информационного конфликта «Сетевая атака – СЗИ от НСД» с необходимым количеством прогонов
(Fig. 8. Simulation model of information conflict "Network attack – SPI from NSD" with the required number of runs)

Поскольку время в «CPN Tools» представляется в виде целого числа, то для получения временной статистики процесса реализации сетевой атаки устанавливается следующая взаимосвязь между модельным (машинным) и реальным временем: 1 ед. = 1 с.

Временная статистика попадания маркера во все позиции представляется в виде табл. 1, имеющей следующие поля: Name – имя позиции; Count – счетчик проходов по графу, начиная с 0; Sum – суммарное количество попаданий маркера в конкретную позицию, Avrg – среднее количество попаданий маркера в позицию; Max – максимальное количество попаданий маркера в позицию; Time Avrg – среднее время нахождения маркера в одном из состояний графовой модели, формально описывающей реализацию сетевой атаки в АС в динамике ее конфликтного взаимодействия с СЗИ от НСД (количественное значение ВВХ сетевой атаки).

Результаты имитационного моделирования (временная статистика) процесса реализации сетевой атаки на информационный ресурс АС в виде количественных значений ее ВВХ представлены в табл. 1.

Таблица 1. Временная статистика процесса реализации сетевой атаки в динамике конфликтного взаимодействия с СЗИ от НСД

Name	Count	Sum	Avrg	Max	Time Avrg
Marking_size_Network_attack'S01_1	8269	0	0.000000	8267	0
Marking_size_Network_attack'S02_1	8269	0	0.000000	8267	0
Marking_size_Network_attack'S03_1	8269	0	0.000000	8267	0
Marking_size_Network_attack'S04_1	8269	0	0.000000	8267	0
Marking_size_Network_attack'S1_1	32885	6805530	206.949367	16349	1
Marking_size_Network_attack'S2_1	16721	39157	2.341772	185	1
Marking_size_Network_attack'S3_1	32561	146986124	4514.177215	16210	22
Marking_size_Network_attack'S4_1	188	52	0.278481	1	22
Marking_size_Network_attack'S5_1	16490	638309	38.708861	139	22
Marking_size_Network_attack'S6_1	371	19010	51.240506	184	22
Marking_size_Network_attack'S7_1	278	7231	26.012658	137	15
Marking_size_Network_attack'S8_1	368	12717	34.556962	182	15
Marking_size_Network_attack'S9_1	188	71	0.379747	2	15
Marking_size_Network_attack'S10_1	143	54	0.379747	2	15
Marking_size_Network_attack'S11_1	32700	148879375	4552.886076	16349	22
Marking_size_Network_attack'S12_1	372	19165	51.518987	185	22
Marking_size_Network_attack'S13_1	32537	126661187	3892.835443	16186	19
Marking_size_Network_attack'S14_1	189	91	0.481013	2	19
Marking_size_Network_attack'S15_1	16514	647391	39.202532	163	19
Marking_size_Network_attack'S16_1	370	16285	44.012658	183	19
Marking_size_Network_attack'S17_1	16358	50089645	3062.088608	16356	1
Marking_size_Network_attack'S18_1	180	2871	15.949367	178	1

Полученные значения ВВХ сетевой атаки в виде времен выполнения ею вредоносных функций (средних времен переходов по СПМ, моделирующей информационный конфликт «Сетевая атака – СЗИ от НСД») могут служить исходными данными для расчета вероятностей и оценивания опасности реализации сетевых атак в защищенных АС ОВД на основе разработки аналитической модели, учитывая особенности и реально существующие недостатки эксплуатации защищенных АС на объектах информатизации ОВД, рассмотренные в [3].

В [2] определены и проанализированы наиболее опасные и часто реализуемые в настоящее время (типовые) сетевые атаки, воздействующие на информационный ресурс защищенных АС ОВД. Среднее время реализации каждой атаки, смоделированной в «CPN Tools» (среднее время перемещения по СПМ из начальной позиции до конечного перехода), рассчитанное по методике, изложенной в [12, 16], приведено в табл. 2.

Таблица 2. Среднее время реализации типовых сетевых атак на информационный ресурс защищенных АС ОВД

№ п/п	Название атаки	Среднее время реализации атаки, с
1	Анализ сетевого трафика (сниффинг пакетов)	24
2	Сканирование сети	19
3	Парольная атака	512
4	Подмена доверенного объекта сети (IP-spoofing)	48
5	Навязывание ложного маршрута	107
6	Внедрение ложного объекта сети (ARP-spoofing)	37
7	Отказ в обслуживании (SYN-flood)	17
8	Удаленный запуск приложений (IP-hijacking)	58

Зная количественные значения ВВХ сетевой атаки в процессе ее конфликтного взаимодействия с СЗИ от НСД, среднее время реализации каждой из указанных атак, а также задавая математические ожидания и средние квадратичные отклонения объемов памяти и производительностей конфликтующих систем, можно не только наблюдать протекание информационного конфликта в его динамике, но также рассчитать вероятности реализации типовых сетевых атак и провести количественную оценку опасности их реализации в защищенных АС ОВД. Полученные результаты могут быть использованы при обосновании количественных требований к СЗИ от НСД с целью повышения реальной защищенности АС при их разработке и эксплуатации на объектах информатизации ОВД.

Заключение

Таким образом, на основе вербальной модели процесса функционирования СЗИ от НСД, в условиях реализации сетевых атак на информационный ресурс защищенных АС ОВД, в статье представлена обобщенная формальная модель функционирования дестабилизирующего воздействия в динамике конфликтного взаимодействия с системой защиты, построенная с использованием СПМ.

На основе обобщенной формальной модели разработана имитационная модель, описывающая механизм информационного конфликта «Сетевая атака – СЗИ от НСД», и проведено имитационное моделирование, используя программную среду «CPN Tools».

По результатам имитационного моделирования, представленным в виде временной статистики процесса реализации сетевой атаки в динамике информационного конфликта с СЗИ от НСД, определены количественные значения ее ВВХ.

Представлены средние времена реализации типовых сетевых атак, воздействующих на информационный ресурс защищенных АС ОВД, полученные путем моделирования данных атак с помощью СПМ в программной среде «CPN Tools».

Полученные значения ВВХ сетевой атаки в виде времен выполнения ею вредоносных функций позволят рассчитать вероятности и провести количественную оценку опасности реализации сетевых атак на этапах всего жизненного цикла функционирования защищенных АС ОВД в соответствии с характеристиками типовых сетевых атак, воздействующих на их информационный ресурс, и типовых систем защиты, используемых в АС ОВД. Данные результаты являются актуальными при обосновании количественных требований к перспективным СЗИ от НСД в процессе разработки АС и их эксплуатации в защищенном исполнении на объектах информатизации ОВД.

СПИСОК ЛИТЕРАТУРЫ:

1. Язов Ю.К. Организация защиты информации в информационных системах от несанкционированного доступа: монография / Ю.К. Язов, С.В. Соловьев. Воронеж: Кварта, 2018. – 588 с.
2. Дровникова И.Г. Анализ типовых сетевых атак на автоматизированные системы органов внутренних дел / И.Г. Дровникова, Е.С. Овчинникова, В.В. Конобеевских // Вестник Дагестан. гос. технич. ун-та. Технич. науки. 2020. Т. 47. № 1(2020). С. 72–85. DOI: https://doi.org/10.21822/2073-6185-2020-47-1-72-85.
3. Дровникова, Ирина Г., Овчинникова, Елена С., Рогозин, Евгений А. Формирование основных показателей опасности сетевых атак в автоматизированных системах органов внутренних дел. Безопасность информационных технологий, [S.l.]. Т. 27, № 3. С. 6–17, сен. 2020. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1288 (дата обращения: 26.11.2020). DOI: http://dx.doi.org/10.26583/bit.2020.3.01.
4. Oliver M. Technological determinism in educational technology research: some alternative ways of thinking about the relationship between learning and technology M. Oliver. Journal of Computer Assisted Learning. 2011. 27(5). P. 373–384. DOI: http://dx.doi.org/10.1111/j.1365-2729.2011.00406.
5. Rebovich G. Enterprise Systems Engineering: Advances in the Theory and Practice G. Rebovich, B. White. Boca Raton: CRC Press, 2011. – 459 p.
6. Djordjevic Nebojsa D. Software quality standards // Vojnoteh. glas. 2017. № 65(1). P. 102–104. URL: https://cyberleninka.ru/article/n/software-quality-standards (дата обращения: 26.11.2020).
7. Дровникова И.Г. Анализ существующих способов и процедур оценки опасности реализации сетевых атак в автоматизированных системах органов внутренних дел и аспекты их совершенствования / И.Г. Дровникова, Е.С. Овчинникова, Е.А. Рогозин // Вестник Воронеж. ин-та МВД России. 2019. № 4. С. 51–63. URL: https://elibrary.ru/item.asp?id=41568748 (дата обращения: 26.11.2020).
8. Акиншин Руслан Н., Ивутин Алексей Н., Есиков Дмитрий О., Страхов Илья А. Применение математического аппарата сетей Петри-Маркова для определения временных и вероятностных характеристик системы управления высоконагруженными веб-порталами с повышенной отказоустойчивостью // Научный вестник МГТУ ГА. 2014. №210 (12). С. 87–90. URL: https://cyberleninka.ru/article/n/primenenie-matematicheskogo-apparata-setey-petri-markova-dlya-opredeleniya-vremennyh-i-veroyatnostnyh-harakteristik-sistemy (дата обращения: 26.11.2020).
9. Моделирование марковских случайных процессов. URL: http://stratum.ac.ru/education/textbooks/modelir/lection33.html (дата обращения: 26.11.2020).
10. Сети Петри. Структура и правила выполнения сетей Петри. URL: https://bit.ly/2TcBs6B (дата обращения: 26.11.2020).
11. Синегубов С.В. Моделирование систем и сетей телекоммуникаций / С.В. Синегубов. – Воронеж: Воронеж. ин-т МВД России, 2016. – 336 с.
12. Романников Д.О. Об использовании программного пакета CPN TOOLS для анализа сетей Петри / Д.О. Романников, А.В. Марков // сб. науч. тр. НГТУ. 2012. № 2(68). С. 105–116. URL: https://elibrary.ru/item.asp?id=22560427 (дата обращения: 26.11.2020).
13. Радько Н.М. Проникновения в операционную среду компьютера: модели злоумышленного удаленного доступа / Н.М. Радько, Ю.К. Язов, Н.Н. Корнеева. Воронеж: Воронеж. госуд. технич. ун-т, 2013. – 265 с.
14. Радько Н.М. Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа / Н.М. Радько, И.О. Скобелев. М.: РадиоСофт, 2010. – 232 с.
15. Дровникова И.Г. К вопросу моделирования процесса функционирования системы защиты информации в условиях реализации сетевых атак на объектах информатизации органов внутренних дел / И.Г. Дровникова, Е.С. Овчинникова // Общественная безопасность, законность и правопорядок в III тысячелетии: матер. междунар. науч.-практич. конф. Ч. 2. Воронеж: ВИ МВД России, 2020. С. 218–225.
16. Дровникова И.Г. Моделирование динамики информационного конфликта в защищенных автоматизированных системах органов внутренних дел на основе сети Петри-Маркова / И.Г. Дровникова, Е.С. Овчинникова, Е.А. Рогозин // Вестник Воронеж. ин-та ФСИН России. 2020. № 4. С. 51–66.
17. Bokova O.I., Drovnikova I.G., Ovchinnikova E.S. and Rodin S.V. Innovative technology for studying the dynamics of network attacks on information resources of the educational environment. ASEDU-2020: 1st International Conference on Advances in Science, Engineering and Digital Education. IOP Conf. Series: Journal of Physics: Conf. Series 1691 (2020) 012063 IOP Publishing. DOI: http://dx.doi.org/10.1088/1742-6596/1691/1/012063.

REFERENCES:

[1] Yazov Yu.K. Organization of information protection in information systems from unauthorized access: monograph Yu.K. Yazov, S.V. Solovyov. Voronezh: Kvarta, 2018. – 588 p. (in Russian).

[2] Drovnikova I.G. Analysis of typical network attacks on automated systems of internal Affairs bodies I.G. Drovnikova, E.S. Ovchinnikova, V.V. Konobeevskikh. Bulletin of Dagestan state technical University. Technical Sciences. 2020. Vol. 47. no. 1(2020). P. 72–85. DOI: https://doi.org/10.21822/2073-6185-2020-47-1-72-85 (in Russian).

[3] Drovnikova, Irina G., Ovchinnikova, Elena S., Rogozin, Evgeni A. Network attacks main danger indicators formation in Internal Affairs Bodies automated systems. IT Security (Russia), [S.l.]. V. 27, no. 3. P. 6–17, sep. 2020. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1288 (accessed: 26.11.2020). DOI: http://dx.doi.org/10.26583/bit.2020.3.01 (in Russian).

[4] Oliver M. Technological determinism in educational technology research: some alternative ways of thinking about the relationship between learning and technology M. Oliver. Journal of Computer Assisted Learning. 2011. 27(5): P. 373–384. DOI: http://dx.doi.org/10.1111/j.1365-2729.2011.00406.

[5] Rebovich G. Enterprise Systems Engineering: Advances in the Theory and Practice G. Rebovich, B. White. Boca Raton: CRC Press, 2011. – 459 p.

[6] Djordjevic Nebojsa D. Software quality standards. Vojnoteh. glas. 2017. no. 65(1). P. 102–104. URL: https://cyberleninka.ru/article/n/software-quality-standards (accessed: 26.11.2020).

[7] Drovnikova I.G. Analysis of existing methods and procedures for assessing the risk of network attacks in automated systems of internal Affairs bodies and aspects of their improvement I.G. Drovnikova, E.S. Ovchinnikova, E.A. Rogozin. Vestnik Voronezh. in-t of the Ministry of internal Affairs of Russia. 2019. № 4. P. 51–63. URL: https://elibrary.ru/item.asp?id=41568748 (accessed: 26.11.2020) (in Russian).

[8] Akinshin Ruslan N. et. al. Application of the mathematical apparatus of Petri-Markov networks to determine the time and probability characteristics of the management system for high-load web portals with increased fault tolerance. R.N. Scientific Bulletin of MSTU GA. 2014. no. 210. P. 87–90. URL: https://cyberleninka.ru/article/n/primenenie-matematicheskogo-apparata-setey-petri-markova-dlya-opredeleniya-vremennyh-i-veroyatnostnyh-harakteristik-sistemy (accessed: 26.11.2020) (in Russian).

[9] Modeling of Markov random processes. URL: http://stratum.ac.ru/education/textbooks/modelir/lection33.html (accessed: 26.11.2020) (in Russian).

[10] Petri Nets. Structure and rules for performing Petri nets. URL: https://bit.ly/2TcBs6B (accessed: 26.11.2020) (in Russian).

[11] Sinegubov S.V. Modeling of telecommunication systems and networks S.V. Sinegubov. Voronezh: Voronezh. in-t of the Ministry of internal Affairs of Russia, 2016. – 336 p. (in Russian).

[12] Romannikov D.O. About using the CPN TOOLS software package for Petri net analysis D.O. Romannikov, A.V. Markov. SB. nauch. Tr. NSTU. 2012. no. 2(68). P. 105–116. URL: https://elibrary.ru/item.asp?id=22560427 (accessed: 26.11.2020) (in Russian).

[13] Radko N.M. Penetration into the computer operating environment: models of malicious remote access N.M. Radko, Yu.K. Yazov, N.N. Korneeva. Voronezh: Voronezh state technical University, 2013. – 265 p. (in Russian).

[14] Radko N.M. Risk models of information and telecommunication systems in the implementation of threats of remote and direct access N.M. Radko, I.O. Skobelev. M: Radiosoft, 2010. – 232 p. (in Russian).

[15] Drovnikova I.G. On the issue of modeling the process of functioning of the information protection system in the conditions of implementation of network attacks on the objects of informatization of internal affairs bodies. I.G. Drovnikova, E.S. Ovchinnikova. Public safety, law and order in the third millennium: mater. International Scientific and Practical Conference Part 2. Voronezh: Voronezh. in-t of the Ministry of Internal Affairs of Russia, 2020. P. 218–225 (in Russian).

[16] Drovnikova I.G. Modeling of information conflict dynamics in protected automated systems of internal affairs bodies based on the Petri-Markov network I.G. Drovnikova, E.S. Ovchinnikova, E.A. Rogozin. Vestnik Voronezh. in-ta of the Federal Penitentiary Service of Russia. 2020. no. 4. P. 51–66 (in Russian).

[17] Bokova O.I., Drovnikova I.G., Ovchinnikova E.S. and Rodin S.V. Innovative technology for studying the dynamics of network attacks on information resources of the educational environment. ASEDU-2020: 1st International Conference on Advances in Science, Engineering and Digital Education. IOP Conf. Series: Journal of Physics: Conf. Series 1691 (2020) 012063 IOP Publishing. DOI: http://dx.doi.org/10.1088/1742-6596/1691/1/012063.

Поступила в редакцию – 23 ноября 2020 г. Окончательный вариант – 15 января 2021 г.
Received – November 23, 2020. The final version – January 15, 2021.

Дмитрий П. Зегжда[1], Игорь Ю. Жуков[2]
[1]Санкт-Петербургский политехнический университет Петра Великого,
Политехническая ул., 29, Санкт-Петербург, 195251, Россия
[2]АО «РАМЭК-ВС»,
Волгоградский пр–т, 2, Москва, 109316, Россия
[1]e-mail: dmitry@ibks.spbstu.ru, https://orcid.org/0000-0002-0232-7248
[2]e-mail: i.zhukov@inbox.ru, https://orcid.org/0000-0002-4429-8799

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ

DOI: http://dx.doi.org/10.26583/bit.2021.1.04

Аннотация. Цель статьи – комплексный анализ вопросов технологической независимости и информационной безопасности вычислительных систем. Применение системного подхода предполагает анализ технологий защиты на всех уровнях архитектуры и их взаимодействие между собой. Рассматриваются аппаратные технологии защиты на уровне процессора и системы команд. Аппаратная поддержка виртуализации, которая обеспечивает поддержку со стороны аппаратного обеспечения такой функции как виртуализация операционных систем, становится необходимой функцией защиты и не уступает в важности уже классическим функциям: управление доступом, идентификация, аутентификация, аудит и контроль безопасности. Помимо аппаратной поддержки виртуализации рассмотрены реализации в современных процессорах группы технологий аппаратной поддержки обособленной доверенной среды. Проведен анализ возможности использования аппаратных технологий защиты злоумышленниками для вредоносных воздействий. По результатам исследований предложен подход по созданию отечественной защищенной архитектуры средств вычислительной техники (СВТ) с использованием зарубежных аппаратных технологий защиты. При этом импортозамещение не должно сводиться исключительно к репликации зарубежных решений, т.к. зарубежные СВТ содержат массу недокументированных возможностей и, как следствие, несут угрозу информационной безопасности.

Ключевые слова: архитектура вычислительных систем, аппаратные технологии защиты, виртуализация, вредоносные воздействия, технологическая независимость, импортозамещение.
Для цитирования: ЗЕГЖДА, Дмитрий П.; ЖУКОВ, Игорь Ю. ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ. Безопасность информационных технологий, [S.l.], v. 28, n. 1, p. 42–61, jan. 2021. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1320>. Дата доступа: 01 feb. 2021. DOI: http://dx.doi.org/10.26583/bit.2021.1.04.

Dmitry P. Zegzhda[1], Igor Y. Zhukov[2]
[1]Peter the Great St. Petersburg Polytechnic University,
29 Politechnicheskaya str., Saint Petersburg, 195251, Russia
[2]JSC «RAMEC VS»,
Volgogradskiy Prospekt, 2, Moscow, 109316, Russia
[1]e-mail: i.zhukov@inbox.ru, https://orcid.org/0000-0002-4429-8799
[2]e-mail: dmitry@ibks.spbstu.ru, https://orcid.org/0000-0002-0232-7248

Features of information security of computer systems

DOI: http://dx.doi.org/10.26583/bit.2021.1.04

Abstract. Presented is a comprehensive analysis of the issues of technological independence and information security of the computing system. The systematic approach involves the analysis of protection technologies at all levels of architecture and its interaction with each other. Hardware protection technologies at the processor and command system level are considered. Hardware support for virtualization turns out to be a necessary security function and is not less important than the already traditional security functions like an access control, identification, authentication, audit and security

control. In addition to hardware support for virtualization we discuss the implementation of the group of technologies for hardware support for a separate trusted environment in modern processors. The analysis of the possibility of using hardware protection technologies by intruders for malicious influences is carried out. Based on the research results, an approach to create a domestic protected architecture of computer equipment using foreign hardware protection technologies is proposed. At the same time, import substitution should not be limited solely to the replication of foreign solutions, since foreign computer equipments contain a lot of undocumented capabilities and, as a result, pose a threat to information security.

Keywords: computer system architecture, hardware protection technologies, virtualization, malicious impacts, technological independence, import substitution.

For citation: ZEGZHDA, Dmitry P.; ZHUKOV, Igor Y. Features of information security of computer systems. IT Security (Russia), [S.l.], v. 28, n. 1, p. 42–61, jan. 2021. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1320>. Date accessed: 01 feb. 2021. DOI: http://dx.doi.org/10.26583/bit.2021.1.04.

Введение

За последние несколько лет мощное развитие получили современные технологии аппаратной защиты [1–6]. Эти технологии являются предметом гордости любой IT-компании. В рамках статьи аппаратные технологии защиты распределим по десяти группам:

– поддержка привилегированного режима и контроль обращения к адресным пространствам;
– защита от угроз со стороны аппаратных устройств;
– аппаратная поддержка независимого контроля целостности системы в процессе загрузки;
– аппаратная поддержка виртуализации;
– аппаратная поддержка обособленной доверенной среды;
– противодействие эксплуатации уязвимостей;
– реализация криптографических примитивов и защищенное хранилище ключей;
– аппаратная идентификация и биометрическая аутентификация пользователей;
– защита от аппаратных сбоев;
– автономный чип контроля управления системой.

Каждая группа технологий содержит сразу несколько решений, однако все они стремятся решить одну из задач обеспечения безопасности системы.

Поддержка привилегированного режима и контроль обращения к адресным пространствам является базовой технологией, которой оснащены практически все современные микропроцессоры.

В первую очередь, она формирует минимально необходимые два режима процессора: разделение ПО на системное – работающее в привилегированном режиме и прикладное – работающее в «пользовательском» режиме процессора.

Вторая технология из этой группы – это реализация базового контроля обращения к изолированным адресным пространствам. Функция изоляции обеспечивает возможность локализации ошибок в рамках одного прикладного процесса, не нарушая работы всей системы. Кроме того, она создает в системе базовые сущности, которые могут быть аутентифицированы субъектами, без которых невозможно обеспечить контроль обращения.

В рамках «защищенного режима» реализуется технология виртуальной памяти, которая сразу решает несколько задач: изоляция каждого процесса в системе друг от друга в отдельном адресном пространстве и обеспечение для каждого процесса одинакового

адресного пространства вне зависимости от реального объема оперативной памяти. Эта технология реализуется в рамках модуля управления памятью (memory management unit – MMU), который является частью практически любого современного микропроцессора.

Вторая группа технологий **защита от угроз со стороны аппаратных устройств** – это технологии, обеспечивающие функции контроля обращения внешних (по отношению к центральному процессору) устройств к аппаратным ресурсам: оперативной памяти и другим устройствам.

Современные устройства научились работать друг с другом, с центральным процессором и памятью на огромных скоростях, в основном, за счет появления технологии DMA (direct memory access). Эта технология фактически разрешила доступ устройств к оперативной памяти без участия центрального процессора. В этой связи процессор стал всего лишь одним из потребителей оперативной памяти [6].

Основная угроза со стороны аппаратных устройств – внедрение вредоносного ПО в их программные прошивки.

Хорошим примером такого устройства является современный видео-адаптер, который не только обладает мощным вычислителем с сотнями процессорных ядер, собственной оперативной памятью (видео-память), но и обладает сложным программным обеспечением и даже реализует функции виртуальной памяти. Таким образом, разграничение обращения внешних устройств к оперативной памяти и их взаимная изоляция являются актуальными задачами [7].

Аппаратно-программные модули доверенной загрузки (АПМДЗ) широко применяются на отечественном рынке. Цель этих систем – обеспечение целостности конфигурации системы путем поэтапной проверки целостности состава аппаратного и программного обеспечения в течении всей процедуры загрузки. Результатом является уверенность пользователей системы в том, что в систему не был внедрен вредоносный код и не была нарушена целостность с момента предыдущего запуска. Это крайне необходимо для обеспечения безопасности работы любой информационной системы.

Суть традиционных АПМДЗ заключается в статическом контроле целостности, когда проверки осуществляются строго последовательно: каждый очередной загружаемый компонент сначала проверяется системой контроля целостности, а только затем (после успешного прохождения проверки) компонент выполняется.

Если в таком способе нарушить цепочку и пропустить хотя-бы один компонент, то это будет серьезным нарушением безопасности, которым сможет воспользоваться нарушитель. Для доверенного запуска системы контроль целостности нужно осуществлять для каждого компонента, в том числе и для тех, которые являются лишь промежуточными и не требуются для долговременной работы пользователей. При этом традиционная технология уже используется на отечественном рынке и в своем составе использует сертифицированные алгоритмы.

Однако, компаниями Intel и AMD [8, 9] была разработана интересная технология динамического контроля целостности. Суть динамического контроля целостности заключается в том, что на начальных этапах запуска системы контроль целостности не осуществляется вовсе. Затем, перед самым запуском ядра ОС (доверенным компонентом всей основной системы, с которой будут работать пользователи) выполняется контроль целостности конфигурации системы атомарным образом – за одну инструкцию (например, в технологии Intel TXT это инструкция GETSEC[ENTER]). Получается, что технология встроена в сам процессор. Однако помимо процессора она задействует возможности чипсета и внешних устройств защиты. За эту инструкцию процессор самостоятельно проверяет, что работает только одно ядро, в строго определенном режиме, что отключены

прерывания, что вся система настроена правильно (таким образом, что ни одно устройство или код не может нарушить или прервать ход дальнейшей проверки), а затем в соответствии с настроенной политикой безопасности процессор выполняет контроль целостности ПО и конфигурации системы. Все выполняется безусловно и атомарно, что обеспечивает надежный механизм контроля целостности. Кроме того, эту инструкцию можно вызвать в любой момент времени, в том числе и повторно.

К сожалению, технологии динамического контроля целостности не используют отечественные криптографические алгоритмы и не могут иметь широкого применения на отечественном рынке. Эти функции требуют реализации в составе процессоров, что конечно, соответствует требованиям нормативных документов с точки зрения цели, но не соответствует этим документам с точки зрения используемых методов алгоритма контроля. Тем не менее, ни что не мешает заменить алгоритмы и получить все преимущества этой мощной технологии.

Очень важная технология **Аппаратная поддержка виртуализации** – которая обеспечивает поддержку со стороны аппаратного обеспечения такой функции как виртуализация операционных систем. Можно утверждать, что виртуализация становится необходимой функцией защиты и не уступает в важности уже классическим функциям: управление доступом, идентификация, аутентификация, аудит и контроль безопасности. Такое значение функции виртуализации операционных систем придает то, что это единственная функция, которая способна обеспечить и гарантировать изоляцию нескольких вычислительных сред друг от друга.

Фактически виртуализация расщепляет аппаратную платформу на несколько программных платформ (виртуальных машин). Важно, что именно такие программные платформы включают в себя полноценную операционную систему со всем многообразием прикладных и системных программных средств, размещенных внутри контролируемой гипервизором виртуальной машине.

На практике такой эффект достигается тем, что в процессоре появляется две группы режимов: режимы монитора виртуальных машин (root или хост) и режимы виртуальных машин (non-root или гость). Кроме того, помимо традиционного MMU вводится дополнительный уровень контроля и виртуализации оперативной памяти.

Понятия гипервизора (его еще называют монитором виртуальных машин) и виртуальной машины были введены еще в 70-х годах прошлого века. Однако за счет возникновения аппаратной поддержки виртуализации и развития облачных систем эти понятия широко используются в IT-индустрии в настоящее время.

В настоящее время обеспечение изоляции вычислительных сред – это очень актуальная задача. Все чаще приходится использовать информационные системы, состоящие из нескольких операционных систем, где часть из них доверенные, другие не являются доверенными. Важно, что пользователям необходимо использовать возможности каждой из частей. Объединять доверенные и не доверенные части вместе в рамках одной операционной системы – невозможно! Только функция виртуализации может обеспечить их гарантированную изоляцию [8, 9].

Поскольку функция виртуализации операционных систем крайне важна для обеспечения безопасности, то ее аппаратная поддержка является краеугольным камнем многих современных средств защиты. На самом деле известно, что гипервизор можно реализовать без аппаратных технологий. Вопрос в том, насколько это будет эффективно и насколько это будет гарантированно с точки зрения надежности работы.

Помимо функции изоляции виртуализация операционных систем способна обеспечить еще целый ряд полезных функций, которые не менее важны с точки зрения безопасности:

– контроль за всеми программными средствами, в том числе ядрами операционных систем, в виртуальной машине;

– управление потоками ввода-вывода между операционной системой и внешними устройствами;

– обеспечение защищенного обмена данными между виртуальными машинами;

– контроль вложенных гипервизоров и виртуальных машин.

Фактически гипервизор может управлять поведением и даже предотвращать нежелательное поведение тех средств, которые не являются доверенными. Последняя функция крайне интересна, поскольку функция виртуализации может использоваться рекурсивно: гипервизор позволяет запускать в виртуальной машине другие гипервизоры. Такой гипервизор будет называться вложенным, как и его виртуальные машины. В этом случае, вложенный гипервизор уже не будет привилегированным, и будет действовать принцип первичности: первый, запущенный на ПЭВМ гипервизор будет привилегированным, а все остальные вложенные гипервизоры будут подчиненными.

Помимо аппаратной поддержки виртуализации в современных процессорах реализована еще одна группа технологий **аппаратной поддержки обособленной доверенной среды**.

Проблема доверия характерна не только для нашей страны. Она на самом деле имеет глобальный характер. Даже такие крупные компании, как Intel и Microsoft, все равно идут к тому, чтобы создать в рамках общего вычислительного пространства некую среду с повышенным уровнем доверия [10–12]. Такая изолированная доверенная среда необходима для обработки ключей и прочей чувствительной конфиденциальной информации. Для этого работа полноценной операционной системы не требуется, поэтому функция виртуализации также не требуется, в группу аппаратной поддержки обособленной доверенной среды входят следующие технологии:

– размещение привилегированного кода в защищенной области памяти;

– разделение вычислительной среды на доверенную и не доверенную;

– обязательная проверка подписи для доверенного кода.

Для решения указанной задачи получили широкое развитие соответствующие технологии, которые обеспечивают в первую очередь целостность и подлинность доверенной среды [13–15]. Кроме того, они ограничивают взаимодействие между доверенной средой и остальной частью системы. Фактически это традиционная защита, только реализованная прямо в рамках архитектуры аппаратного обеспечения.

В рамках этой группы следует выделить несколько любопытных технологий и описать их более подробно.

Во-первых, следует указать технологию ARM TrustZone [12], которая позволяет разделять код, данные и внешние устройства на два домена (доверенный и не доверенный). При этом на аппаратном уровне не только контролируется целостность доверенного домена, но и запрещен доступ внешним устройствам к данным доверенного домена.

Во-вторых, технология SMM (System Management Mode). Дело в том, что технология SMM известна уже давно. Изначально она решала ряд далеких от безопасности специфических задач. Как указано в официальной документации, в настоящее время SMM – это самый привилегированный режим работы процессора. Код в

этом режиме изолирован от всего остального кода и к нему запрещен доступ со стороны аппаратных устройств. Де-факто SMM формирует полноценную изолированную среду.

В-третьих, следует обратить внимание на самую «свежую» технологию – Intel SGX (Safer Guard Extension). Эта технология любопытна тем, что она, в отличие от других, обеспечивает создание изолированной вычислительной среды в рамках непривилегированного прикладного процесса операционной системы. В классической архитектуре информационных систем, чем привилегированнее компонент, тем он более защищён и тем больше к нему доверие. Технология Intel SGX поступает наоборот: она позволяет создать так называемый анклав (защищенную область кода и данных) в рамках непривилегированного прикладного процесса. При этом доступ к нему запрещен аппаратно со стороны других процессов, ядра операционной системы, гипервизора и любых внешних устройств. Такой любопытный результат достигается благодаря тому, что весь код и данные в рамках анклава хранится в общей оперативной памяти в зашифрованном виде. Такой мощный ход был реализован благодаря тому, что современные процессоры Intel [16] прямо в кристалле реализуют множество криптографических функций. В результате данные анклава в открытом виде существуют только глубоко в ядре процессора. Кроме того, технология обеспечивает аппаратный контроль целостности кода, попадающего в анклав за счет аппаратной проверки подписи перед запуском этого кода.

Противодействие эксплуатации уязвимостей. С точки зрения практики, защищенная система это та, в которой отсутствуют уязвимости. Можно определить уязвимость как специфический вид ошибки, который позволяет нарушить безопасность системы. В любой программе есть ошибки, однако не любая ошибка является уязвимостью. Не все ошибки позволяют осуществить атаку и тем более обеспечить нарушителю возможность проникнуть в систему [17].

Кроме того, есть такое понятие, как уязвимость нулевого дня. Это такая уязвимость, про которую никто в системе не знает, поэтому ни одна система защиты противостоять не может. Как следствие, эта уязвимость остается доступной для нарушителя [18].

Поэтому разработчики операционных систем и разработчики процессоров ввели меры для противодействия уязвимостям, что фактически сформировало второй эшелон защиты. Другими словами, если в первом эшелоне (в стандартных средствах контроля обращения во всех доверенных загрузчиках, гипервизорах и прочем) существует уязвимость, которую нарушитель нашел и воспользовался ею, то, благодаря второму эшелону, ему создается ряд препятствий, которые придется также преодолеть.

Типизация памяти (type enforcement): процессору указывается, где код, где стек, где данные, что выполнять можно, что модифицировать нельзя, и т. д. Кроме того, целая группа технологий препятствует передаче управления из кода на одном уровне привилегий в код на другом уровне привилегий:

- контроль выполнения, чтения, записи для виртуальных адресных пространств;
- управление типами кэширования для областей памяти;
- управление границами сегментов и типизация памяти;
- запрет обращения к непривилегированному коду из привилегированного режима.

Все перечисленное – это достаточно эффективные функции. Они реально работают на практике и обеспечивают тот самый второй эшелон защиты. Сама архитектура современных операционных систем, зачастую, препятствует применению этих технологий, поскольку некоторые системные элементы современных ОС в своем

поведении очень похожи на эксплуатацию уязвимости. Например, антивирусы или средства виртуализации часто используют такие приемы, которые облегчают разработку ПО и повышают производительность, но при этом они отходят от требований безопасности и нарушают правила, делая свое поведение похожим на уязвимость. Именно поэтому указанные технологии защиты, к сожалению, применить на все 100% не представляется возможным, хотя нарушителям создаются дополнительные препятствия.

Однако необходимость наличия технологий защиты от эксплуатации уязвимостей потребовала что-то менять. В результате необходимые функции были добавлены в модель виртуальной страничной памяти (что является частью MMU – memory management unit). Такой подход позволил разработчикам размечать код, стек, данные и иные сегменты памяти как им удобно. При этом с точностью до страницы (4 Кб) указываются атрибуты обращения: для заданной области памяти: чтение, модификация, выполнение, область системная или прикладная. Такой подход оказался простым и удобным, что способствовало его внедрению во все современные ОС.

Важной функцией защиты является **криптография**. Для современных систем необходима полноценная реализация криптографических функций, которая не только обеспечивает приемлемую производительность, но и защиту ключевой информации. Рассмотрим несколько таких технологий подробнее.

Во-первых, для решения задач ускорения криптографических функций, что крайне необходимо для современных систем, обычно используют ПЛИС системы. Однако на современных процессорах эту задачу решают путем добавления новых инструкций: например Intel AES-NI и MIPS OmniShield. Указанные технологии реализуют западные криптографические алгоритмы, которые уже встроены в процессор. Однако Intel уже давно анонсировала технологию Intel Xeon FPGA, которая должна позволить разработчикам ПО добавлять в процессор свои инструкции для реализации криптографических примитивов, которые необходимы пользователям.

Во-вторых, следует отметить популярную технологию TPM (trusted platform module), которая представляет собой изолированный чип, основная задача которого обеспечить защищенное хранилище ключей. Это достигается путем того, что сам чип хранит в себе уникальный ключ, который никогда не покидает кристалл и защищен физически от всевозможных рентгеновских сканеров и иных средств чип-реверсинга (реверс-дизайна). В самом чипе реализуется множество криптографических функций (более 20-ти) которые могут использовать тот самый внутренний ключ.

Другой важной функцией, которая важна с точки зрения архитектуры системы является **биометрическая аутентификация**. Необходимость аутентификации возникает постоянно, а пользователи не могут создать такое количество ключей и паролей, а главное их запомнить. В результате создается огромный риск утечки и компрометации этих самых ключей. Биометрическая аутентификация очень легка с точки зрения использования и минимизирует эту угрозу. Поэтому поддержка такой аутентификации тоже встраивается во многие современные вычислительные системы и тоже является элементом архитектуры.

Ошибки в программных средствах могут приводить к уязвимостям и атакам на системы, а ошибки в аппаратном обеспечении и природные воздействия на него, могут приводить к потере данных и отказу в обслуживании. Поэтому современная архитектура тоже оснащается средствами защиты от аппаратных сбоев, которые позволяют преодолеть такие проблемы.

Другими словами, помимо ошибок, допущенных разработчиками, на нарушение целостности данных могут влиять и внешние факторы. Поэтому для защиты от подобных

нарушений в современные системы был внедрен целый ряд технологий для защиты от аппаратных сбоев. Эти технологии внедряются практически на каждом аппаратном компоненте современных ПЭВМ. Для пользователей и программистов они являются прозрачными.

Что такое доверие – достаточно сложный вопрос. Понятно, что доверие имеет некую иерархическую природу: когда одни компоненты зависят от других. Например, операционная система контролирует приложения. Соответственно, приложение доверяет операционной системе. При этом гипервизор контролирует операционную систему и операционная система доверяет гипервизору. Процессор контролирует операционную систему и гипервизор. Следовательно, гипервизор и операционная система доверяют процессору.

Что контролирует процессор? Раньше внешние устройства на материнской плате не имели в своем составе функций контроля и были достаточно простыми. Однако со временем на материнской плате современных ПЭВМ появился чип, реализующий функции независимого контроля и управления системой. Это чипсет, который часто называют «южный мост». Мотивацией к такому развитию послужила необходимость реализации удаленной диагностики, управления и восстановления систем после сбоев. Эта необходимость появилась из-за того, что современным системным администраторам требуется обслуживать большое количество компьютеров одновременно. Это касается не только огромных дата-центров с облачными системами, но и обычного корпоративного сегмента, где работают стандартные конфигурации ПЭВМ. В результате, практически все современные компьютеры на рынке обладают таким независимым автономным чипом контроля (рис. 1).

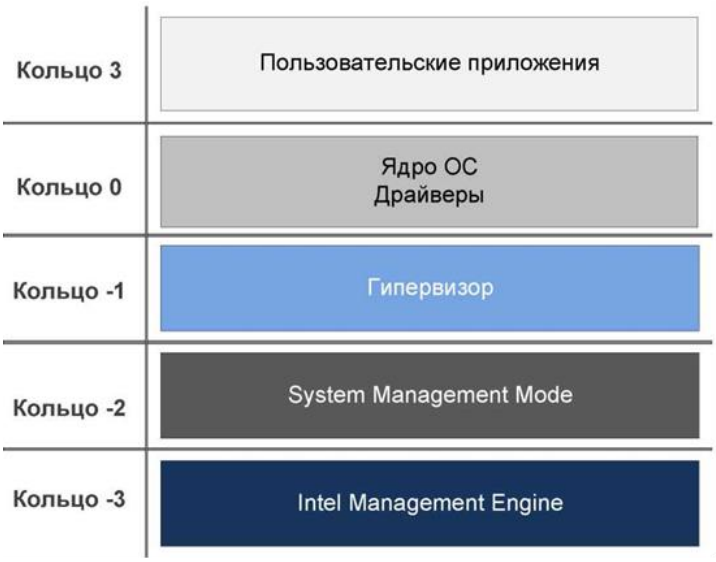


Рис 1. Новый уровень контроля и управления в системе – «чипсет»
Fig. 1. A new level of control and management in the system – «chipset»

Удаленный контроль и диагностика не единственная технология, реализуемая на этом чипе. В частности, автономный чип управления играет роль в реализации функций защиты ноутбуков от кражи, а также функции защиты авторского контента (так называемый DRM – digital rights management). При краже этот чип может самостоятельно удалить все конфиденциальные данные с компьютера, или сообщить через сайт пользователю о своем местоположении.

Фактически автономный чип управления является компьютером в компьютере. Он обладает доступом к оперативной памяти, системам управления питанием, возможностью фильтровать сетевой траффик, осуществлять активное независимое взаимодействие по сети (например, в рамках технологии Intel AMT реализуется полноценный веб-сервер), имеет доступ к видео-карте. Описание технологий защиты, которые реализуются с участием этого чипа, говорят о том, что все эти возможности чипу действительно необходимы. Однако, достаточно очевидно, что в этом чипе функций безопасности на самом деле гораздо больше. Это связано с тем, что вырабатывается определенный уровень доверия к приложению, операционной системе и процессору, но на самом деле доверять необходимо этому автономному чипу – «южному мосту», поскольку все остальное функционирование системы зависит от него. К сожалению, вопрос доверия к этому чипу становится особенно непростым из-за практически полного отсутствия документации на него.

В результате исследования составлена табл. 1, в которой представлены все рассмотренные технологии и их наличие в различных современных процессорах.

Таблица 1. Распространенность аппаратных технологий защиты среди современных микропроцессоров

	Intel x86, (Skylake)	ARM Cortex-A, Байкал-M	AMD Bulldozer	MIPS Varrior Байкал-T1	VIA Nano	PowerPC	Эльбрус	Соболь	TPM	Intel 100 series	КРИПТОН-ЗАМОК
Защита от угроз со стороны аппаратных устройств	да		да					да		да	
Аппаратная поддержка независимого контроля целостности системы в процессе загрузки	да	да	да					да	да		да
Аппаратная поддержка виртуализации	да	да	да	да	да	да					
Аппаратная поддержка обособленной доверенной среды	да	да	да	да			да				
Противодействие эксплуатации уязвимостей	да	да	да	да	да	да	да				
Реализация криптографических примитивов и защищенное хранилище ключей	да	да	да		да			да	да		да
Аппаратная идентификация и биометрическая аутентификация пользователей								да			да
Автономный чип контроля и управления системой	да		да							да	
Защита от аппаратных сбоев	да	да	да	да	да	да	да	?		да	?

Из табл. 1 следует, что очевидным лидером по количеству реализованных технологий защиты являются процессоры Intel. Этот вывод достаточно понятен, поскольку Intel является на текущий момент лидером на рынке микропроцессоров.

Эта компания производит полный спектр микропроцессоров, материнских плат, графических и сетевых адаптеров, чипсетов и других устройств. При этом, микропроцессоры Intel представлены во всех видах современных средств вычислительной техники: от контроллеров умных домов (Intel Edison) и мобильных телефонов до суперкомпьютеров.

Такая популярность процессоров Intel и архитектуры x86 неразрывно связана с двумя важными аспектами.

Во-первых, популярность провоцирует большое внимание к себе, что на практике делает проблему безопасности наиболее актуальной именно для этой платформы. Пока не было массовых компьютеров, проблема безопасности информации не стояла так остро. Но за счет широкой распространенности неквалифицированные пользователи и потребители соприкоснулись с этой техникой. При этом, возникла проблема безопасности, поскольку безопасность без человека существует. В результате такой популярности, именно от процессоров Intel стало требоваться как можно больше возможностей по защите, поскольку для них и реализуется больше всего угроз.

Во-вторых, жизнь и развитие технологий сказываются так, что при выборе той или иной архитектуры, того или иного процессора, решающий вклад имеет фактор наличия большого количества ПО для этой платформы, и, соответственно, количество разработчиков и пользователей, обученных этому программному обеспечению. За счет такого «рычага» Intel интенсивно внедряет свои технологии во все остальные сегменты. В результате все самые мощные суперкомпьютеры построены на архитектуре Intel, потому что пользователи хотят использовать популярное программное обеспечение, которое уже разработано для архитектуры x86.

1. Технологии защиты средств вычислительной техники

Широкая доступность ПК с архитектурой x86 и систем разработки ПО для них обусловило распространение этой архитектуры во все классы СВТ [3].

Современные персональные компьютеры (ПК) не только набрали огромную популярность и получили широкую распространенность, но и приобрели весь возможный спектр функциональных возможностей: они участвуют в сетевом взаимодействии, могут быть мощными вычислительными средствами, могут использовать различные датчики, управлять простыми механизмами, взаимодействовать с радиоканалами WiFi/GSM, запускать виртуальные машины, осуществлять перенаправление сетевого траффика и предоставлять различные сетевые сервисы другим пользователям, и еще многое другое.

Т.о. персональные компьютеры – это универсальное средство СВТ. С развитием современных технологий стало ясно, что уход от универсальности в сторону специализации устройств позволяет добиться лучших результатов и получить больше преимуществ. Можно выделить два основных направления развития персональных компьютеров, что привело к появлению новых видов СВТ (рис. 2).

Во-первых, развитие ПК в сторону увеличения вычислительной мощности и параллельности привело к появлению суперкомпьютеров. Кроме того, объединение множества компьютеров в вычислительную сеть привело к появлению интернет-серверов и облачных систем.

Во-вторых, уменьшение энергопотребления и облегчение функций современных процессоров привело к появлению мобильных устройств. Как развитие этого направления, появились киберфизические системы, в которых компьютерная техника выступает в роли маломощных, но «умных» датчиков. Кроме того, снижение энергопотребления и

фокусирование вычислительной техники на одной задаче привело к появлению такого вида СВТ как телекоммуникационное оборудование.

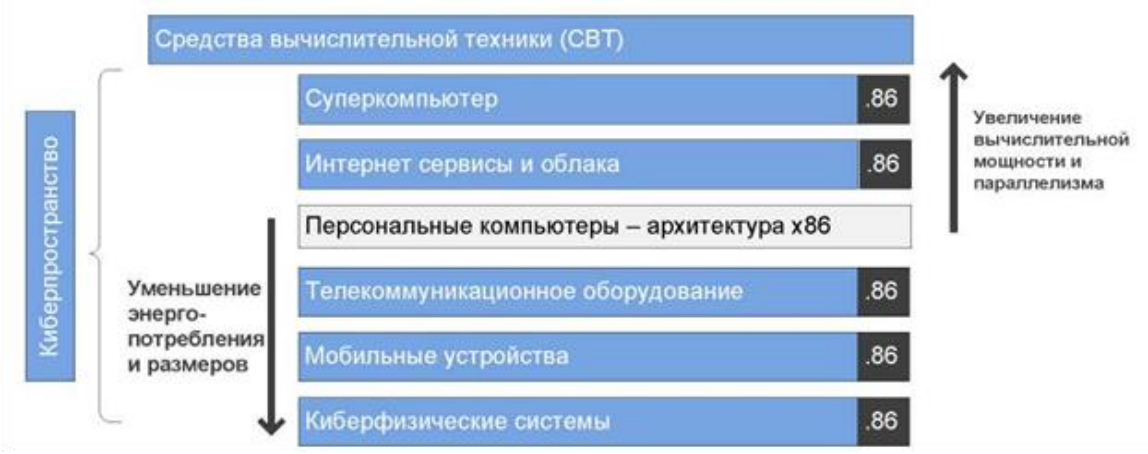


Рис. 2. Появление различных видов СВТ из ПК
Fig. 2. The emergence of various types of Computer Equipment from Personal Computers

Выделенные аппаратные технологии защиты эффективно используются при построении одной из самых распространенных инфраструктур в мире компании Apple, использующей технологии защиты на уровне процессора, СВТ (компьютера и/или мобильного устройства), операционных систем (iMAC и iOS), а также облачной системы (AppStor, iTune).

2. Угрозы аппаратных технологий защиты

Однако, некоторые технологии защиты, которые имеют аппаратную поддержку, могут быть использованы не только для решения задач защиты, но и могут быть использованы злоумышленниками для повышения качества своих средств атаки и нападения. Такими обоюдоострыми свойствами обладают две из рассмотренных аппаратных технологий защиты:

- аппаратная поддержка виртуализации;
- автономный чип контроля и управления системой.

Рассмотрим, как эти аппаратные технологии могут использоваться вредоносным программным обеспечением (ВПО). ВПО может использовать аппаратную технологию виртуализации для захвата управления системой без нарушения ее работы. Кроме того, ВПО может использовать эту технологию для скрытия своего присутствия и своей активности. Это происходит благодаря тому, что средства управления (гипервизор) фактически являются отдельным объектом атаки. При этом атака направляется туда, где нет средств защиты. Это не учитывать совершенно невозможно. Практика показывает, что уже известны такие атаки со стороны аппаратного обеспечения и со стороны программного обеспечения, которые сильно завязаны на аппаратные технологии

Наиболее известна атака, под названием Blue Pill (рис. 3), которая была продемонстрирована Иоанной Рутковской в 2006 г. в рамках конференции Black Hat. Продемонстрированная атака приводит к тому, что программное средство Blue Pill из программы Windows становится гипервизором. Гипервизор создает виртуальную машину и переносит в нее ОС, после чего начинает контролировать ее поведение, скрывая свое присутствие. Фактически нарушитель создает виртуальную ОС, реализует свои средства в

гипервизоре вне этой самой ОС. При этом злоумышленник становится совершенно прозрачен и невидим для средств защиты. Средства защиты функционируют в рамках операционной системы и играют по ее правилам, которые теперь свободно может менять нарушитель. В результате такую атаку не обнаруживают ни антивирусы, ни любые другие используемые средства защиты. Важно подчеркнуть, что это происходит не потому, что средства защиты плохо работают, а потому что они принципиально обнаружить такое воздействие на систему не могут, поскольку они живут внутри этой самой виртуальной машины, которую организовал злоумышленник. Раз такой практический эксперимент был продемонстрирован, то это реальность, а не теория.

Рис. 3. Использование виртуализации в эксперименте Blue Pill
Fig. 3. Using virtualization in the Blue Pill experiment

Другая группа аппаратных технологий защиты, которую может использовать ВПО – это автономный чип контроля и управления системой. Для наглядности эта группа технологий будет рассматриваться на примере Intel ME (Management Engine), она же Intel AMT (Active Management Technology) и Intel vPro. Эта технология фактически реализует автономную операционную систему на базе чипсета (второй по важности аппаратный чип в компьютере после процессора). В результате чипсет становится даже более привлекательной целью, чем основной процессор и ОС потому, что попав в операционную среду Intel ME можно выполнять все те действия, которые хочет выполнять обычно нарушитель. При этом злоумышленник остается абсолютно невидимым и недосягаемым для средств защиты, запущенных на центральном процессоре, так как реализация этих функций осуществляются вне ОС, в которой он работает.

Изначально технология Intel ME предназначена для того, чтобы управлять самим процессором и другими аппаратными средствами компьютера. Кроме того, на базе технологии Intel ME был реализован целый калейдоскоп различных технологий, который позволяют удаленно диагностировать состояние компьютера в дата-центрах, позволяют выключать и стирать удаленно конфиденциальные данные, загружаться с виртуальных DVD дисков, удаленно устанавливать операционные системы, скрывать доступ к заданным областям экрана для защиты видео материалов от копирования, осуществлять фильтрацию сетевых пакетов, скрывать активную работу с сетью, в том числе через WiFi. По мнению экспертов, в этой технологии кроется самая серьезная угроза. Вот известный список возможностей, которые получает нарушитель, в случае успешного перехвата управления над Intel ME:

- контроль СВТ на любой стадии загрузки ОС;
- манипулирование системным окружением СВТ;
- манипулирование аппаратными технологиями защиты;

– наличие собственного DMA-контроллера с обходом MMU;
– максимальная изоляция исполняемого кода ME/AMT от ОС;
– постоянное функционирование на дежурном питании;
– доступ к OnBoard-устройствам (GPU, USB/Ethernet/WiFi/NFC);
– удаленное управление СВТ (централизованные/децентрализованные схемы);
– прослушивание сетевого трафика / сбор парольно-адресной информации;
– возможность перенаправления/модификации/зеркалирования сетевого трафика;
– организация p2p-сети для выхода за периметр ЛВС;
– мониторинг активности пользователя;
– подмена изображения на экране;
– сбор информации со всех подключаемых устройствах (флэш-накопители /телефоны/токены/датчики);
– взаимодействие с API ОС для сбора пользовательской информации (адресная книга телефона/медиа-контент/данные токенов).

Как же противодействовать тому, что нарушитель может использовать такие опасные возможности архитектуры, как аппаратная технология виртуализации и автономный чип контроля и управления системой? Во-первых, возникает искушение от этих технологий просто отказаться: раз этими средствами может воспользоваться нарушитель, то это следует просто вырезать и убрать из системы.

По мнению экспертов, это неправильный подход потому, что это шаг назад. Ведь, если от них отказаться, то пользователи и разработчики, а не только злоумышленники, не смогут их использовать для полезных целей. Действительно, технология виртуализации и Intel ME предоставляют прекрасные и полезные возможности, которые повышают эффективность и позволяют решать более сложные задачи. Самый простой пример, без этих технологий современный дата-центр не построить. Без виртуализации экономические затраты будут слишком большие и ресурсы будут простаивать, а без технологии подобной Intel ME не обеспечить администрирование такого центра и не осуществить своевременное выявление аппаратных сбоев, которые в таких масштабах не редкость. На самом деле, отказываться от этих технологий нет необходимости. Эта проблема безопасности информации имеет решение.

Рассмотрим аппаратную поддержку виртуализации: чем можно нейтрализовать ее использование со стороны нарушителя? Во-первых, эффективно работает аппаратная технология независимого контроля целостности в процессе загрузки. Эта технология гарантирует, что гипервизор нельзя встроить в установленную на ПК прошивку. Во-вторых, тот же самый чип контроля и управления системой (даже Intel ME) следует использовать для того, чтобы предотвратить захват гипервизора нарушителем или установку гипервизора (такого как Blue Pill) в систему. Следовательно, на самом деле эти технологии образуют некую иерархию (рис. 4).

Иерархия характеризуется последовательностью контроля: более приоритетная с аппаратной точки зрения технология может контролировать другую технологию, в основе иерархии находится автономный чип контроля и управления системой, потому что он лежит на самом низком уровне системы – это даже не процессор с его режимами, а отдельный чип. Очевидно, что, если нарушитель хочет преодолеть защиту и, если он не может преодолеть ее «в лоб», то он должен «пролезть» под ней, на более низком уровне, что в частности было с успехом продемонстрировано Ионной Рутковской не только в 2006 г., но и в 2009 г., когда она успешно внедрила свой код в Intel ME.

Получается, чтобы обеспечить безопасность, следует обеспечить доверие к тому компоненту, который располагается на самом низком уровне иерархии. В результате, этот

компонент обладает самым высоким уровнем управления и контроля, и является, таким образом, корнем доверия.

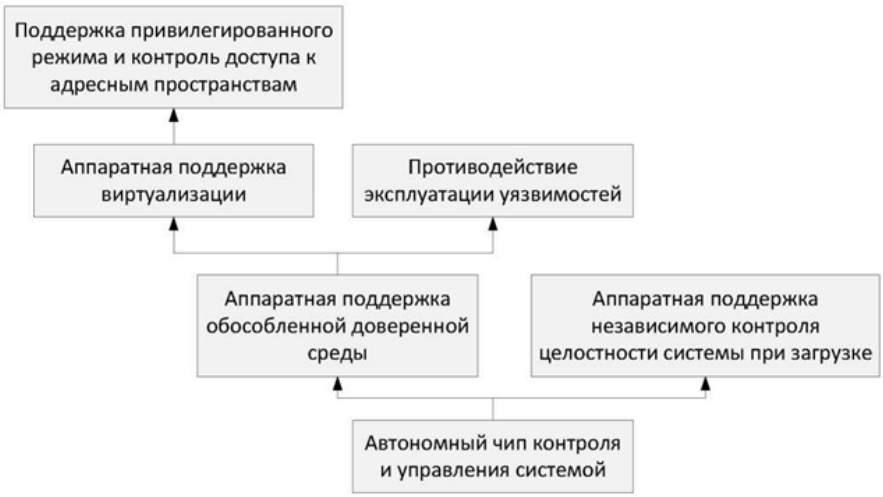


Рис. 4. Иерархическая зависимость технологий
Fig. 4. Hierarchical dependence of technologies

Раньше считалось, что таким компонентом является ядро процессора. Однако в настоящее время стало понятно, что этот компонент извлечен из процессора. По мнению экспертов, такая интерпретация понятия «доверие» и есть то, к чему должно сводиться импортозамещение. Импортозамещение не должно повторять то, ЧТО уже есть на рынке. Необходимо сосредоточиться на том компоненте системы, который будет контролировать все элементы СВТ. Вместе с этим, следует учитывать научно-технический задел, чтобы обеспечить более высокий уровень доверия ко всей системе.

Архитектура отечественного СВТ должна включать автономное средство защиты, полностью контролирующее функционирование информационной системы, обеспечивающее доверие и безопасность [19].

3. Архитектура защищенных СВТ

При рассмотрении задачи построения современных СВТ с использованием зарубежных технологий следует отметить еще несколько важных моментов.

Во-первых, импортозамещение не должно сводиться исключительно к репликации зарубежных решений. Вместо этого следует создавать и совершенствовать отечественные технологии. Это позволит обеспечить стимулирование отечественного производства и развитие научных и проектно-конструкторских исследований и разработок.

Во-вторых, на этом пути возникает указанная ранее проблема: зарубежные СВТ содержат массу недокументированных возможностей (НДВ) и как следствие несут угрозу информационной безопасности. При этом проведение достоверного анализа на НДВ для высокотехнологичных СВТ на практике невозможно. Тем не менее, также невозможно полностью отказаться от совместимости отечественных СВТ с зарубежным программным и аппаратным обеспечением. Решение проблемы заключается в том, что архитектура отечественного СВТ должна включать автономное аппаратное средство защиты, полностью контролирующее функционирование информационной системы, обеспечивающее доверие и безопасность.

В-третьих, необходимым условием внедрения этого решения будет востребованность конечными пользователями, причем не только государственными и корпоративными, но и массовыми.

В-четвертых, для того, чтобы некоторое аппаратное или программно-аппаратное средство могло быть использовано в государственном секторе, оно должно быть безопасно, что гарантируется исполнением процедуры сертификации. Эта процедура подтверждает обеспечение целого ряда требований, указанных в законодательстве. При этом существующие отечественные защищенные аппаратные средства обладают рядом недостатков, в сравнении с зарубежными аналогами:

– неполная совместимость с современной массовой аппаратурой. В результате необходима постоянная адаптация к новым устройствам, многообразие которых порождает уникальные требования к каждому из них;

– ограниченная совместимость с приложениями, вызванная необходимостью фиксации версий ПО и прошивок, и отсутствие определенной функциональности, что является следствием выполнения требований по безопасности в рамках процедуры сертификации;

– ограничения на внешнюю среду. После сертификации гарантии безопасности сохраняются только при работе в доверенном окружении. При этом отсутствуют какие-либо гарантии при взаимодействии средства с непроверенным окружением;

– сама по себе необходимость проведения процедуры сертификации фактически означает недоверие к средствам защиты, поскольку ее действенность признается только при работе с ограниченным набором сертифицированных решений.

Следовательно, необходимо разработать архитектуру современного отечественного СВТ, которая учитывает все указанные факторы и, по возможности, лишена указанных недостатков. Для защиты программного обеспечения предлагается использовать так называемую интеграционную парадигму, которая базируется на четырех постулатах:

– контроль всех без исключения взаимодействий в системе;

– инвариантность средств защиты по отношению к приложениям и ресурсам;

– контроль информационных взаимодействий на основе четко определенных правил, составляющих формальную модель;

– оценка безопасности, как текущего состояния системы, так и прогнозирование безопасности будущих состояний.

Рассмотрим использование интеграционной парадигмы для защиты программного обеспечения в системах с архитектурой x86, и затем перейдем к защищенной архитектуре СВТ. Современным СВТ присущ иерархический контроль на аппаратном уровне. Для систем на базе x86 такая иерархия порождает иерархию компонентов программного обеспечения. Однако не все режимы находятся в иерархическом отношении. Некоторые из них находятся на одном уровне. Например, режим ядра может содержать несколько подрежимов в зависимости от разрядности исполняемого кода или используемых данных, что не порождает иерархии контроля. Все эти режимы обладают одинаковыми привилегиями. Тем не менее, сразу три группы аппаратных технологий защиты все-таки порождают иерархию контроля:

– поддержка привилегированного режима и контроль обращения к адресным пространствам;

– аппаратная поддержка виртуализации;

– аппаратная поддержка обособленной доверенной среды.

Основываясь на этих технологиях, применив интеграционную парадигму для защиты программного обеспечения в такой иерархической системе, эксперты пришли к выводу, что реализуя маленький, компактный и очень простой, однако при этом и очень эффективный гипервизор, который размещен на самом-самом низком уровне, в системе возникает возможность обеспечить и контроль, и безопасность для всех вложенных в него систем (рис. 5).

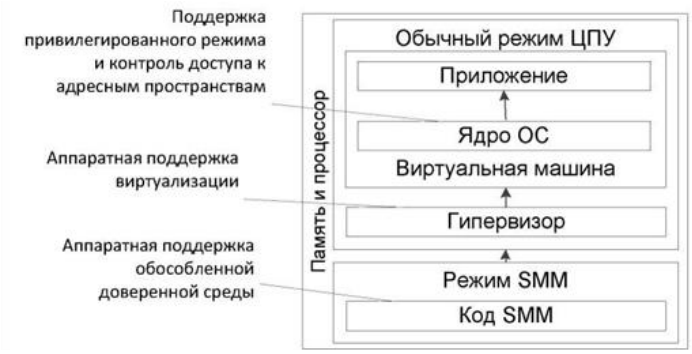


Рис. 5. Иерархия программного обеспечения в системах x86
Fig. 5. Software hierarchy in x86 systems

Такая архитектура еще называется «тонкий» гипервизор или гипервизор одной виртуальной машины. Этот гипервизор не обеспечивает планирования работы виртуальных машин – она у него одна и постоянно работает. Вместо этого он контролирует поведение всех программных компонентов в виртуальной машине, а также все взаимодействия и информационные потоки между программными компонентами в виртуальной машине и реальным аппаратным обеспечением. Предложенный подход был успешно реализован в виде опытного образца. В первых версиях разработанного опытного образца был просто гипервизор и операционная система, а в более новых редакциях за счет добавления поддержки режима SMM, сформирована более сложная конструкция.

Однако смысл от этого не изменился. Это принцип матрешки, когда одни компоненты вкладываются в другие. То, что находится снаружи, полностью контролирует и управляет теми компонентами, что находятся внутри. За счет такой архитектуры система защиты не дает нарушителям решить задачу кибератаки и захвата управления.

Основными преимуществами использования интеграционной парадигмы на примере гипервизора являются (рис. 6):

– управление безопасностью централизовано и сосредоточено в изолированном компоненте;

– возможность контролировать обмен виртуализованной системы с внешней средой с целью устранения скрытых каналов утечки информации;

– поведение виртуализованной системы тождественно поведению реальной системы и ПО работает без изменений;

– возможность имитации внешней среды для виртуализованной системы;

– объем кода гипервизора ничтожен по сравнению с ОС и приложениями;

– эксплуатация уязвимостей не приведет к компрометации изолированных средств защиты;

– сбои в виртуализованной системе могут быть оперативно нейтрализованы путем отката или сброса в исходное состояние.

По мнению экспертов, тот же самый подход применим и к аппаратному обеспечению. Стоит заметить, что Intel технологией ME делает, в какой-то степени, такой же шаг, вынося функции управления на внешний чипсет.

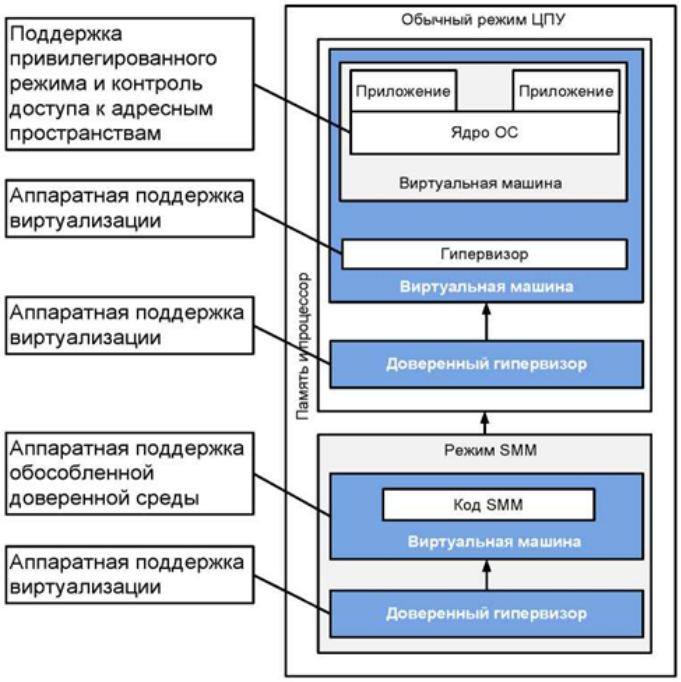


Рис. 6. Использование гипервизора как средства реализации интеграционной парадигмы
Fig. 6. Using the hypervisor as a means of implementing the integration paradigm

Интеграционную парадигму можно предложить для решения задачи построения защищенного средства СВТ (рис. 7).

По сути, предлагается разработать и создать еще один чип, контролирующий Intel ME (чипсет), контролирующий процессор, либо самим научиться контролировать поведение процессора с помощью каких-то своих чипсетов. Таким образом, будет повторяться та самая матрешка, которая и будет обеспечивать безопасность за счет того, что самый внешний слой (тот компонент системы, который контролирует все остальные) оказывается доверенным. По мнению экспертов, такой путь будет оптимальным решением рассматриваемой задачи достижения технологической независимости и цифрового суверенитета. Основными особенностями предлагаемого решения являются:

– последовательная реализация доверенных СВТ путем интеграции импортных и отечественных компонентов;

– контроль всех информационных потоков и взаимодействий со стороны отечественных доверенных средств на всех этапах интеграции;

– использование принципа матрешки – контроль вложенных компонентов и совместимость с внешними технологиями, процессорами и чипсетами;

– универсальный механизм подтверждения доверия с помощью отечественной криптографии;

– полное сохранение функциональных возможностей контролируемых систем.

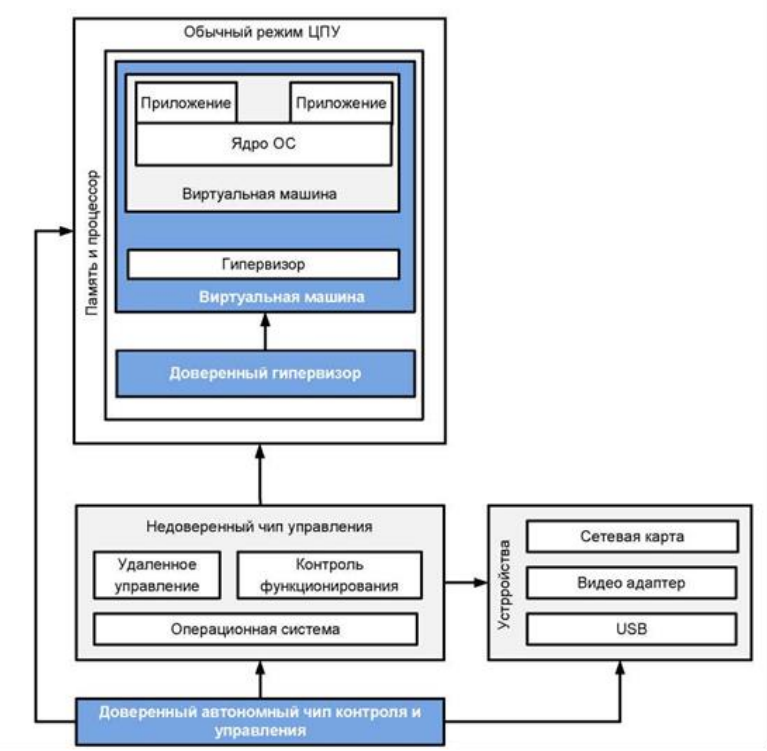


Рис. 7. Использование доверенного автономного чипа контроля и управления как средства реализации интеграционной парадигмы
Fig. 7. Using a trusted autonomous control and management chip as a means of implementing the integration paradigm

Заключение

При выборе технической и/или программной платформы, решая задачи обеспечения совместимости с имеющимся заделом разработанных и применяемых изделий, каждое ведомство планирует свое развитие на перспективу. При этом, целесообразно применять наиболее полный набор сертифицированных решений.

В условиях острого информационного противоборства отечественные разработки не должны сводиться исключительно к репликации зарубежных решений.

СПИСОК ЛИТЕРАТУРЫ:

1. Таненбаум Э., Остин Т. Архитектура компьютера. 6-е изд. – СПб.: Питер, 2019. – 816 с.
2. Intel® 64 and IA-32 Architecture Software Developer's Manual, Volume 1: Basic Architecture. URL: https://www.intel.com/content/www/us/en/architecture-and-technology/64-ia-32-architectures-software-developer-vol-1-manual.html (дата обращения: 01.12.2020).
3. Григорий Речистов. Десять имён для одной архитектуры. Блог компании Intel. 13 ноября 2013. URL: https://habrahabr.ru/company/intel/blog/201462/ (дата обращения: 01.12.2020).
4. Miles Murdocca, Vincent Heuring. Computer architecture and organization: an integrated approach / Miles J. Murdocca, Vincent P. Heuring. – Hoboken, N. J.: Wiley, cop. 2007. – 524 p. URL: https://www.researchandmarkets.com/reports/2239761/computer_architecture_and_organization_an (дата обращения: 01.12.2020).
5. Фаулер М. Архитектура корпоративных программных приложений. – М.: Издательский дом "Вильямс", 2006. – 544 с.
6. Rushby, John (1981). "Design and Verification of Secure Systems". 8th ACM Symposium on Operating System Principles. Pacific Grove, California, US. P. 12–21. DOI: https://doi.org/10.1145/800216.806586.

7. Alex Voica – New OmniShield platform implements multi-domain security for connected devices. URL: https://www.imgtec.com/blog/omnishield-multi-domain-security-connected-devices/ (дата обращения: 01.12.2020).
8. Intel® Virtualization Technology for Directed I/O, Architecture Specification, June 2016. URL: https://software.intel.com/sites/default/files/managed/c5/15/vt-directed-io-spec.pdf (дата обращения: 01.12.2020).
9. AMD I/O Virtualization Technology (IOMMU) Specification. URL: https://www.amd.com/system/files/TechDocs/48882_IOMMU_3.05_PUB.pdf (дата обращения: 01.12.2020).
10. Intel® Trusted Execution Technology: Software Development Guide URL: https://cs.technion.ac.il/~cs236376/readings/intel-txt-software-development-guide.pdf (дата обращения: 01.12.2020).
11. Дударев Д.А., Кравцов А.Ю., Полетаев В.М., Полтавцев А.В., Романец Ю.В., Сырчин В.К. Устройство создания доверенной среды для компьютеров специального назначения. Патент RU №2569577 C1. Заявка RU 2014132337/08, 06.08.2014. Опубликовано 27.11.2015. Бюл. №33. МПК G06F21/30, G06F21/50, G06F12/14.
12. ARM Security Technology, Building a Secure System using TrustZone® Technology. URL: https://static.docs.arm.com/genc009492/c/PRD29-GENC-009492C_trustzone_security_whitepaper.pdf (дата обращения: 01.12.2020).
13. Intel® Virtualization Technology Specification for the IA-32 Intel® Architecture URL: http://andrewl.dreamhosters.com/library/docs_intel/virtualization_Apr05.pdf (дата обращения: 01.12.2020).
14. Intel VMX technology, G. Lettieri, 28 Oct. 2015 URL: http://lettieri.iet.unipi.it/virtualization/2016/vn05.pdf (дата обращения: 01.12.2020).
15. AMD Secure Virtual Machine Architecture Reference Manual. URL: https://www.mimuw.edu.pl/~vincent/lecture6/sources/amd-pacifica-specification.pdf
16. Intel® 64 and IA-32 Architectures Software Developer's Manual Volume 3B: System Programming Guide, Part 2 URL: https://software.intel.com/content/www/us/en/develop/articles/intel-sdm.html (дата обращения: 01.12.2020).
17. Barabanov A.V., Markov A.S., Tsirlov V.L. Information Security Controls Against Cross-Site Request Forgery Attacks on Software Application of Automated Systems. Journal of Physics: Conference Series. 2018. V. 1015. P. 042034. DOI: https://doi.org/10.1088/1742-6596/1015/4/042034.
18. Barabanov A.V., Markov A.S., Tsirlov V.L. Statistics of Software Vulnerability Detection in Certification Testing. Journal of Physics: Conference Series. 2018. V. 1015. P. 042033. DOI: https://doi.org/10.1088/1742-6596/1015/4/042033.
19. Borzykh S., Markov A., Tsirlov V., Barabanov A. Detecting Code Security Breaches by Means of Dataflow Analysis. In CEUR Workshop Proceedings, 2017, Vol-2081. P. 15–20. URL: http://ceur-ws.org/Vol-2081/paper04.pdf (дата обращения: 01.12.2020).

REFERENCES:

[1] Andrew S. Tanenbaum, Todd Austin. Structured computer organization. 6 edition. – Saint Petersburg: Piter, 2019. – 816 p. (in Russian).
[2] Intel® 64 and IA-32 Architecture Software Developer's Manual, Volume 1: Basic Architecture. URL: https://www.intel.com/content/www/us/en/architecture-and-technology/64-ia-32-architectures-software-developer-vol-1-manual.html (accessed: 01.12.2020).
[3] Gregory Rechistov. Ten names for a single architecture. Intel's blog. November 13, 2013. URL: https://habrahabr.ru/company/intel/blog/201462/ (accessed: 01.12.2020).
[4] Miles J. Murdocca, Vincent P. Heuring. Computer architecture and organization: an integrated approach – Hoboken, N. J.: Wiley, cop. 2007. – 524 p. URL: https://www.researchandmarkets.com/reports/2239761/computer_architecture_and_organization_an (accessed: 01.12.2020)
[5] Fowler M. Architecture of corporate software applications M.: Williams Publishing House, 2006. – 544 p. (in Russian).
[6] Rushby, John (1981). "Design and Verification of Secure Systems". 8th ACM Symposium on Operating System Principles. Pacific Grove, California, US. P. 12–21. DOI: https://doi.org/10.1145/800216.806586

[7] Alex Voica – New OmniShield platform implements multi-domain security for connected devices. URL: https://www.imgtec.com/blog/omnishield-multi-domain-security-connected-devices/ (accessed: 01.12.2020).
[8] Intel® Virtualization Technology for Directed I/O, Architecture Specification, June 2016. URL: https://software.intel.com/sites/default/files/managed/c5/15/vt-directed-io-spec.pdf (accessed: 01.12.2020)
[9] AMD I/O Virtualization Technology (IOMMU) Specification. URL: https://www.amd.com/system/files/TechDocs/48882_IOMMU_3.05_PUB.pdf (accessed: 01.12.2020)
[10] Intel® Trusted Execution Technology: Software Development Guide. URL: https://cs.technion.ac.il/~cs236376/readings/intel-txt-software-development-guide.pdf (accessed: 01.12.2020).
[11] Dudarev D.A., Kravtsov A.Yu., Poletaev V.M., Poltavtsev A.V., Romanets Ju.V., Syrchin V.K. Device to create trusted execution environment for special-purpose computers. Patent RU 2569577 C1. Application RU 2014132337/08, 06.08.2014. Published 27.11.2015, bull. No. 33. IPC G06F21/30, G06F21/50, G06F12/14. (in Russian).
[12] ARM Security Technology, Building a Secure System using TrustZone® Technology. URL: https://static.docs.arm.com/genc009492/c/PRD29-GENC-009492C_trustzone_security_whitepaper.pdf (accessed: 01.12.2020).
[13] Intel® Virtualization Technology Specification for the IA-32 Intel® Architecture. URL: http://andrewl.dreamhosters.com/library/docs_intel/virtualization_Apr05.pdf (accessed: 01.12.2020).
[14] Intel VMX technology, G. Lettieri, 28 Oct. 2015 URL: http://lettieri.iet.unipi.it/virtualization/2016/vn05.pdf (accessed: 01.12.2020).
[15] AMD Secure Virtual Machine Architecture Reference Manual URL: https://www.mimuw.edu.pl/~vincent/lecture6/sources/amd-pacifica-specification.pdf (accessed: 01.12.2020).
[16] Intel® 64 and IA-32 Architectures Software Developer's Manual Volume 3B: System Programming Guide, Part 2. URL: https://software.intel.com/content/www/us/en/develop/articles/intel-sdm.html (accessed: 01.12.2020).
[17] Barabanov A.V., Markov A.S., Tsirlov V.L. Information Security Controls Against Cross-Site Request Forgery Attacks on Software Application of Automated Systems. Journal of Physics: Conference Series. 2018. V. 1015. P. 042034. DOI: https://doi.org/10.1088/1742-6596/1015/4/042034.
[18] Barabanov A.V., Markov A.S., Tsirlov V.L. Statistics of Software Vulnerability Detection in Certification Testing. Journal of Physics: Conference Series. 2018. V. 1015. P. 042033. DOI: https://doi.org/10.1088/1742-6596/1015/4/042033.
[19] Borzykh S., Markov A., Tsirlov V., Barabanov A. Detecting Code Security Breaches by Means of Dataflow Analysis. In CEUR Workshop Proceedings, 2017, Vol-2081. P. 15–20. URL: http://ceur-ws.org/Vol-2081/paper04.pdf (accessed: 01.12.2020).

Поступила в редакцию – 01 декабря 2020 г. Окончательный вариант – 14 января 2021 г.
Received – December 01, 2020. The final version – January 14, 2021.

Александр А. Бердюгин
Финансовый университет при Правительстве Российской Федерации
(Финансовый университет),
Щербаковская ул., 38, Москва, 105187, Россия
e-mail: brdgn@bk.ru, https://orcid.org/0000-0003-2301-1776

РЕИНЖИНИРИНГ БИЗНЕС-ПРОЦЕССОВ КОММЕРЧЕСКОГО БАНКА В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

DOI: http://dx.doi.org/10.26583/bit.2021.1.05

Аннотация. Актуальность темы статьи обусловлена отсутствием научно-практической проработки вопросов реорганизации труда в кредитно-финансовом учреждении с учетом развития технологий и киберпреступности. Объект исследования – деятельность кредитной организации. Предмет – реинжиниринг бизнес-процессов банка, являющийся альтернативой методикам «Шесть сигм» и «Кайдзен». Цель этих методик – повышение качества бизнес-процессов коммерческого банка и минимизация количества ошибок операционной деятельности. Проведенный обзор источников позволил определить требования к обеспечению кибербезопасности и повышению доверия клиентов к технологиям электронного банкинга. Проанализирована динамика развития стран мира по их готовности перехода к электронному правительству в зависимости от значения валового национального продукта на душу населения. В качестве ключевого показателя деятельности предприятия разработан метод оценки для вычисления размера штрафа киберпреступникам. Приведен пример количественной оценки штрафа. Анализируемый реинжиниринг бизнес-процесса коммерческого банка направлен на улучшение процесса работы клиента и сотрудника банка за компьютером. Исследована и обоснована необходимость внедрения метода скоростного набора текста (смежная с кибербезопасностью тема) в образовательную программу России. Результаты исследования могут использоваться для дальнейших практических разработок риск-менеджмента кредитных организаций, использующих технологии электронного банкинга.
Ключевые слова: реинжиниринг бизнес-процессов, технологии электронного банкинга, риск воздействия кибератак, информационная безопасность, метод скоростной печати.
Для цитирования: БЕРДЮГИН, Александр А. РЕИНЖИНИРИНГ БИЗНЕС-ПРОЦЕССОВ КОММЕРЧЕСКОГО БАНКА В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ. Безопасность информационных технологий, [S.l.], v. 28, n. 1, p. 62–73, jan. 2021. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1319>. Дата доступа: 03 feb. 2021. DOI: http://dx.doi.org/10.26583/bit.2021.1.05.

Alexander A. Berdyugin
Financial University under the Government of the Russian Federation (Financial University),
Scherbakovskaya str., 38, Moscow, 105187, Russia
e-mail: brdgn@bk.ru, https://orcid.org/0000-0003-2301-1776

Reengineering of business processes of a commercial bank in the information space

DOI: http://dx.doi.org/10.26583/bit.2021.1.05

Abstract. The need in this research arises since issues of labor reorganization in a financial institution has not been elaborated and studied scientifically and practically, considering development of technology and cybercrime. The article deals with reorganization of labor in a credit and financial institution. The object of research is the operations of a credit institution. The subject is reengineering of business processes of a Bank, which is an alternative to the “Six Sigma” and “Kaizen” methods. The purpose of these methods is to improve the quality of business processes of a commercial bank minimizing the number of operational errors. The review of sources made it possible to determine the requirements for ensuring cybersecurity and increasing customer confidence in electronic banking technologies. Development dynamics of the countries of the world according to their readiness of transition to e-government, depending on the value of the gross national product per capita, is analyzed. As a key performance indicator of the company, an

assessment method has been developed for calculate the amount of fine for cybercriminals. An example of a quantitative assessment of the penalty is given. The studied reengineering of the business process of a commercial bank is aimed at improving the process of work of the client and the bank employee at the computer. The necessity of introducing the method of high-speed typing (a topic related to cybersecurity) in the educational program of Russia is investigated and justified. The research results may be of further use for the development of risk management in credit institutions using electronic banking technologies.
Keywords: reengineering of business processes, electronic banking technologies, the risk of cyberattacks, information security, high-speed printing method.
For citation: BERDYUGIN, Alexander A. Reengineering of business processes of a commercial bank in the information space. IT Security (Russia), [S.l.], v. 28, n. 1, p. 62–73, jan. 2021. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1319>. Date accessed: 03 feb. 2021. DOI: http://dx.doi.org/10.26583/bit.2021.1.05.

Введение

Цифровая революция является эпохой в истории человечества, где все связаны друг с другом онлайн, все имеют доступ к цифровым финансовым услугам. Значительная часть IT-бюджета банка расходуется на техническое обслуживание, а не на инновации [1]. По прогнозам Международной корпорации данных (IDC), к 2020 г. на услуги, оборудование и программное обеспечение кибербезопасности будет затрачено до 101,6 млрд долл. Это на 38% больше, чем 73,7 млрд долл. в 2016 г. [2]. По другим данным, уже в 2019 г. мировой рынок информационной безопасности достиг 119,9 млрд долл[1].

В работе [3] считают, что сдерживает использование технологий электронного банкинга (ТЭБ) три аспекта:

1. Сомнения клиентов в возможностях и защищенности финансовых технологий по причине компьютерной преступности и низкой надежности аппаратно-программного обеспечения ТЭБ;
2. Низкие показатели качества обеспечения дистанционных банковских услуг и удобства программного продукта;
3. Недостаточный уровень финансовой и компьютерной грамотности клиента ТЭБ.

Необходимость улучшений по этим направлениям не утратила актуальности и в настоящее время. Однако, по мнению автора, нужна реконструкция бизнес-модели, чему посвящен реинжиниринг бизнес-процессов в сфере информационных технологий коммерческого банка.

1. Обзор материалов по теме исследования

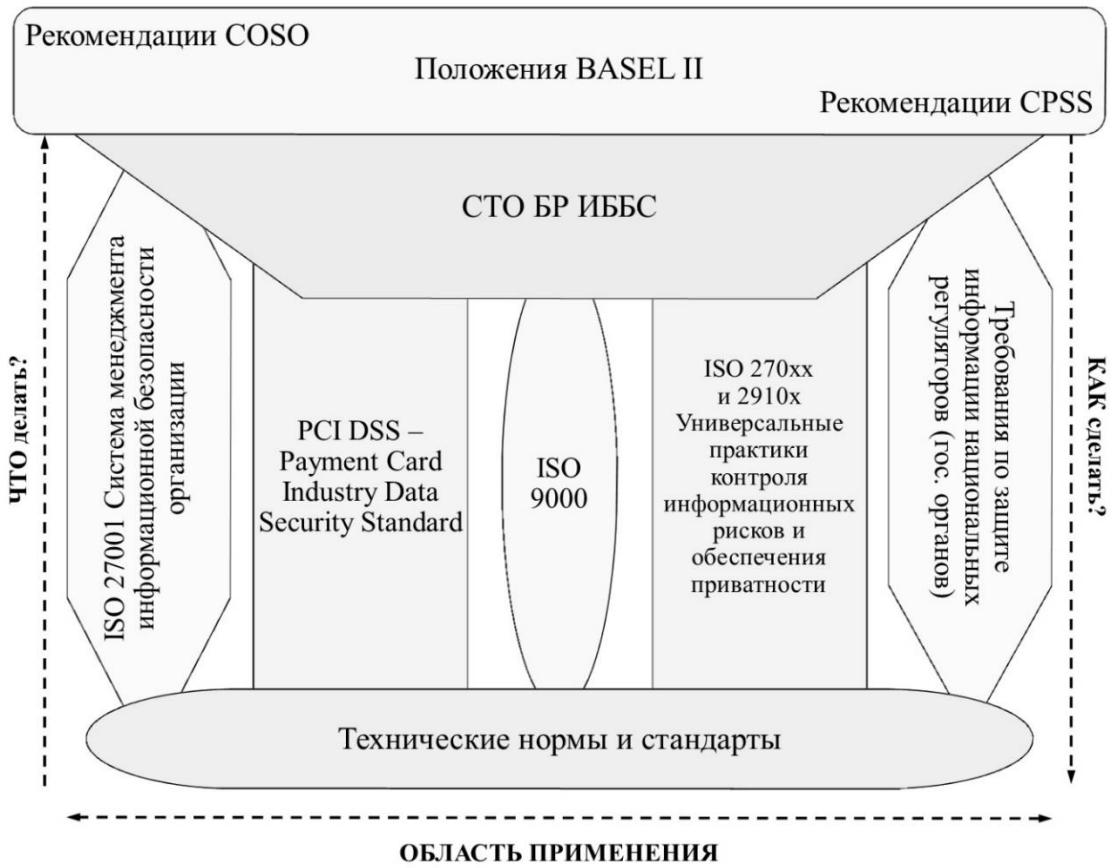
В работе используется определение «Риск воздействия кибератак» (РВКа) при наличии общепризнанных «риск нарушения информационной безопасности» или «риск кибербезопасности». Данный термин введен в [4–5].

Существующие возможности позволяют выбирать те решения по обеспечению информационной безопасности ТЭБ, которые смогут обеспечить наиболее комфортную деятельность в цифровом операционном пространстве банка и эффективное осуществление корпоративного контроля и менеджмента. Кредитные организации России должны выбирать комплементарные (взаимодополняющие) решения, которые охватывают корпоративный менеджмент в цифровой сфере и цифровую среду кредитно-финансовой организации (рис. 1).

Целями деятельности комиссии COSO (англ. The Committee of Sponsoring Organizations of the Treadway Commission, USA) является изучение факторов, которые

[1]Информационная безопасность (мировой рынок). Портал по теме корпоративной информатизации. URL: https://www.tadviser.ru/a/275984 (дата обращения: 10.12.2020).

способны приводить к мошенничеству с финансовой отчетностью, а также выработка рекомендаций по обеспечению информационной безопасности организации и действий по важнейшим аспектам управления организацией, внутреннего контроля, минимизации рисков компаний и противодействия мошенничеству.



COSO – The Committee of Sponsoring Organizations of the Treadway Commission (Комитет спонсорских организаций);

CPSS (КПРС) – Committee on Payment and Settlement Systems, Комитет по платежным и расчетным системам Банка международных расчетов (Bank for International Settlements – BIS);

СТО БР ИББС – стандарты Банка России по обеспечению информационной безопасности банков страны;

ISO 9000 – стандарты Международной организации стандартизации по менеджменту качества;

ISO 270xx – стандарты Международной организации стандартизации по управлению информационной безопасностью;

PCI DSS – стандарт безопасности данных индустрии платежных карт; подразумевается комплексный подход к обеспечению информационной безопасности данных платежных карт.

Рис. 1. Нормативы и стандарты по обеспечению кибербезопасности ТЭБ [6]
(Fig. 1. Regulations and standards for cybersecurity of electronic banking technologies [6])

Стандарты Центробанка России «СТО/РС БР ИББС», описывающие методологию обеспечения информационной безопасности, могут быть дополнены рекомендациями и

положениями по управлению кибербезопасностью, содержащимися в международных стандартах ISO/IEC (комплексы 270xx и 2910x), которые направлены на решение определенной задачи управления информационной безопасностью коммерческого банка.

Набор взаимодополняющих документов PCI DSS (Payment Card Industry Data Security Standard, Стандарт безопасности данных индустрии платежных карт) создан компетентными органами международных платежных систем Visa, MasterCard, American Express, JCB и Discover. Стандарты PCI DSS являются совокупностью из двенадцати детализированных требований обеспечения информационной безопасности держателей платежных карт (с учетом передачи, хранения и обработки этих карт в информационных инфраструктурах организаций).

Набор единых требований, стандартов и методик регулирования банковского дела, которые принимаются в различных странах, разрабатывается Ба́зельским комитетом по банковскому надзору (БКБН). Эта организация действует при Банке международных расчетов. Совершенствованию банковского надзора посвящены документы Basel II, а также Basel III и Basel IV [6]. С их содержанием, а также со статьями ведущих экспертов в области банковского надзора можно познакомиться на сайте БКБН https://www.bis.org.

В [4–5] рассматриваются документы Basel II при наличии Basel III и IV. Причина в том, что внедрение итогового набора регуляторных требований к банкам, включающего в себя все изменения Базеля III и пересмотренные подходы к оценке рыночного риска, первоначально планировавшееся на 2019 г., теперь перенесено на 2022 г. Банк России собирается внедрить соответствующие изменения в регулирование кредитно-финансовой деятельности Российской Федерации, в т.ч. в части регулирования рыночного риска, в сроки, предусмотренные БКБН[2]. Пандемия COVID-19, возможно, затормозит развитие. О внедрении Ба́зель IV речь вообще не идет.

Поскольку банковская отрасль чрезвычайно консервативна и нередко инертна [1], то любые нововведения должны быть очень аккуратны. В работе [7], посвященной реинжинирингу, наряду с методическими указаниями, приведены примеры (кейсы) фундаментальной переработки и радикальной перестройки бизнес-процессов для того, чтобы получить максимальный эффект от производственно-хозяйственной и финансово-экономической деятельности. Предложена модель PEMM, позволяющая оценить стадии развития сложных процессов компании, по 9 направлениям:

1. Проектирование сквозного (межфункционального) процесса;
2. Исполнители бизнес-процесса;
3. Компетенции руководителя процесса;
4. Инфраструктура (информационная система);
5. Определение и использование показателей результата деятельности;
6. Представители высшего руководства;
7. Качество обслуживания и культура работы предприятия;
8. Специалисты в области перестройки и реализации процессов;
9. Структура управления процессами.

Таким образом, модель PEMM позволяет определить стадию развития внедряемого бизнес-процесса и увидеть, какое направление должно быть улучшено или доработано [7]. Методология реинжиниринга, используемая с 1990 г., имеет значительные преимущества, такие как снижение затрат и рост производительности, улучшение качества продукции и повышение удовлетворенности клиентов [8]. Схема взаимодействий при реализации РВКа в кредитной организации (инцидента информационной безопасности) представлена на рис. 2.

[2]См. подробнее о сроках внедрения Базеля III: URL: https://cbr.ru/press/pr/?file=06022018_120000ik2018-02-06t11_55_45.htm (дата обращения: 24.11.2020).

Схема иллюстрирует переход от децентрализованной (местные SOC) к централизованной (государственные CERT и CSIRT) системе управления РВКа в ТЭБ.

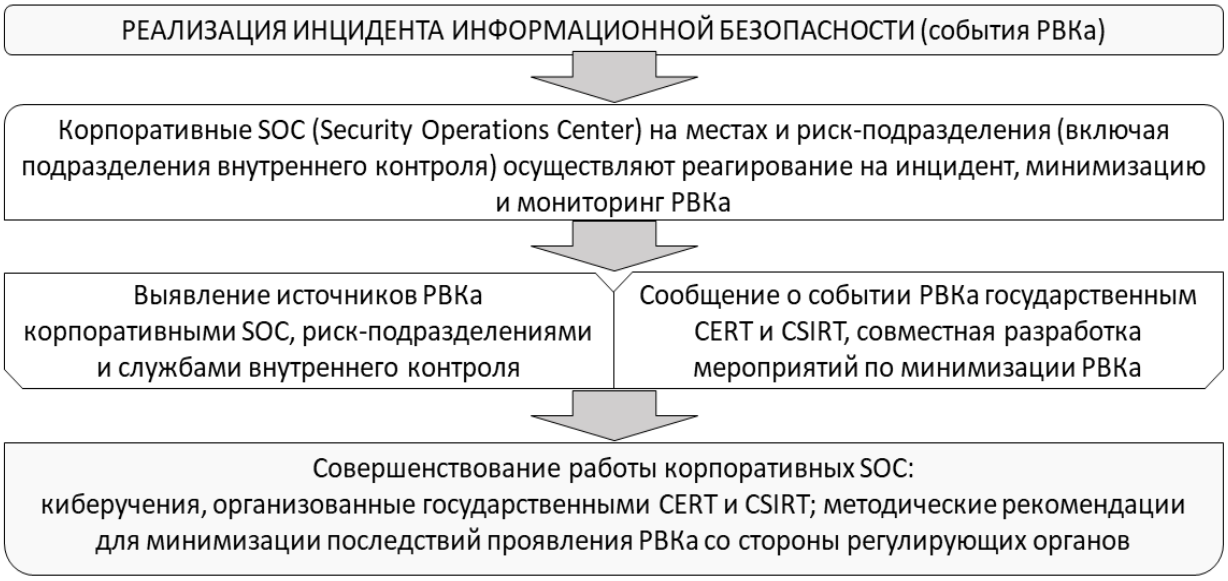


Рис. 2. Схема взаимодействий при реализации РВКа в банке
(Fig. 2. Scheme of interactions in the risk of cyberattacks in a bank)

Таким образом, основа для доверительного отношения клиентов и контрагентов банка к его продуктам формируется благодаря использованию общепризнанных лучших практик, получивших отражение в основных стандартах и требованиях к реализации деятельности организации [6]. Тем не менее, развитие цифровых финансовых технологий требует внедрения новых межфункциональных бизнес-процессов.

2. Разработка метода оценки деятельности киберпреступников

Проанализируем справочные данные о развитии информационного потенциала разных стран, где основной его количественной характеристикой выбран интегральный показатель «Индекс развития электронного правительства»[3] (табл. 1 и рис. 3).

Неоднородность информационного пространства имеет тенденцию к возрастанию как на уровне отдельного пользователя и бизнеса, так и на уровне суверенных государств [9], что видно из столбцов «Прирост показателя ВНП» и «Прирост индекса E-gov» таблицы. Это становится причиной возникновения очередных вызовов международной (информационной) безопасности.

Коэффициенты корреляции в первом случае 0,78; во втором случае 0,66. Данные подтверждают, что гаджеты перестали быть признаком роскоши и прочнее вошли в нашу жизнь. Рассматриваемая неоднородность говорит нам о том, что качество услуг ТЭБ и удобство программного продукта (см. введение, п. 2) – параметры относительные и они зависят как от производителя, так и от нарушителей кибербезопасности.

Внедрение новых бизнес-процессов в рамках реинжиниринга содержит разработку новой системы показателей для измерения результата деятельности (англ. Key Performance

[3]Рейтинг стран мира по индексу развития электронного правительства. URL: https://gtmarket.ru/ratings/e-government-development-index (дата обращения: 10.01.2021).

Indicators, KPI) компании, потому что инструменты, которые используются в большинстве компаний для измерения и улучшения производительности, малоэффективны [7] и их эффективность снижается со временем и цифровизацией. В [5] автор определил формулу для оценки резервируемого капитала, который выделяется под киберриск в составе операционного риска банка:

$$R_{\text{РВКа}} = \alpha \cdot \frac{1}{3} \cdot \sum_{i=1}^{3} \text{ВД}_i \Big/ \frac{n \cdot IQ_{\text{ZL}} \cdot r}{(d+v) \cdot t}, \quad (1)$$

где числитель $K_{\text{ОР}} = \alpha \cdot \frac{1}{3} \cdot \sum_{i=1}^{3} ВД_i$ задает размер капитала, который выделяется на покрытие операционных рисков в коммерческом банке методом базового индикатора (см. подробнее соглашение БКБН – Basel II). В знаменателе дроби – оценка эффективности киберoружия[4] ($ef = \frac{n \cdot IQ_{\text{ZL}} \cdot r}{(d+v) \cdot t}$, безразмерная величина). Однако данная формула может быть применена для определения размера штрафа, выносимого киберпреступникам.

Приведем пример расчета для следующих данных:

- размер капитала, который резервируется в кредитной организации на покрытие операционного риска равен $K_{\text{ОР}} = 10\,000\,000$ руб.
- средний размер ущерба от одной реализации РВКа в ТЭБ, – $n = 11\,000\,000$ руб[5].
- коэффициент интеллекта киберпреступников, привлеченных к ответственности, чаще всего лежит в интервале 70–90, согласно [10]. Поэтому возьмем $IQ_{\text{ZL}} = 80$ [6].
- восстановление непрерывности банковской деятельности (равно времени остановки бизнеса) после реализации РВКа заняло $r = 4$ часа.
- услуги хакеров и расходы на оборудование оценим в $d + v = 500\,000$ руб.
- время изготовления киберoружия $t = 8$ дн. $\times 9$ ч. $= 72$ часа.

Результат вычислений $R_{\text{РВКа}} = 102\,272,7$ руб. получен подстановкой рассмотренных значений в формулу (1) и может представлять размер штрафа, который налагается на компьютерных преступников. Актуальность формулы возросла, когда в ноябре 2020 г. власти России внесли в Государственную Думу законопроект о введении штрафов за нарушение информационной безопасности объектов критической информационной инфраструктуры страны[7].

[4]Обобщенный термин, предлагаемый автором, включает комплекс мер, направленных на осуществление кибератаки и реализацию РВКа.

[5]Лаборатория Касперского подсчитала средний ущерб от кибератаки на бизнес. URL: https://ria.ru/20160915/1477053600.html (дата обращения: 20.12.2020).

[6]Деанонимизацией (установлением личности в сети) занимается форензика. Действия в Интернете регистрируются на Web-серверах в специальных журналах, а записи с камер видеонаблюдения, установленных в общественных местах, будут подтверждением действий. Это используется при проведении следственных мероприятий.

[7]Нарушение IT-безопасности КИИ в РФ может грозить штрафом до 500 тыс. рублей. URL: https://www.securitylab.ru/news/513744.php (дата обращения: 23.11.2020).

Таблица 1. Динамика развития стран мира по готовности перехода к электронному правительству в зависимости от ВНП на душу населения

Наиболее развитые страны мира	**ВНП на душу населения, 2002 (долл.)**	**Индекс готовности перехода к E-gov, 2004**	**ВНП на душу населения, 2019 (долл.)**	**Индекс готовности перехода к E-gov, 2020**	**Прирост показателя ВНП**	**Прирост индекса E-gov**
Швейцария	40680,0	0,75	70989,0	0,8907	74,51%	18,76%
Соединенные Штаты Америки	37870,0	0,91	65281,0	0,9297	72,38%	2,16%
Япония	34180,0	0,73	43236,0	0,8989	26,50%	23,14%
Дания	33570,0	0,90	59830,0	0,9758	78,22%	8,42%
Исландия	30910,0	0,77	60061,0	0,9101	94,31%	18,19%
Швеция	28910,0	0,87	55815,0	0,9365	93,06%	7,64%
Великобритания	28320,0	0,89	48710,0	0,9358	72,00%	5,15%
Финляндия	27060,0	0,82	51324,0	0,9452	89,67%	15,27%
Австрия	26810,0	0,75	59111,0	0,8914	120,48%	18,85%
Нидерланды	26230,0	0,80	59687,0	0,9228	127,55%	15,35%
Бельгия	25760,0	0,75	54545,0	0,8047	111,74%	7,29%
Германия	25270,0	0,79	56052,0	0,8524	121,81%	7,90%
Франция	24730,0	0,67	49435,0	0,8718	99,90%	30,12%
Канада	24470,0	0,84	51342,0	0,8420	109,82%	0,24%
Австралия	21950,0	0,84	53320,0	0,9432	142,92%	12,29%
Италия	21570,0	0,66	44197,0	0,8231	104,90%	24,71%
Сингапур	21230,0	0,83	101376,0	0,9150	377,51%	9,71%
Республика Корея	12030,0	0,86	43029,0	0,9560	257,68%	11,49%
Россия	2610,0	0,50	29181,0	0,8244	1018,05%	64,88%
Румыния	2260,0	0,55	32297,0	0,7605	1329,07%	38,27%
Китай	1100,0	0,44	16785,0	0,7948	1425,91%	82,46%
Индия	540,0	0,39	7034,0	0,5964	1202,59%	53,75%

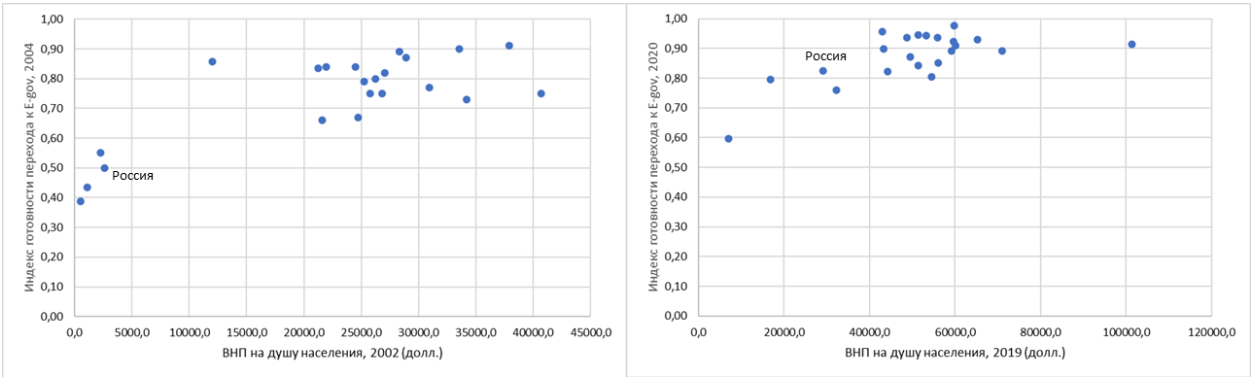


Рис. 3. Индекс готовности перехода к электронному правительству в зависимости от ВНП на душу населения (по странам) на начало 2000-х и конец 2010-х гг.
(Fig. 3. Index of readiness for the transition to e-government, depending on GNP per capita (by country) at the beginning of the 2000s and the end of the 2010s)

3. Метод скоростной печати на клавиатуре как организационно-технический бизнес-процесс повышения производительности труда

Реинжиниринг бизнес-процессов и уровень внедрения в компании корпоративной информационной системы (чем и являются ТЭБ) – это различные процессы, которые не должны совмещаться. Если проводится реинжиниринг, то технологии, автоматизирующие процесс, должны «накладываться» только на правильно построенный сквозной бизнес-процесс. Поэтому в данной статье предложено изменение процесса, который проходит через все функции компании, добавляющие ценность продукту, и направлен на работу персонала и клиентов *с уже имеющимися* технологиями. Данный бизнес-процесс назовем методом скоростной печати (МСП) – тема, смежная с информационной безопасностью. Научный результат включает многолетний опыт автора статьи и его эмпирические наблюдения за служащими и клиентами банковских, риэлторских и других офисов, подтвержденные статистикой.

Группа ученых из Aalto University в Финляндии проанализировала технику набора текста на клавиатуре 168 тыс. человек из 200 стран мира и обнаружила, что пользователи, которые набирают текст быстрее, допускают меньше ошибок, а пользователи, которые печатают медленнее, тратят больше времени на поиск и исправление опечаток[8].

За рубежом МСП – часть школьной программы. В Европе десятипальцевой печатью владеет большинство специалистов «офисных» профессий [11]. Свыше 70% американцев печатают вслепую; в России менее 10% таких людей [12]. Автору удалось связаться с первой и единственной советской чемпионкой по скоростному набору текста на компьютере Элеонорой Алексеевной Лукиной. По ее словам, в Чехии серьезное обучение слепой печати включено в программы почти 100% средних школ и насчет взрослых людей тоже не менее серьезно: от поступающих на государственную службу требуется скорость в МСП не менее 400 зн./мин. Это достигнуто усилиями Ярослава Завьячича и чешской Interinfo (Interinfo – национальное отделение общества Intersteno[9]).

Согласно работам классиков, мозг человека эволюционировал от систематического ручного труда [13]. МСП аналогичен соблюдению правил дорожного движения, без чего на автодороге был бы хаос. Создавая эффект «лежачего полицейского», МСП затормаживает бессознательное движение пользователя вперед при наборе текста, благодаря чему позволяет существенно повысить производительность труда. В музыке порядок расположения и последовательность чередования пальцев рук при игре на музыкальных инструментах называется аппликатурой (от нем. Applikatur и лат. applico – прикладываю, прижимаю). Правильное расположение пальцев – это важный составной элемент мастерства исполнителя. Поэтому аппликатуре уделяется особое внимание (автор знаком с этим на собственном опыте, т.к. осваивал игру на баяне в музыкальной школе).

Навык МСП так же элементарен, как дезинфекция рук врача перед хирургической операцией. Сейчас необходимость дезинфекции рук является аксиомой, но 175 лет назад это невежество приводило к смертям от послеродового сепсиса, вызванного невидимыми частицами (бактериями) на руках хирурга [14].

Благодаря МСП достигается *непрерывность печатания*. Пользователю не приходится искать нужную клавишу и палец, которым ее нажать, – это происходит автоматически. Именно на непрерывности базируется японская методика «Кайдзен»

[8]Электронный журнал “Naked Science”. Ученые сформулировали новые правила скоростного набора текста. URL: https://naked-science.ru/article/sci/uchenye-sformulirovali-novye-pravila (дата обращения: 22.11.2020).
[9]International Federation for Information and Communication Processing – профессиональное некоммерческое сообщество, направленное на развитие мировых достижений в области технического обеспечения информационного процесса (см. подробнее: intersteno.ru и intersteno.org).

(яп. 改善), направленная на улучшение бизнес-процессов предприятия, а также всех аспектов деятельности. Непрерывность производственного процесса подразумевает ликвидацию незапланированных остановок и задержек в работе, что является достаточным основанием для роста производительности труда (в том числе в кредитно-финансовой деятельности).

Для самостоятельного овладения МСП можно обойтись и без платных тренажеров. В 2009 г. автором статьи был разработан тренажер, который приведен на рис. 4 и устанавливается на рабочий стол монитора. Выровняв текстовый редактор так, как показано на рис. 4., пользователю достаточно набирать любой текст, ориентируясь на мышечную память, сразу «вслепую».

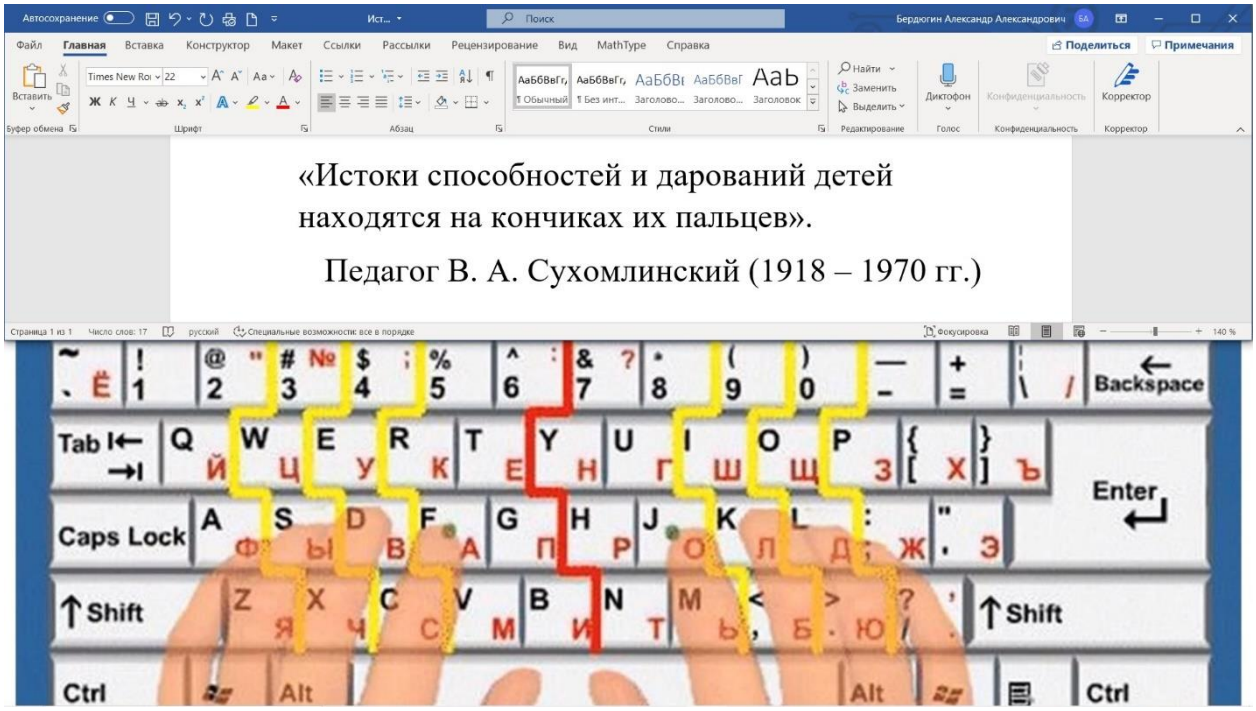


Рис. 4. Тренажер МСП для самостоятельного освоения
(Fig. 4. High-speed printing simulator for self-development)

Для разминки между занятиями МСП может использоваться кистевой эспандер – резиновый тор умеренной жесткости. Кроме того, гимнастика для глаз также полезна для восстановления кровоснабжения в глазных мышцах. Упоминание о кистевом эспандере здесь обусловлено II законом Ньютона в импульсном виде:

$$\vec{F} = m \cdot \frac{d\vec{v}}{dt} \Leftrightarrow d\vec{v} = \frac{\vec{F} \cdot dt}{m},$$

где $\vec{F}$ – прилагаемая одиночная сила; m – масса тела; dt – изменение времени движения. При этом изменение скорости $d\vec{v}$ прямо пропорционально прилагаемой силе.

МСП не решит всех проблем информационной безопасности, но позволит избежать ряда незначительных ошибок, которые в совокупности могут дать катастрофическую реализацию РВКа (заметить скрытую переадресацию браузера на мошеннический сайт легче, глядя в монитор при наборе текста). Более того, МСП может стать одним из биометрических признаков клиента (например, работы [15–16] посвящены анализу

функционального динамического комплекса навыков пользователя для воспроизведения аутентифицирующего жеста) – тема для дальнейших исследований.

МСП на клавиатуре предлагается ввести в образовательную программу России для развития мышечной памяти пользователя и повышения его киберграмотности [11, 12, 17]. Практическая целесообразность освоения МСП в школе обусловлена тем, что в повседневной деятельности человек должен обладать навыком по информатике, который имеет прикладное значение в реальной жизни[10].

Освоение МСП на уроках информатики будет способствовать развитию физических умений обращения с компьютером наряду с улучшением интеллектуальных качеств, а это, в свою очередь, – укреплению киберграмотности и компьютерной дисциплины. Следующий шаг после освоения МСП – соревнования на сайтах, подобных http://klavogonki.ru/ (клавиатурный тренажер в игровой форме).

Заключение

Соответствие коммерческого банка – участника финансовой системы передовым практикам и/или общепризнанным известным стандартам, которые проверены временем и имеют независимую оценку (аудит), является основой для доверия его контрагентов и клиентов к финансовым технологиям этого банка.

Неоднородность киберпространства порождает нестабильность качества услуг ТЭБ и удобства программного продукта. Одна из причин неоднородности – компьютерная преступность. В статье предложена оценка для определения штрафа за нарушение защиты критической информационной инфраструктуры.

Проанализирована скоростная печать на клавиатуре как межфункциональный бизнес-процесс, который будет способствовать увеличению производительности и дохода кредитной организации за счет уменьшения доли затрат и количества операционных ошибок, порождаемых непредусмотренными прерываниями при наборе текста (уровень финансовой и компьютерной грамотности клиента и специалиста банка).

СПИСОК ЛИТЕРАТУРЫ:

1. King B. Bank 4.0: Banking Everywhere, Never at a Bank. Singapore: John Wiley & Sons Limited, 2018. – 352 p.
2. Skinner C. Digital Human: The Fourth Revolution of Humanity Includes Everyone. Singapore: Marshall Cavendish International (Asia), 2018. – 328 p.
3. Поспелов А.Л., Ревенков П.В. Что сдерживает использование дистанционных каналов обслуживания? // Расчеты и операционная работа в коммерческом банке. 2015. № 1 (125). С. 70–75. URL: http://www.reglament.net/bank/raschet/2015_1/get_article.htm?id=3823 (дата обращения: 18.12.2020).
4. Бердюгин А.А., Ревенков П.В. Оценка риска воздействия кибератак в технологиях электронного банкинга (пример программной реализации) // Финансы: теория и практика. 2020. Т. 24, № 6. С. 51–60. DOI: http://dx.doi.org/10.26794/2587-5671-2020-24-6-51-60.
5. Ревенков П.В., Бердюгин А.А. Метод количественной оценки риска воздействия кибератак в условиях электронного банкинга // Банковское дело. 2020. №7. С. 32–37.
6. Воронин А.С. Национальная платежная система. Бизнес-энциклопедия. М.: КНОРУС: ЦИПСиР, 2013. – 424 с.
7. Хаммер Майкл, Лиза Хершман. Быстрее, лучше, дешевле: Девять методов реинжиниринга бизнес-процессов. М.: Альпина Паблишер, 2017. – 352 с.
8. Mahmoud AbdEllatif, Marwa Salah Farhan, Naglaa Saeed Shehata. Overcoming business process reengineering obstacles using ontology-based knowledge map methodology. Future Computing and Informatics Journal. 2018. V. 3, Iss. 1, P. 7–28. DOI: https://doi.org/10.1016/j.fcij.2017.10.006.

[10]См. подробнее № 25 еженедельника «Аргументы и Факты», статья «Почему задания ЕГЭ по математике такие простые?». URL: https://aif.ru/dontknows/actual/pochemu_zadaniya_ege_po_matematike_takie_prostye (дата обращения: 08.12.2020).

9. Роговский Е.А. Кибер-Вашингтон: глобальные амбиции. М.: Международные отношения, 2014. – 848 с.
10. Arthur Jensen. The g Factor: The Science of Mental Ability. Greenwood Publishing Group, Inc. (GPG), Santa Barbara, California, 1998. – 648 p.
11. Ильнер А.О. Подготовка переводчиков в России и за рубежом: сравнительный анализ // Образование и наука. 2010. № 8 (76). С. 65–70. URL: https://cyberleninka.ru/article/n/podgotovka-perevodchikov-v-rossii-i-za-rubezhom-sravnitelnyy-analiz (дата обращения: 11.12.2020).
12. Шахиджанян В.В. Готов научить всех // Авиасалоны мира. 2007. № 2. С. 46–47. URL: https://issuu.com/dizone/docs/aviasalony_all_2007_mini (дата обращения: 11.12.2020).
13. Лобанов В.В. Роль труда в опытах физического воспитания В.С. Пирусского // Вестник Томского государственного педагогического университета. 2013. № 9 (137). С. 181–187. URL: https://www.elibrary.ru/item.asp?id=20933711 (дата обращения: 12.12.2020).
14. Newsom S. W. B. Ignaz Philipp Semmelweis. Journal of Hospital Infection. 1993. V. 23, Iss. 3. P. 175–187. URL: https://sciencedirect.com/science/article/abs/pii/019567019390023S (дата обращения: 10.12.2020).
15. Козлов Ю.Е. Использование методов визуальной аналитики для получения комплексного показателя качества биометрической аутентификации с использованием механизма жестовой манипуляции // Научная визуализация. 2019. Т. 11. № 2. С. 99–113. URL: http://sv-journal.org/2019-2/08/ (дата обращения: 18.12.2020). DOI: http://dx.doi.org/10.26583/sv.11.2.08.
16. Береснева, Анастасия В.; Епишкина, Анна В. Подходы к онлайн верификации собственноручной подписи. Безопасность информационных технологий, [S.l.]. Т. 27, № 2. С. 78–85, июнь 2020. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1272. (дата обращения: 18.12.2020). DOI: http://dx.doi.org/10.26583/bit.2020.2.06.
17. Андреев А.Н., Румянцев С.А. Особенности подготовки специалистов в сфере информационных технологий и использование компьютерных программ с целью повышения качества самообразования // Труды международного симпозиума «Надежность и качество». 2012. Т. 1. С. 388–391. URL: https://noosphere.ru/pubs/344211 (дата обращения: 18.12.2020).

REFERENCES:

[1] King B. Bank 4.0: Banking Everywhere, Never at a Bank. Singapore: John Wiley & Sons Limited, 2018. – 352 p.
[2] Skinner C. Digital Human: The Fourth Revolution of Humanity Includes Everyone. Singapore: Marshall Cavendish International (Asia), 2018. – 328 p.
[3] Pospelov A.L., Revenkov P.V. What hinders the use of remote service channels? Calculations and operational work in a commercial Bank. 2015, no. 1 (125). P. 70–75 URL: http://www.reglament.net/bank/raschet/2015_1/get_article.htm?id=3823 (accessed: 18.12.2020) (in Russian).
[4] Berdyugin A.A., Revenkov P.V. Cyberattack risk assessment in electronic banking technologies (the case of software implementation). Finance: Theory and Practice. 2020. V. 24, no. 6. P. 51–60. DOI: http://dx.doi.org/10.26794/2587-5671-2020-24-6-51-60. (in Russian)
[5] Revenkov P.V., Berdyugin A.A. Method of quantifying the risk of cyberattacks in the context of electronic banking. Bankovskoye delo = Banking. 2020, no. 7. P. 32–37 (in Russian).
[6] Voronin A.S. National payment system. Business encyclopedia, Moscow: KNORUS: Tsipsir, 2013. – 424 p.
[7] Hammer M., Hershman L. Faster Cheaper Better: The 9 Levers for Transforming How Work Gets Done. Moscow, Alpina Publisher, 2017. – 352 p.
[8] Mahmoud AbdEllatif, Marwa Salah Farhan, Naglaa Saeed Shehata. Overcoming business process reengineering obstacles using ontology-based knowledge map methodology. Future Computing and Informatics Journal. 2018. V. 3, Iss. 1, P. 7–28. DOI: https://doi.org/10.1016/j.fcij.2017.10.006.
[9] Rogovsky E.A. Cyber-Washington: global ambitions. Moscow: International relations; 2014. – 848 p. (in Russian).
[10] Arthur Jensen. The g Factor: The Science of Mental Ability. Greenwood Publishing Group, Inc. (GPG), Santa Barbara, California, 1998. – 648 p.
[11] Ilner A.O. The analysis of training translators and interpreters in Russia and abroad. Education and Science. 2010, no. 8 (76). P. 65–70. URL: https://cyberleninka.ru/article/n/podgotovka-perevodchikov-v-rossii-i-za-rubezhom-sravnitelnyy-analiz (accessed: 11.12.2020) (in Russian).
[12] Shakhidjanyan V.V. Ready to teach everyone. Airshows of the world. 2007, no. 2. 46–47. URL: https://issuu.com/dizone/docs/aviasalony_all_2007_mini (accessed: 11.12.2020) (in Russian).
[13] Lobanov V.V. The role of craft in the physical education practices by V.S. Pirussky. Bulletin of the Tomsk State Pedagogical University. 2013, no. 9 (137). P. 181–187. URL: https://www.elibrary.ru/item.asp?id=20933711. (accessed: 12.12.2020) (in Russian).

[14] Newsom S. W. B. Ignaz Philipp Semmelweis. Journal of Hospital Infection. 1993. V. 23, Iss. 3. P. 175–187. URL: https://sciencedirect.com/science/article/abs/pii/019567019390023S (accessed: 10.12.2020)

[15] Kozlov Yu.E. Use of methods of visual analytics to obtain integrated indicator of the quality of biometric authentication using the mechanism gesture manipulation. Scientific Visualization, 2019. V. 11, no. 2. P. 99–113. URL: http://sv-journal.org/2019-2/08/ (accessed: 18.12.2020). DOI: https://doi.org/10.26583/sv.11.2.08.

[16] Beresneva, Anastasia V., Epishkina, AnnaV. Approaches to online handwritten signature verification. IT Security (Russia), [S.l.]. V. 27, no. 2. P. 78–85, June 2020. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1272. (accessed: 18.12.2020). DOI: http://dx.doi.org/10.26583/bit.2020.2.06.

[17] Andreev A.N., Rumyantsev S.A. Features of training specialists in the field of information technologies and the use of computer programs to improve the quality of self-education. Proceedings of the international Symposium “Reliability and quality”, 2012. V. 1. P. 388–391. URL: https://noosphere.ru/pubs/344211 (in Russian).

Поступила в редакцию – 19 декабря 2020 г. Окончательный вариант – 01.02.2021 г.
Received – December 19, 2020. The final version – February 01, 2021.

Михаил А. Иванов[1], Ирина Г. Коннова[2], Евгений А. Саликов[3], Мария А. Степанова[4]
[1,3]Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, Москва, 115409, Россия
[1,2]Финансовый университет при Правительстве Российской Федерации
(Финансовый университет),
Ленинградский пр-т, 49, Москва, 125993, Россия
[1,4]Российский государственный университет (НИУ) им. И.М. Губкина,
Ленинский пр–т, 65, корпус 1, Москва, 119991, Россия
[1]e-mail: maivanov@mephi.ru, https://orcid.org/0000-0002-3204-8055
[2]e-mail: igkonnova@fa.ru, https://orcid.org/0000-0003-1228-6256
[3]e-mail: esalikov51@gmail.com, https://orcid.org/0000-0002-3387-1000
[4]e-mail: maha2702@list.ru, https://orcid.org/0000-0003-3880-9537

ОБФУСКАЦИЯ ЛОГИЧЕСКИХ СХЕМ ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ НА РЕГИСТРАХ СДВИГА С ЛИНЕЙНЫМИ И НЕЛИНЕЙНЫМИ ОБРАТНЫМИ СВЯЗЯМИ

DOI: http://dx.doi.org/10.26583/bit.2021.1.06

Аннотация. Цель работы – продемонстрировать возможность использования технологии Logic Encryption для защиты от реверс-инжиниринга логических схем генераторов псевдослучайных чисел на регистрах с линейными и нелинейными обратными связями. Рассматриваемые методы защиты основаны на использовании дополнительных логических элементов в структуре генератора, чтобы скрыть его оригинальные функциональные возможности. Обфускация логической схемы генератора меняет его конструкцию таким образом, что устройство работает правильно, только в том случае, если сигналы на дополнительных ключевых входах генератора принимают правильные значения. Показано, что даже при небольшой разрядности генераторов можно обеспечить огромное количество вариантов реализации ГПСЧ с различным числом состояний и различными свойствами. Введено понятие генератора (M + 1)-последовательности. Продемонстрирована возможность трансформации генераторов (M – 1)- и (M – 3)-последовательностей в генераторы (M + 1)-последовательностей. Главной проблемой IoT является его уязвимость к кибератакам. Предлагаемые методы позволяют повысить безопасность IoT устройств.

Ключевые слова: обфускация, регистр сдвига с линейной обратной связью, регистр сдвига с нелинейной обратной связью, (M + 1)-последовательность, генератор псевдослучайных чисел.
Для цитирования: ИВАНОВ, Михаил А. и др. ОБФУСКАЦИЯ ЛОГИЧЕСКИХ СХЕМ ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ НА РЕГИСТРАХ СДВИГА С ЛИНЕЙНЫМИ И НЕЛИНЕЙНЫМИ ОБРАТНЫМИ СВЯЗЯМИ. Безопасность информационных технологий, [S.l.], v. 28, n. 1, p. 74–83, jan. 2021. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1322>. Дата доступа: 08 feb. 2021. DOI: http://dx.doi.org/10.26583/bit.2021.1.06.

Michael A. Ivanov[1], Irina G. Konnova[2], Evgeniy A. Salikov[3], Maria A. Stepanova[4]
[1,3]National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Kashirskoe shosse, 31, Moscow, 115409, Russia
[1,2]Financial University under the Government of the Russian Federation (Financial University),
Leningradskiy Prospekt, 49, Moscow, 125993, Russia
[1,4]National University of Oil and Gas "Gubkin University",
Leninskiy Prospekt, 65, building 1, Moscow, 119991, Russia
[1]e-mail: maivanov@mephi.ru, https://orcid.org/0000-0002-3204-8055
[2]e-mail: igkonnova@fa.ru, https://orcid.org/0000-0003-1228-6256
[3]e-mail: esalikov51@gmail.com, https://orcid.org/0000-0002-3387-1000
[4]e-mail: maha2702@list.ru, https://orcid.org/0000-0003-3880-9537

Obfuscation of logic schemes of pseudo-random number generators based on linear and non-linear feedback shift registers

DOI: http://dx.doi.org/10.26583/bit.2021.1.06

Abstract. The paper describes methods of protection against reverse engineering of logic circuits of pseudo-random number generators (PRNG) on linear and non-linear feedback shift registers. These methods are based on the use of additional logic elements in the structure of the generator to hide its original functionality. Obfuscation of the generator logic circuit changes its design such that the device works correctly only if the signals at the additional key inputs of the generator take on the correct values. It is shown that even with a small bit capacity of generators, it is possible to provide a huge number of PRNG implementations with different numbers of states and different properties. The concept of a (M + 1)-sequence generator is introduced. The possibility of transforming (M – 1)- and (M – 3)-sequences generators into (M + 1)-sequences generators is demonstrated. The proposed methods can be used to ensure the security of IoT devices.

Keywords: obfuscation, linear feedback shift register, non-linear feedback shift register, (M + 1)-sequence, pseudo-random number generator.

For citation: IVANOV, Michael A. et al. Obfuscation of logic schemes of pseudo-random number generators based on linear and non-linear feedback shift registers. IT Security (Russia), [S.l.], v. 28, n. 1, p. 74–83, jan. 2021. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1322>. Date accessed: 08 feb. 2021. DOI: http://dx.doi.org/10.26583/bit.2021.1.06.

Введение

В последние годы серьезной угрозой безопасности компьютерных систем стало вредоносное аппаратное обеспечение. Из-за аутсорсинга в процессе изготовления интегральных схем (ИС) появляются проблемы, связанные с внедрением аппаратных закладок, подделками ИС, пиратством и несанкционированным перепроизводством.

Наиболее эффективные возможности по предотвращению вышеперечисленных угроз предоставляют технологии Logic Encryption и Design Obfuscation [1–6], реализация второй их них может быть основана на использовании генераторов псевдослучайных чисел (ГПСЧ) с нестандартной диаграммой переключений, например, генераторов ($M – p$ + 1)-последовательностей и генераторов ($M – 2^n$ + 1)-последовательностей, где p – простое, а n – натуральное [7].

В работе рассматриваются особенности применения технологии Logic Encryption для запутывания логической схемы двоичных ГПСЧ (pseudo-random number generator – PRNG) на регистрах сдвига с линейными и нелинейными обратными связями (соответственно linear feedback shift register – LFSR и nonlinear feedback shift register – NLFSR).

1. Регистры сдвига с линейными и нелинейными обратными связями

ГПСЧ на LFSR и NLFSR уже достаточно давно применяются для решения различных задач защиты информации от случайных и умышленных деструктивных воздействий [8–14]. Можно выделить следующие области их использования:

- самотестирование цифровых устройств на БИС;
- вероятностное тестирование цифровых устройств;
- формирование CRC-кодов;
- построение скремблеров и дескремблеров;
- построение ГПСЧ с нестандартными диаграммами переключений;
- построение поточных и блочных симметричных криптоалгоритмов.

На рис. 1 приведены примеры наиболее распространенных схем ГПСЧ на LFSR и NLFSR, где рассматривается четырехразрядный случай, т.е. $N = 4$, где N – степень характеристического многочлена.

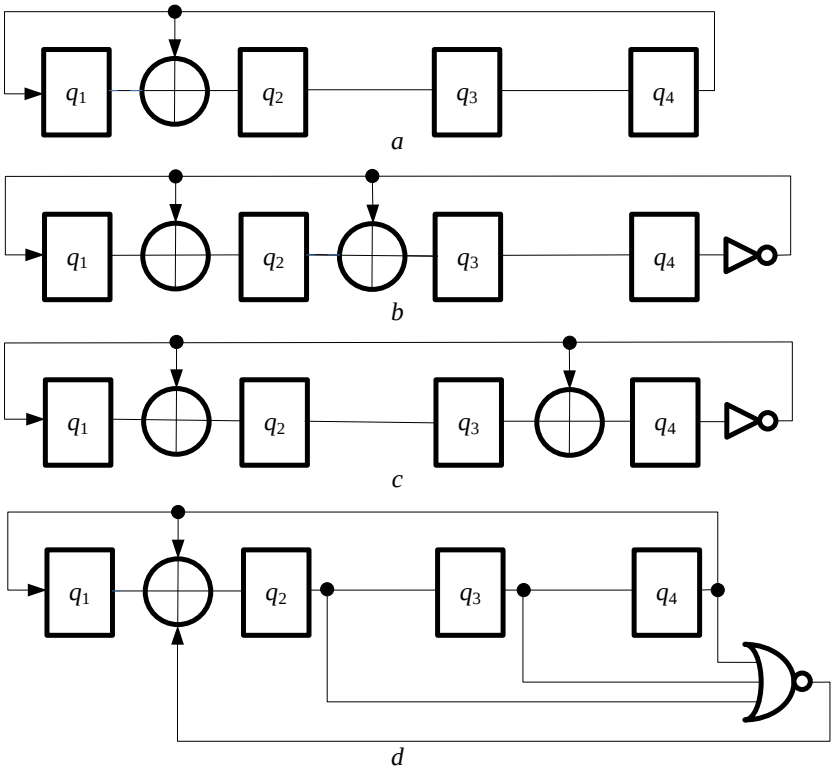


Рис. 1. Четырехразрядные ГПСЧ: a – генератор M-последовательности; b – генератор (M – 1)-последовательности; c – генератор (M – 3)-последовательности; d – генератор (M + 1)-последовательности. $M = 2^N - 1$

Fig. 1. 4-bit PRNG: a – M-sequence generator; b – (M – 1)-sequence generator; c – (M – 3)-sequence generator; d – (M + 1)-sequence generator. $M = 2^N - 1$

На рис. 1,*a* приведена схема генератора *M*-последовательности, построенного по схеме Галуа, соответствующего характеристическому многочлену $\varphi(x) = x^4 + x + 1$, примитивному над полем Галуа GF(2). Диаграмма переключений устройства имеет вид 15-1, иначе говоря, состоит из двух кодовых колец, одно длиной 15 включает в себя все ненулевые состояния генератора, второе длиной 1 включает состояние «все нули», переходящее само в себя. Уравнения работы генератора имеют вид:

$$q_1(t + 1) = q_4(t),$$
$$q_2(t + 1) = q_1(t) \oplus q_4(t),$$
$$q_3(t + 1) = q_2(t),$$
$$q_4(t + 1) = q_3(t),$$

где $\oplus$ - операция сложения по модулю два, $q_i(t)$ и $q_i(t + 1)$ – содержимое i-го разряда генератора соответственно в моменты времени t и $(t + 1)$, $i = 1, 2, 3, 4$.

На рис. 1,*b* приведен генератор $(M – 1)$-последовательности, построенный на основе генератора Галуа, соответствующего характеристическому многочлену $\varphi(x) = (x + 1)(x^3 + x^2 + 1) = x^4 + x^2 + x + 1$, где $\lambda_1(x) = x^3 + x^2 + 1$ – примитивный над полем GF(2). Диаграмма переключений генератора имеет вид 14-2, при этом при корректной работе устройства свертка по модулю два состояния элементов памяти генератора в

каждом такте меняет свое значение на противоположное. Уравнения работы устройства имеют вид:

$$q_1(t+1) = q_4(t) \oplus 1,$$
$$q_2(t+1) = q_1(t) \oplus q_4(t) \oplus 1,$$
$$q_3(t+1) = q_2(t) \oplus q_4(t) \oplus 1,$$
$$q_4(t+1) = q_3(t).$$

В общем случае при разрядности генератора, равной N, диаграмма переключений генератора $(M-1)$-последовательности имеет вид $(2^N - 2) - 2$.

На рис. 1,*c* приведен генератор $(M-3)$-последовательности, построенный на основе генератора Галуа, соответствующего характеристическому многочлену $\varphi(x) = (x+1)^2(x^2+x+1) = x^4 + x^3 + x + 1$, где $\lambda_2(x) = x^2 + x + 1$ – примитивный над полем GF(2). Диаграмма переключений генератора имеет вид 12-4, при этом при корректной работе устройства в этом режиме свертка по модулю два состояния элементов памяти генератора в каждом такте также меняет свое значение на противоположное. Уравнения работы устройства имеют вид:

$$q_1(t+1) = q_4(t) \oplus 1,$$
$$q_2(t+1) = q_1(t) \oplus q_4(t) \oplus 1,$$
$$q_3(t+1) = q_2(t),$$
$$q_4(t+1) = q_3(t) \oplus q_4(t) \oplus 1.$$

В общем случае при разрядности генератора, равной N, диаграмма переключений генератора $(M-3)$-последовательности имеет вид $(2^N - 4) - 4$.

Термины $(M-1)$-последовательность и $(M-3)$-последовательность были введены в [11].

На рис. 1,*d* приведена каноническая схема генератора $(M+1)$-последовательности, построенного на основе устройства, показанного на рис. 1,*a*. Диаграмма переключений генератора состоит из одного кодового кольца длиной 16. Когда устройство оказывается в состоянии 1000, единичный сигнал на выходе элемента ИЛИ-НЕ обеспечивает переключение устройства в ранее запрещенное состояние 0000. Сигнал на выходе элемента ИЛИ-НЕ по-прежнему равен единице, поэтому в следующем такте устройство возвращается обратно в основной цикл, переходя в состояние 0100. Уравнения работы генератора имеют вид:

$$q_1(t+1) = q_4(t),$$
$$q_2(t+1) = q_1(t) \oplus q_4(t) \oplus z,$$
$$q_3(t+1) = q_2(t),$$
$$q_4(t+1) = q_3(t),$$

где z – сигнал на выходе элемента ИЛИ-НЕ,

$$z = \begin{cases} 1, & \text{если } q_2 q_3 q_4 = 000, \\ 0, & \text{в противном случае.} \end{cases}$$

2. Шифрование логики

Рассмотрим базовую идею технологии Logic Encryption. Шифрование логической схемы цифрового устройства (рис. 2,*a*) дает возможность использовать дополнительные логические элементы в структуре ИС, чтобы скрыть ее оригинальные функциональные возможности. Иначе говоря, это попытка максимально усложнить понимание логики работы защищаемой схемы для неавторизованных лиц. Шифрование логической схемы (по сути ее обфускация) меняет конструкцию ИС таким образом, что она работает правильно, только в том случае, если сигналы на дополнительных ключевых входах устройства принимают правильные значения. Схема обфускации предполагает использование дополнительной схемы преобразования ключей, реализованной на основе

блока памяти с защитой от НСД. Этот блок памяти устанавливается или активируется на заключительном этапе создания ИС перед ее продажей конечному потребителю.

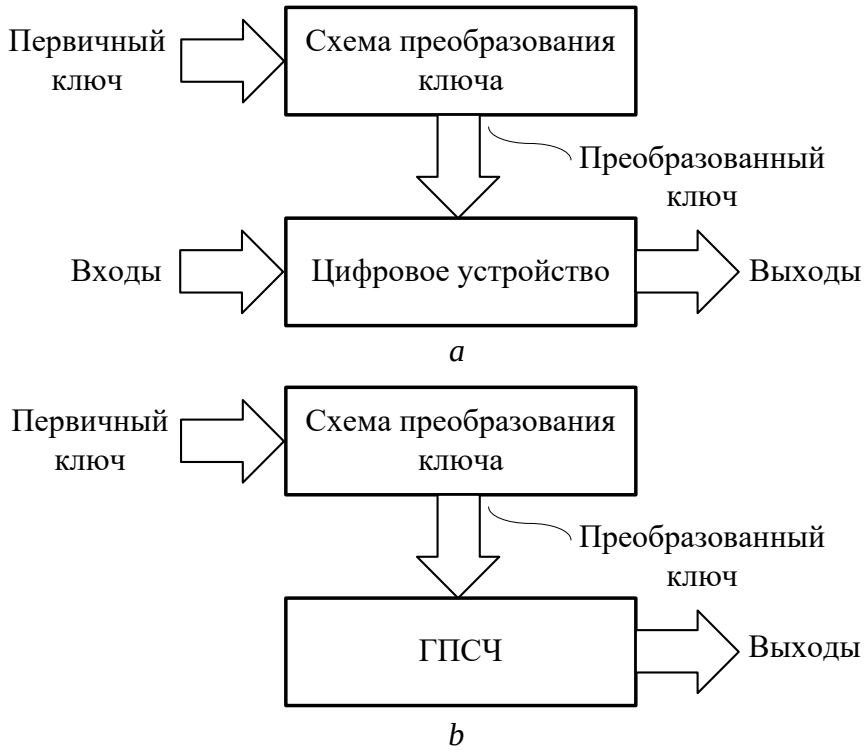


Рис. 2. Шифрование логической схемы цифрового устройства: a – общая схема; b – реализация идеи для ГПСЧ
Fig. 2. Logic encryption in the digital device design: a – a general logic encryption scheme; b – the general design scheme for PRNG

3. Шифрование логической схемы ГПСЧ

На рис. 2,*b* приведен пример реализации этой идеи, когда защищаемое от реверс-инжиниринга устройство – это ГПСЧ. На рис. 3 показан простейший пример шифрования схемы четырехразрядного генератора, построенного с использованием конструкции Галуа. В зависимости от значений на ключевых входах k_1k_0 устройство реализует одну из четырех диаграмм переключений, приведенных в табл. 1.

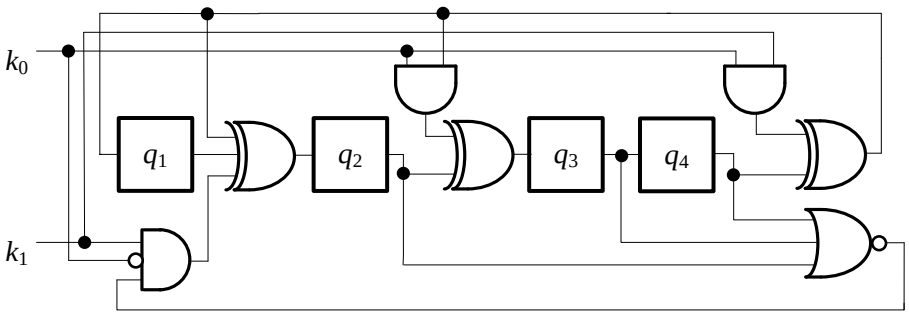


Рис. 3. Простейший пример шифрования логической схемы двоичного четырехразрядного ГПСЧ. Выходами генератора являются выходы разрядов q_1, q_2, q_3, q_4
Fig. 3. A simple logic encryption design of binary 4-bit PRNG. q_1, q_2, q_3, q_4 – generator outputs

Таблица 1. Зависимость диаграммы переключений устройства от значения ключа k_1k_0

Режим	Ключ	Диаграмма переключений
0	0 0	Два цикла длиной 15 и 1
1	0 1	Четыре цикла длиной 7, 7, 1 и 1
2	1 0	Один цикл длиной 16
3	1 1	Два цикла длиной 14 и 2

На рис. 4 приведен еще один пример реализации шифрования логической схемы с использованием схемы преобразования ключей, реализованной на основе блока замены – классического криптографического примитива. В зависимости от значений на первичных ключевых входах $K_3K_2K_1K_0$ устройство функционирует в одном из 16-ти возможных режимов, некоторые из которых приведенных в табл. 2.

Таблица 2. Зависимость диаграммы переключений устройства от значения Primary Key

$K_3\,K_2\,K_1\,K_0$	$k_4\,k_3\,k_2\,k_1\,k_0$	Диаграмма переключений
0 0 0 0	0 0 0 0 1	Два цикла длиной 15 и 1
0 0 0 1	0 0 1 0 0	Два цикла длиной 15 и 1
0 0 1 0	0 0 0 1 1	Четыре цикла длиной 7, 7, 1 и 1
0 0 1 1	0 0 1 1 0	Четыре цикла длиной 7, 7, 1 и 1
0 1 0 0	1 0 0 0 1	Один цикл длиной 16
0 1 0 1	0 0 1 1 1	Четыре цикла длиной 5, 5, 5 и 1
0 1 1 0	0 1 1 1 0	Два цикла длиной 14 и 2
0 1 1 1	0 1 0 1 1	Два цикла длиной 14 и 2
1 0 0 0	0 1 0 0 1	Два цикла длиной 15 и 1
1 0 0 1	0 1 1 0 0	Два цикла длиной 15 и 1
1 0 1 0	0 1 1 0 1	Два цикла длиной 12 и 4
...		

4. Моделирование зашифрованной схемы ГПСЧ

На рис. 5 приведена более сложная схема зашифрованного четырехразрядного PRNG с девятью ключевыми входами, а значит способная выполнять 2^9 различных функций, среди которых 32 варианта генераторов M-последовательностей, 16 вариантов генераторов (M – 1)-последовательностей, 8 вариантов генераторов (M – 3)-последовательностей. Была разработана программа, которая перебирала двоичные наборы на входах $k_8\ k_7\ k_6\ k_5\ k_4\ k_3\ k_2\ k_1\ k_0$ и определяла для каждого набора соответствующую периодическую структуру генератора. Моделирование работы устройства позволило выявить более десяти необычных режимов работы схемы, один из которых приведен на рис. 6. Схема интересна тем, что генератор дважды «сбивается с ритма», когда при $z = 1$ нарушается закон изменения значения свертки в каждом такте, который реализуется на остальной части диаграммы переключений. Таким образом, выявлена принципиальная

возможность модификации схемы генератора (M – 1)- последовательности и превращения ее в схему генератора (M + 1)- последовательности.

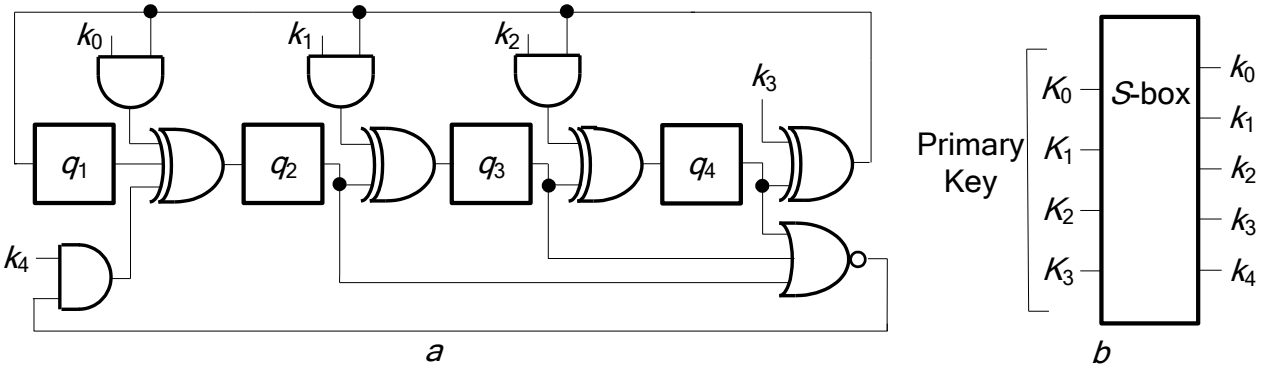


Рис. 4. Простейший пример шифрования логической схемы двоичного четырехразрядного генератора с использованием схемы преобразования ключа:
a – схема устройства с ключевыми входами;
b – схема преобразования ключа на основе блока замены (S-блока)
Fig. 4. A simple logic encryption design of 4-bit PRNG with key transformation scheme:
a – 4-bit PRNG with key inputs; b – key transformation scheme based on the use of S-box

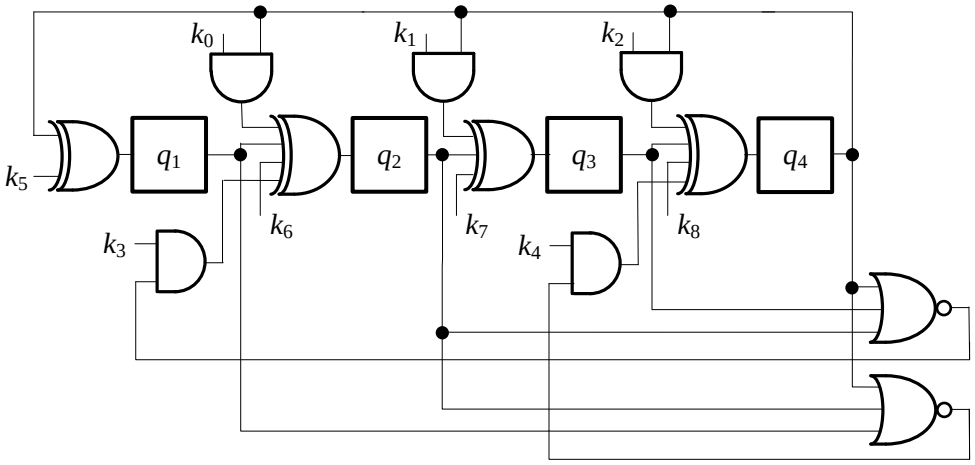


Рис. 5. Схема зашифрованного двоичного четырехразрядного ГПСЧ
Fig. 5. Encrypted binary 4-bit PRNG

На рис. 5 приведено устройство, построенное на базе генератора Галуа, соответствующего характеристическому многочлену $\varphi(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + 1$ над полем GF(2). Уравнения работы базового генератора имеют вид:

$$q_1(t + 1) = q_4(t) \oplus c_1,$$
$$q_2(t + 1) = q_1(t) \oplus a_1q_4(t) \oplus c_2,$$
$$q_3(t + 1) = q_2(t) \oplus a_2q_4(t) \oplus c_3,$$
$$q_4(t + 1) = q_3(t) \oplus a_3q_4(t) \oplus c_4,$$

где $a_i \in \{0, 1\}$– коэффициенты многочлена $\varphi(x)$, $c_i \in \{0, 1\}$– управляющие входы устройства. В общем случае при произвольной разрядности генератора, равной N, уравнения принимают вид:

$$q_1(t + 1) = q_N(t) \oplus c_1,$$

$$q_j(t+1) = q_{j-1}(t) \oplus a_{j-1}q_N(t) \oplus c_j,$$
$$j = 2, 3, \ldots, N.$$

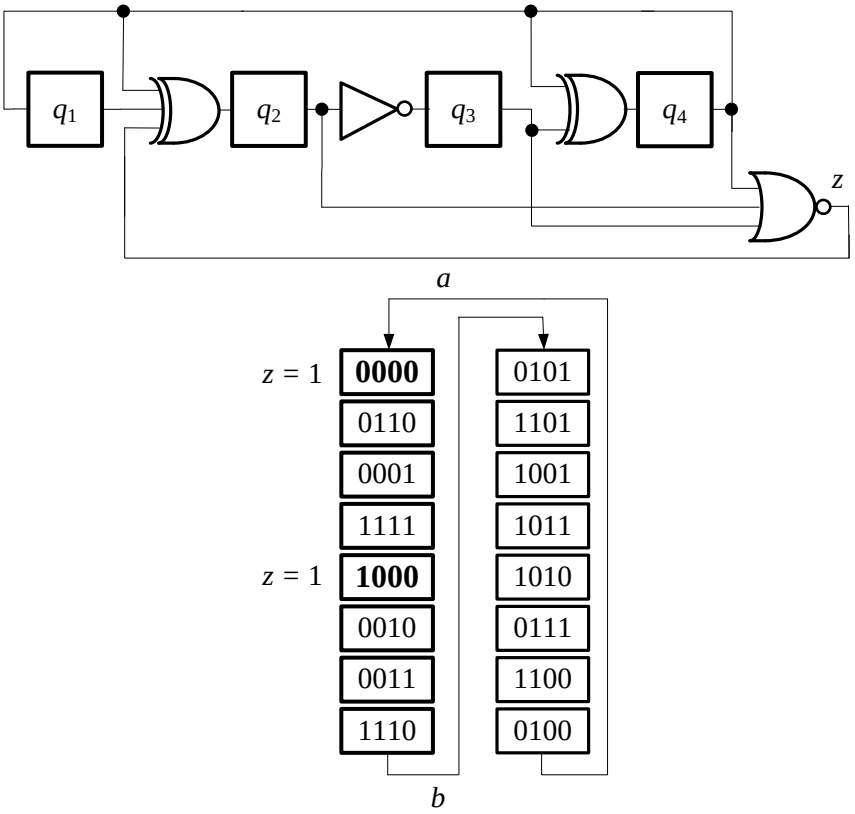


Рис. 6. Логика работы двоичного четырехразрядного генератора при $k_8\ k_7\ k_6\ k_5\ k_4\ k_3\ k_2\ k_1\ k_0 = 0\ 1\ 0\ 0\ 0\ 1\ 1\ 0\ 1$: a – эквивалентная схема устройства; b – диаграмма его переключений
Fig. 6. Generator operation logic at key value $k_8\ k_7\ k_6\ k_5\ k_4\ k_3\ k_2\ k_1\ k_0 = 0\ 1\ 0\ 0\ 0\ 1\ 1\ 0\ 1$: a – generator equivalent circuit; b – generator state transition graph

Заключение

Рассмотрены методы обфускации логических схем генераторов псевдослучайных чисел на регистрах сдвига с линейными и нелинейными обратными связями. Показано, что даже при небольшой разрядности генераторов можно обеспечить огромное количество вариантов реализации ГПСЧ с различным числом состояний и различными свойствами. Таким образом, обоснована эффективность технологии Logic Encryption применительно к защите от реверс-инжиниринга логической схемы ГПСЧ на регистрах сдвига с линейными обратными связями. Эффективность обусловлена тем, что с ростом разрядности генераторов возрастает число возможных характеристических многочленов максимального периода. В общем случае это число равно $M_2(N)$, где $\varphi(\cdot)$ – число Эйлера. Соответственно растет число возможных канонических вариантов схем генераторов $(M + 1)$-, M-, $(M - 1)$- и $(M - 3)$-последовательностей. В общем случае при разрядности генератора, равной N, эти числа равны

$$N_{M+1} > N_M,$$
$$N_M = \frac{2^N \varphi(2^N - 1)}{N}, N_{M-1} = \frac{2^{N-1} \varphi(2^{N-1} - 1)}{N - 1}, N_{M-3} = \frac{2^{N-1} \varphi(2^{N-2} - 1)}{N - 2}.$$

Таким образом, на практике применение идеи запутывания логической схемы устройства помимо решения вышеперечисленных проблем с вредоносным аппаратным обеспечением, подделками ИС, пиратством и несанкционированным перепроизводством позволяет реализовать механизм скрытых (особо защищенных) функций устройства, например, для защиты технического решения от использования по двойному назначению.

Генераторы рассмотренного класса активно используются для реализации минималистских (light-weight) алгоритмов защиты информации, в том числе криптографических. Области использования таких алгоритмов – RFID-технологии и Интернет вещей.

Дальнейшее развитие идеи запутывания схемы двоичного ГПСЧ может быть связано с увеличением числа генераторов (M + 1)-последовательностей, добавлением режимов генерации последовательностей с предпериодом, а также возможности построения генераторов, функционирующих в поле GF(2^n).

СПИСОК ЛИТЕРАТУРЫ:

1. Chakraborty R.S. and Bhunia S., HARPOON: An Obfuscation-Based SoC Design Methodology for Hardware Protection, in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. Vol. 28, no. 10. P. 1493–1502, Oct. 2009. DOI: http://dx.doi.org/10.1109/TCAD.2009.2028166.
2. Tehranipoor M. and Koushanfar F., A Survey of Hardware Trojan Taxonomy and Detection, in IEEE Design & Test of Computers. Vol. 27, no. 1. P. 10–25, Jan.-Feb. 2010. DOI: http://dx.doi.org/10.1109/MDT.2010.7.
3. Li L. and Zhou H., Structural transformation for best-possible obfuscation of sequential circuits, 2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), Austin, TX, 2013. P. 55–60, DOI: http://dx.doi.org/10.1109/HST.2013.6581566.
4. Baumgarten A., Tyagi A. and Zambreno J. Preventing IC Piracy Using Reconfigurable Logic Barriers, in IEEE Design & Test of Computers. Vol. 27, no. 1. P. 66–75, Jan.-Feb. 2010, DOI: http://dx.doi.org/10.1109/MDT.2010.24.
5. Chakraborty, Rajat Subhra: Hardware security through design obfuscation, Submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy.Thesis Adviser: Dr. Swarup Bhunia. Department of Electrical Engineering and Computer Science. Case Western Reserve University, May, 2010. URL:https://etd.ohiolink.edu/apexprod/rws_etd/send_file/send?accession=case1270133481&disposition=inline (дата обращения: 20.01.2021).
6. Becker G.T., Fyrbiak M., Kison C. (2017) Hardware Obfuscation: Techniques and Open Challenges. In: Bossuet L., Torres L. (eds) Foundations of Hardware IP Protection. Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-50380-6_6.
7. Ivanov M.A., Kliuchnikova B.V., Salikov E.A., Starikovskii A.V. (2020) New Class of Non-binary Pseudorandom Number Generators. In: Misyurin S., Arakelian V., Avetisyan A. (eds) Advanced Technologies in Robotics and Intelligent Systems. Mechanisms and Machine Science, vol 80. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-33491-8_35.
8. Dubrova E.A. Scalable Method for Constructing Galois NLFSRs with Period 2^n –1 using Cross-Join Pairs. Cryptology ePrint Archive, Report 2011/632, 2011. URL: http://eprint.iacr.org/2011/632 (дата обращения: 20.01.2021).
9. Dubrova E.A. Method for Generating Full Cycles by a Composition of NLFSRs. URL: https://eprint.iacr.org/2012/492.pdf (дата обращения: 20.01.2021).
10. Dubrova E., Teslenko M. and Tenhunen H. 2008. On analysis and synthesis of (n, k)-non-linear feedback shift registers. In Proceedings of the conference on Design, automation and test in Europe (DATE '08). Association for Computing Machinery, New York, NY, USA. P. 1286–1291. DOI: https://doi.org/10.1145/1403375.1403686 (дата обращения: 20.01.2021).
11. Песошин В.А., Кузнецов В.М. Генераторы псевдослучайных и случайных чисел на регистрах сдвига. Казань: Изд-во Казанского гос. техн. ун-та, 2007. URL: https://elibrary.ru/item.asp?id=19590566 (дата обращения: 20.01.2021).
12. Кузнецов В.М., Песошин В.А. Генераторы равновероятностных псевдослучайных последовательностей на регистрах сдвига. Известия высших учебных заведений. Поволжский регион. Технические науки. 2012, № 1. С. 21–28. URL: https://elibrary.ru/item.asp?id=17893013 (дата обращения: 20.01.2021).
13. Кузнецов В.М., Песошин В.А. Генераторы случайных и псевдослучайных последовательностей на цифровых элементах задержки. Казань: Изд-во Казанского гос. техн. ун-та, 2013. – 336 с. URL: https://elibrary.ru/item.asp?id=32597446 (дата обращения: 20.01.2021).

14. Pesoshin, V.A., Kuznetsov, V.M. & Shirshova, D.V. Generators of the equiprobable pseudorandom nonmaximal-length sequences based on linear-feedback shift registers. Autom Remote Control 77, 1622–1632 (2016). DOI: https://doi.org/10.1134/S0005117916090095.

REFERENCES:

[1] Chakraborty R.S. and Bhunia S., HARPOON: An Obfuscation-Based SoC Design Methodology for Hardware Protection, in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. Vol. 28, no. 10. P. 1493–1502, Oct. 2009. DOI: http://dx.doi.org/10.1109/TCAD.2009.2028166.

[2] Tehranipoor M. and Koushanfar F., A Survey of Hardware Trojan Taxonomy and Detection, in IEEE Design & Test of Computers. Vol. 27, no. 1. P. 10–25, Jan.-Feb. 2010, DOI: http://dx.doi.org/10.1109/MDT.2010.7.

[3] Li L. and Zhou H., Structural transformation for best-possible obfuscation of sequential circuits, 2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), Austin, TX, 2013. P. 55–60, DOI: http://dx.doi.org/10.1109/HST.2013.6581566.

[4] Baumgarten A., Tyagi A. and Zambreno J. Preventing IC Piracy Using Reconfigurable Logic Barriers, in IEEE Design & Test of Computers. Vol. 27, no. 1. P. 66–75, Jan.-Feb. 2010. DOI: http://dx.doi.org/10.1109/MDT.2010.24.

[5] Chakraborty, Rajat Subhra: Hardware security through design obfuscation, Submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy.Thesis Adviser: Dr. Swarup Bhunia. Department of Electrical Engineering and Computer Science. Case Western Reserve University, May, 2010. URL:https://etd.ohiolink.edu/apexprod/rws_etd/send_file/send?accession=case1270133481&disposition=inline (accessed: 20.01.2021).

[6] Becker G.T., Fyrbiak M., Kison C. (2017) Hardware Obfuscation: Techniques and Open Challenges. In: Bossuet L., Torres L. (eds) Foundations of Hardware IP Protection. Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-50380-6_6.

[7] Ivanov M.A., Kliuchnikova B.V., Salikov E.A., Starikovskii A.V. (2020) New Class of Non-binary Pseudorandom Number Generators. In: Misyurin S., Arakelian V., Avetisyan A. (eds) Advanced Technologies in Robotics and Intelligent Systems. Mechanisms and Machine Science, vol 80. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-33491-8_35.

[8] Dubrova E.A. Scalable Method for Constructing Galois NLFSRs with Period 2^n –1 using Cross-Join Pairs. Cryptology ePrint Archive, Report 2011/632, 2011. URL: http://eprint.iacr.org/2011/632 (accessed: 20.01.2021).

[9] Dubrova E.A. Method for Generating Full Cycles by a Composition of NLFSRs. https://eprint.iacr.org/2012/492.pdf (accessed: 20.01.2021).

[10] Dubrova E., Teslenko M. and Tenhunen H. 2008. On analysis and synthesis of (n, k)-non-linear feedback shift registers. In Proceedings of the conference on Design, automation and test in Europe (DATE '08). Association for Computing Machinery, New York, NY, USA. P. 1286–1291. DOI: https://doi.org/10.1145/1403375.1403686 (accessed: 20.01.2021).

[11] Pesoshin V.A., Kuznecov V.M. Generatory psevdosluchajnyh i sluchajnyh chisel na registrah sdviga. Kazan: Izd-vo Kazanskogo gos. tehn. un-ta, 2007. URL: https://elibrary.ru/item.asp?id=19590566 (accessed: 20.01.2021) (in Russian).

[12] Kuznecov V.M., Pesoshin V.A. Generatori ravnoveroyatnostnih psevdosluchainih posledovatelnostei na registrah sdviga. Izvestiya visshih uchebnih zavedenii. Povoljskii region. Tehnicheskie nauki. 2012, no. 1. P. 21–28. URL: https://elibrary.ru/item.asp?id=17893013 (accessed: 20.01.2021) (in Russian).

[13] Kuznecov V.M., Pesoshin V.A. Generatori sluchainih i psevdosluchainih posledovatelnostei na cifrovih elementah zaderjki. Kazan: Izd-vo Kazanskogo gos. tehn. un-ta, 2013. – 336 s. URL: https://elibrary.ru/item.asp?id=32597446 (accessed: 20.01.2021) (in Russian).

[14] Pesoshin, V.A., Kuznetsov, V.M. & Shirshova, D.V. Generators of the equiprobable pseudorandom nonmaximal-length sequences based on linear-feedback shift registers. Autom Remote Control 77, 1622–1632 (2016). DOI: https://doi.org/10.1134/S0005117916090095.

Поступила в редакцию – 25 января 2021 г. Окончательный вариант – 01 февраля 2021 г.
Received – January 25, 2021. The final version – February 01, 2021.

Сергей В. Скрыль[1], Виктор В. Гайфулин[2], Дмитрий В. Домрачев[3],
Владимир М. Сычев[4], Юлия В. Грачёва[5]

[1,4,5]Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)» (МГТУ им. Н.Э. Баумана), ул. 2-я Бауманская, 5, Москва, 105005, Россия

[2,3]Федеральное государственное казенное военное образовательное учреждение высшего образования «Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С.М. Штеменко» Министерства обороны, ул. Красина, 4, Краснодар, 350063, Россия

[1]e-mail: skryl@bmstu.ru, https://orcid.org/0000-0002-4309-6255

[2]e-mail: Gayfulin2007@yandex.ru, https://orcid.org/0000-0001-6026-5885

[3]e-mail: dobryi01@list.ru, https://orcid.org/0000-0002-0443-8304

[4]e-mail: dviu@mail.ru, https://orcid.org/0000-0002-2372-8980

[5]y.v.gracheva@yandex.ru, https://orcid.org/0000-0003-0884-5617

АКТУАЛЬНЫЕ ВОПРОСЫ ПРОБЛЕМАТИКИ ОЦЕНКИ УГРОЗ КОМПЬЮТЕРНЫХ АТАК НА ИНФОРМАЦИОННЫЕ РЕСУРСЫ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

DOI: http://dx.doi.org/10.26583/bit.2021.1.07

Аннотация. Статья посвящена анализу возможностей существующего методического аппарата определения актуальных угроз безопасности информации по оценке киберустойчивости значимых объектов критической информационной инфраструктуры (ЗО КИИ). В статье обосновывается актуальность вопросов повышения эффективности механизмов защиты информационных ресурсов этих объектов от компьютерных атак как предпосылки обеспечения их киберустойчивости. Даются определения данного понятия. Подробно анализируются существующие методики вероятностной оценки актуальных угроз безопасности информации на примере оценки уровня угрозы компьютерной атаки на информационные ресурсы ЗО КИИ. Приводятся принципиальные недостатки этих методик – эмпирический характер оценки, отсутствие учета тех случайных состояний угроз безопасности информации, которые характеризуют их динамику, а также ограниченное число случайных событий, в тех моделях, которые учитывают динамику возникновения и реализации угроз безопасности информации. Анализируются обстоятельства, не позволяющие характеризовать существующий уровень проработки методов оценки эффективности защиты информации от несанкционированного доступа (НСД), как достаточный для адекватной характеристики киберустойчивости. Приводятся основания, указывающие на необходимость адекватной оценки эффективности защиты информационных ресурсов ЗО КИИ от компьютерных атак как предпосылки обоснованности требований к мерам обеспечения киберустойчивости этих объектов. Обосновываются направления преодоления недостатков существующих методик оценки эффективности защиты информации от НСД.

Ключевые слова: компьютерная атака, значимые объекты критической информационной инфраструктуры, киберустойчивость, оценки угроз компьютерных атак.

Для цитирования: СКРЫЛЬ, Сергей В. и др. АКТУАЛЬНЫЕ ВОПРОСЫ ПРОБЛЕМАТИКИ ОЦЕНКИ УГРОЗ КОМПЬЮТЕРНЫХ АТАК НА ИНФОРМАЦИОННЫЕ РЕСУРСЫ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ. Безопасность информационных технологий, [S.l.], v. 28, n. 1, p. 84–94, jan. 2021. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1323>. Дата доступа: 05 feb. 2021. DOI: http://dx.doi.org/10.26583/bit.2021.1.07.

Sergey V. Skryl'[1], Victor V. Gaifulin[2], Dmitry V. Domrachev[3],
Vladimir M. Sychev[4], Yulia V. Gracheva[5]
[1,4,5]Federal State Educational Institution of Higher Education
«Bauman Moscow State Technical University»,
2nd Bauman str., 5, Moscow, 105005, Russia
[2,3]Federal State Government Military Educational Establishment education
«Krasnodar Higher Military awarded by the Order of Zhukov and by the Orders of October Revolution and the Red Banner School named after the general of the Army S.M. Shtemenko» of the Department of Defense of Russian Federation,
Krasina str., 4, Krasnodar, 350063, Russia
[1]e-mail: skryl@bmstu.ru, https://orcid.org/0000-0002-4309-6255
[2]e-mail: Gayfulin2007@yandex.ru, https://orcid.org/0000-0001-6026-5885
[3]e-mail: dobryi01@list.ru, https://orcid.org/0000-0002-0443-8304
[4]e-mail: dviu@mail.ru, https://orcid.org/0000-0002-2372-8980
[5]y.v.gracheva@yandex.ru, https://orcid.org/0000-0003-0884-5617

Topical issues of the problem of assessment of threats of cyber attacks on information resources of significant facilities of critical information infrastructure

DOI: http://dx.doi.org/10.26583/bit.2021.1.07

Annotation: This paper opens a series of studies devoted to the problems of assessing the characteristics of measures to ensure the cyber resilience of information resources of critical information infrastructure objects. The paper substantiates the relevance of issues of increasing the efficiency of mechanisms for detecting, preventing and eliminating the consequences of computer attacks on the information resources of critical information infrastructure objects as a prerequisite for ensuring the cyber stability of these objects. A detailed analysis of the methodological apparatus of probabilistic assessment of the relevance of threats to information security is provided, the provisions of which are reflected in the regulatory and methodological documents of the FSTEC of Russia. The circumstances that do not allow characterizing the existing level of development of mathematical methods in the field of information protection against unauthorized access as high are analyzed. The necessity of solving the problems of adequate assessment of the effectiveness of mechanisms for detecting, preventing and eliminating the consequences of computer attacks on the information resources of critical information infrastructure objects is substantiated as a prerequisite for substantiating the requirements for measures to ensure the cyber stability of these segments.
Keywords: computer attack, critical information infrastructure objects, cyber stability of critical information infrastructure objects, the effectiveness of mechanisms for detecting, preventing and eliminating the consequences of computer attacks on information resources of critical information infrastructure objects, assessment of current threats to information security.
For citation: SKRYL', Sergey V. et al. Topical issues of the problem of assessment of threats of cyber attacks on information resources of significant facilities of critical information infrastructure. IT Security (Russia), [S.l.], v. 28, n. 1, p. 84–94, jan. 2021. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1323>. Date accessed: 05 feb. 2021. DOI: http://dx.doi.org/10.26583/bit.2021.1.07.

Введение

Анализ перспектив развития теории и практики построения инфокоммуникационной среды [1] позволяет выявить устойчивую тенденцию расширения возможностей распределенной обработки данных [2] за счет совершенствования механизма теледоступа в информационной инфраструктуре.

Вместе с тем подобная тенденция, как позитивная, влечет за собой и ряд негативных факторов, наиболее серьезным из которых выступают объективно существующие уязвимости объектов информационной инфраструктуры для информационно-технического воздействия (ИТВ) [3]. Реализация нарушителем такого рода воздействия приводит к снижению эффективности информационных технологий, реализуемых этими объектами,

что, в свою очередь, приводит к ущербу в тех областях, в интересах которых они функционируют. Если такой ущерб существенный, то соответствующую информационную инфраструктуру относят к критической[1] [4].

Исходя из анализа состояния информационной безопасности и национальных приоритетов Российской Федерации в Доктрине информационной безопасности одним из основных направлений обеспечения информационной безопасности определено «повышение защищенности критической информационной инфраструктуры и устойчивости ее функционирования, развитие механизмов обнаружения и предупреждения информационных угроз и ликвидации последствий их проявления, вызванных информационно-техническим воздействием на объекты критической информационной инфраструктуры»[2].

1. Киберустойчивость значимых объектов критической информационной инфраструктуры как объект исследования

Характерным для значимых объектов критической информационной инфраструктуры (ЗО КИИ) типом ИТВ являются компьютерные атаки, которые представляют собой целенаправленное несанкционированное воздействие на информацию, на ресурс автоматизированной информационной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств[3]. Следует отметить, что для объектов ЗО КИИ наряду с термином «компьютерная атака» часто применяется эквивалентный по смыслу термин «кибератака» [5]. Это послужило основанием для использования термина «киберустойчивость» для характеристики устойчивости функционирования этих систем в условиях кибератак. Несмотря на усиленную в последнее время эксплуатацию данного термина, включая использование его в официальных документах, официальной трактовки данного понятия не существует. Среди многочисленных авторских определений наиболее обоснованным можно считать определение, приводимое в [6]: «под киберустойчивостью понимается способность информационно-телекоммуникационной сети поддерживать управление в условиях воздействия компьютерных атак» и приводимое в [7]: «киберустойчивость – это свойство информационной системы, позволяющее ей существовать в условиях постоянных атак»

Среди зарубежных трактовок данного понятия следует выделить определение киберустойчивости, используемое IBM: «киберустойчивость – это выравнивание возможностей по предотвращению, обнаружению и реагированию для управления, смягчения и ухода от кибератак».

Понимание свойства киберустойчивости позволяет поменять отношение к компьютерным атакам и усвоить крайне важное обстоятельство, что защититься от всех атак нельзя. Необходимо проектировать информационную систему как киберустойчивую. От этого и строится стратегия обеспечения киберустойчивости.

Указанное требование позиционирует механизмы обеспечения киберустойчивости ЗО КИИ в качестве базовых для государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

[1]Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
[2]Доктрина информационной безопасности Российской Федерации, утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646. Российская газета, 2016.
[3]ГОСТ Р 51275-2006: Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

Касаясь направлений совершенствования данной системы, обозначенных в Указе Президента РФ «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»[4], одной из важнейших задач является «осуществление контроля степени защищенности информационных ресурсов Российской Федерации от компьютерных атак».

Решение данной задачи напрямую связано с решением проблемы адекватной оценки механизмов обеспечения киберустойчивости ЗО КИИ. Вместе с тем высокая технологическая сложность этих механизмов относит вопросы их исследования, с целью обоснования направлений совершенствования, к числу сложных как в научном, так и в практическом плане. В свою очередь всесторонний и системный характер [8] подобных исследований достигается адекватностью оценки [9] возможностей механизмов обеспечения киберустойчивости ЗО КИИ по реализации функций обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы этих объектов.

В соответствии с системным подходом, исследование механизмов обеспечения киберустойчивости в рамках такой довольно специфичной области, как информационная среда ЗО КИИ, связано с решением проблемы оценки их возможностей по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные ресурсы с достаточной степенью адекватности для обоснованности решений о направлениях совершенствования этих механизмов. В соответствии с положениями статьи 12 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»[5] выработка мер по повышению устойчивости функционирования ЗО КИИ осуществляется на основе оценки ее безопасности.

Поэтому крайне актуальной проблемой является повышение адекватности существующих методик оценки эффективности мер защиты информации для обоснованности решений о направлениях совершенствования процессов обнаружения, предупреждения и ликвидации последствий компьютерных атак на их информационные ресурсы объектов ЗО КИИ.

Касаясь принципиальных вопросов выбора методов исследования, следует учитывать характерную особенность ЗО КИИ, относящихся к системам, для исследования которых, вследствие существенного ущерба от риска нарушения безопасности исследуемых информационных процессов, не могут быть применены натурные эксперименты. Это обусловливает необходимость использования математического моделирования в качестве методологического аппарата для исследования вопросов обеспечения киберустойчивости таких объектов [10].

[4]Указ Президента РФ от 22 декабря 2017 № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

[5]Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

2. Возможности существующего методического аппарата определения актуальных угроз безопасности информации по оценке уровня угрозы компьютерной атаки

Официальными методиками, регламентирующими процедуру оценки защищенности информации, являются методики вероятностной оценки актуальных угроз безопасности информации, приводимые в ряде нормативно-методических документов ФСТЭК России. В основу этих методик положена экспертиза факторов, способствующих возникновению угроз безопасности информации.

Проанализируем возможность использования этих методик для оценки уровня угрозы компьютерной атаки на информационные ресурсы значимого объекта КИИ.

В соответствии с положениями рассматриваемых методик отнесение факторов, способствующих возникновению угроз компьютерных атак, осуществляется путем установления, на основе эмпирического опыта, соответствия между такого рода источниками и их признаками. В результате формируется множество $\{a_k\}$, $k = 1, 2, \ldots, |\{a_k\}|$, элементы которого являются признаками источников угроз, а индексы – их номерами.

Для ЗО КИИ источниками угроз компьютерных атак являются:

$k = 1$ – иностранные спецслужбы;

$k = 2$ – криминальные структуры;

$k = 3$ – конкурирующие организации;

$k = 4$ – персонал объекта;

$k = 5$ – производители оборудования и организации, осуществляющие ремонт и обслуживание средств вычислительной техники (СВТ) и периферийного оборудования объекта;

a_1 – наличие интереса у иностранных спецслужб к информационным ресурсам объекта;

a_2 – наличие интереса у криминальных структур к информационным ресурсам объекта;

a_3 – наличие интереса представителей промышленно-деловой и финансово-кредитной среды, конкурирующих с промышленными и финансовыми организациями, использующих информационные ресурсы объекта;

a_4 – самостоятельное проведение должностными лицами объекта обслуживания СВТ и периферийного оборудования;

a_5 – использование несертифицированного программного обеспечения (ПО) при техническом обслуживании и ремонтно-восстановительных работах на объекте.

Особенностью выявления уязвимостей информационных ресурсов значимого объекта КИИ, через которые возможна реализация угроз компьютерных атак, является использование расчетных методик, позволяющих установить факт потенциальной возможности угрозы.

При определении уязвимостей информационных ресурсов объекта к реализации угроз компьютерных атак проводится экспертный анализ информационной среды объекта. В результате формируется множество $\{b_l\}$, $l = 1, 2, \ldots, L$, элементы которого определяют уязвимости. При этом индексы соответствуют номерам уязвимостей из их перечня.

В случае оценки уровня угрозы компьютерной атаки на информационные ресурсы объекта уязвимыми для такого рода угроз являются:

b_1 – драйверы средств ввода информации;

b_2 – драйверы средств отображения информации;

b_3 – драйверы средств обработки информации;

b_4 – драйверы микросхем BIOS;

b_5 – ПО серверов с открытым физическим доступом;
b_6 – ПО коммуникационного оборудования объекта;
b_7 – стек протоколов TCP/IP;
b_8 – шлюз выхода в Internet;
b_9 – протоколы межсетевого взаимодействия прикладного уровня;
b_{10} – недокументированные точки межсетевого взаимодействия;
b_{11} – открытые общие сетевые ресурсы;
b_{12} – несертифицированные компоненты ПО;
b_{13} – электронная почта;
b_{14} – Web-браузер;
b_{15} – кабели оборудования объекта на участках, где к ним имеется физический доступ.

Для количественной оценки уязвимости, через которую возможна реализация компьютерной атаки на информационные ресурсы значимого объекта КИИ, определяется вероятностью наличия соответствующих благоприятных условий. Данная вероятность оценивается экспертно специалистами в области кибербезопасности. Результаты оценки представляются лингвистическими значениями: «да», «вероятно», «возможно», «маловероятно» и «нет», характеризующими возможности использования k-м источником угрозы компьютерной атаки l-ой уязвимости. Каждому из пяти лингвистических значений ставится в соответствие вероятность p_{kl} использования k-м источником l-ой уязвимости. На основании данной вероятности определяется вероятность P_l использования l-й уязвимости (l = 1, 2, …, 15) возможными пятью источниками угроз:

$$P_l = 1 - (\gamma_{1}\cdot(1 - p_{l1})\cdot\gamma_{2}\cdot(1 - p_{l2})\cdot\gamma_{3}\cdot(1 - p_{l3})\cdot\gamma_{4}\cdot(1 - p_{l4})\cdot\gamma_{5}\cdot(1 - p_{l5})), \quad (1)$$

где γ_{lk} – коэффициент соответствия, равный 1, если l-я уязвимость соответствует k-му источнику и 0, если не соответствует.

Это позволяет сформировать множество $\{u_m\}$, m = 1, 2, …, M, угроз компьютерных атак [11]:

u_1 – загрузка вредоносного ПО с функциями альтернативной ОС с расширенными полномочиями;
u_2 – несанкционированное копирование информации;
u_3 – несанкционированная модификация информации;
u_4 – внедрение ложного доверенного объекта;
u_5 – подмена системного ПО;
u_6 – перенаправление сетевого трафика;
u_7 – манипулирование данными в удаленном режиме;
u_8 – вскрытие электронного почтового ящика;
u_9 – блокирование электронного почтового ящика;
u_{10} – подмена Web-браузеров;
u_{11} – использование ошибок в алгоритмах прикладного ПО;
u_{12} – блокирование хоста пользователя;
u_{13} – блокирования маршрутизатора;
u_{14} – обход межсетевого экрана.

Количественной характеристикой уровня m-ой угрозы компьютерной атаки, где m = 1, 2, …, 14, на информационные ресурсы ЗО КИИ является вероятность:

$$P_m^{(Y)} = 1 - \prod(1 - \alpha_{lm} \cdot P_l), \quad (2)$$

где P_l – соответствует выражению (1);

α_{lm} – коэффициент актуальности уязвимостей информации объекта для инициализации угроз компьютерных атак, равный 1, если *l*-я уязвимость актуальна для инициализации *m*-ой угрозы и 0, если не актуальна.

Значения коэффициента актуальности уязвимостей информации ЗО КИИ для инициализации угроз компьютерных атак приводятся в табл. 1.

Количественной характеристикой деструктивного воздействия компьютерных атак на информационные ресурсы ЗО КИИ является вероятность:

$$P_m^{(Д)} = 1 - \prod(1 - \delta_{mn} \cdot P_m^{(У)}), \quad (3)$$

где $P_m^{(У)}$ – соответствует выражению (2);

n – номер деструкции (1 – несанкционированное копирование информации, 2 – ее несанкционированная модификация, 3 – блокирование доступа к информационным ресурсам объекта);

δ_{mn} – коэффициент деструкции, равный 1, если *m*-я угроза реализует *n*-ю деструкцию и 0, если не реализует.

Значения коэффициента деструкции угроз компьютерных атак на информационные ресурсы ЗО КИИ приводятся в табл. 2. В таблице использованы следующие условные обозначения деструкций: *НК* – несанкционированное копирование информации, *НМ* – несанкционированная модификация информации, *БД* – блокирование доступа к информационным ресурсам.

Таблица 1. Значения коэффициента актуальности уязвимостей информации ЗО КИИ для инициализации угроз компьютерных атак

Угрозы компьютерных атак	**Уязвимости информационных ресурсов ЗО КИИ к реализации угроз компьютерных атак**														
	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8	b_9	b_{10}	b_{11}	b_{12}	b_{13}	b_{14}	b_{15}
u_1	1	0	0	0	1	1	0	0	0	0	0	1	1	1	1
u_2	0	0	0	0	1	0	0	1	1	1	1	1	1	1	1
u_3	1	1	1	0	1	0	0	1	1	1	1	1	1	1	1
u_4	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1
u_5	1	1	1	0	0	0	0	0	0	0	0	0	1	1	1
u_6	1	1	1	0	1	1	1	1	1	1	0	0	1	1	1
u_7	1	1	1	0	0	0	1	0	0	0	0	0	1	0	0
u_8	1	1	1	0	0	1	0	0	1	0	0	0	1	1	0
u_9	1	1	1	0	0	1	0	0	1	0	0	0	1	1	0
u_{10}	1	1	1	0	0	1	0	0	1	0	0	0	1	0	1
u_{11}	1	1	0	0	0	0	0	0	0	0	1	0	1	0	0
u_{12}	1	0	0	0	0	1	0	1	0	0	0	1	0	0	0
u_{13}	1	0	0	0	0	1	0	1	0	1	1	1	0	0	0
u_{14}	1	1	1	0	0	0	0	0	0	0	0	0	1	0	0

Таблица 2. Значения коэффициента деструкции угроз компьютерных атак на информационные ресурсы ЗО КИИ

Деструкции	**Угрозы компьютерных атак**													
	u_1	u_2	u_3	u_4	u_5	u_6	u_7	u_8	u_9	u_{10}	u_{11}	u_{12}	u_{13}	u_{14}
НК	1	1	0	1	0	0	1	1	0	1	1	0	0	1
НМ	1	0	1	1	1	1	1	0	0	1	1	0	0	1
БД	1	0	0	1	0	0	1	0	1	1	1	1	1	1

Из изложенного следует, что достоинством существующих методик оценки актуальных угроз безопасности информации является простота процедур оценки. К

недостаткам же, принципиально ограничивающих их использование для адекватной оценки мер обеспечения киберустойчивости ЗО КИИ, следует отнести отсутствие возможности учета динамики воздействия такого рода угроз, и низкая статистическая достоверность, характерная для экспертных оценок.

3. Обстоятельства, обусловливающие необходимость совершенствования методик оценки

Анализируя в целом существующий уровень проработки вопросов использования методов математического моделирования в проблематике защиты информации от компьютерных атак, можно выявить ряд обстоятельств, не позволяющих рассматривать применяемый аппарат математического моделирования как адекватный.

Первое обстоятельство связано с применением процедур оценки возможностей нарушителя, основанных на эмпирике. Характерным примером здесь является рассмотренная выше методика ФСТЭК России, регламентирующая порядок оценки актуальных угроз безопасности информации. Как показано в [12] и лингвистический характер оценки субъектно-объектных отношений между угрозами и порождающими их уязвимостями информации, и последующий переход к количественному представлению их вероятностных характеристик, основанные на экспертном подходе, привносят большую долю субъективизма в результаты оценки и, как следствие, являются причиной низкой адекватности используемых процедур оценки.

Второе обстоятельство связано с отсутствием учета тех случайных состояний угроз безопасности информации, которые характеризуют их динамику. В п. 5 «Определение вероятностей реализации угроз» нормативно методического документа ФСТЭК России, регламентирующего порядок оценки актуальных угроз безопасности информации, прямо указывается, что модели для определения вероятности угрозы в динамике ее возникновения и реализации в настоящее время отсутствуют.

Третье обстоятельство связано с ограниченным числом случайных событий, в тех моделях, которые учитывают динамику возникновения и реализации угроз безопасности информации. К таким моделям относятся модели, учитывающие лишь продолжительность угрозы, но не учитывающие случайные состояния, связанные с динамикой их возникновения [13, 14].

Преодоление указанных недостатков в проблематике оценки киберустойчивости ЗО КИИ возможно лишь в том случае, когда формальное описание угроз компьютерных атак на информационные ресурсы этих объектов позволяет математически представить все условия, характерные для динамики такого рода угроз.

Характеризуя в целом потенциал методологии компьютерной безопасности, следует отметить, что исследования в данной области позволили дать всестороннюю характеристику угроз НСД к компьютерной информации [6, 11, 15, 16]. Вместе с тем, применяемые в исследованиях методики не обладают той степенью системности, которая позволила бы в формализованном представлении исследуемых процессов учесть особенности динамики компьютерных атак.

Реализованные в рамках данных методик подходы к систематизации проявлений такого рода угроз носят субъективный характер и в крайне ограниченном виде отражают системные проявления субъектно-объектных отношений в процессах, характерных для данной предметной области, включая формальную интерпретацию динамики компьютерных атак. Исключение составляют приведенные в [17, 18] математические модели своевременности реагирования на компьютерные атаки, учитывающие не только длительность угрозы и реагирования на нее средствами защиты, но и моменты начала атаки

и ее обнаружения. Вместе с тем, наличие в этих моделях целого ряда ограничений, связанных с использованием стандартных математических абстракций, не позволило обеспечить ожидаемую степень адекватности.

Заключение

Возрастающие требования к обеспечению киберустойчивости ЗО КИИ в целом и требования к обоснованности характеристик процессов обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы этих объектов, в частности, ставят вопросы оценки угроз компьютерных атак в разряд актуальных и нуждающихся в проработке как в методическом, так и в прикладном плане.

СПИСОК ЛИТЕРАТУРЫ:

1. Величко В.В., Катунин Г.П., Шувалов В.П.; под ред. профессора Шувалова В.П. Основы инфокоммуникационных технологий: учебное пособие для вузов. М.: Горячая линия–Телеком, 2009. – 712 с.
2. Пятибратов А.П., Гудыно Л.П., Кириченко А.А. Вычислительные системы, сети и телекоммуникации: учебник. М.: Финансы и статистика, 2004. – 512 с.
3. Гриняев С.Н. Поле битвы – киберпространство. Теория, приемы, средства, методы и системы ведения информационной войны. М.: Харвест, 2004. – 426 с.
4. Гавдан, Григорий П., Иваненко, Виталий Г., Салкуцан, Алексей А. Обеспечение безопасности значимых объектов критической информационной инфраструктуры. Безопасность информационных технологий, [S.l.]. Т. 26, № 4. С. 69–82, дек. 2019. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1232 (дата обращения: 14.10.2020). DOI: http://dx.doi.org/10.26583/bit.2019.4.05.
5. Электронный словарь: сайт. URL: https://ru.wiktionary.org/wiki/кибератака (дата обращения: 14.10.2020).
6. Коцыняк М.А., Кулешов И.А., Кудрявцев А.М., Лаута О.С. Киберустойчивость информационно-телекоммуникационной сети / СПб.: Бостон-спектр, 2015. – 150 с.
7. Лукацкий А.В. Киберустойчивость, киберживучесть, кибернадежность, кибернепрерывность. URL: http://www.iksmedia.ru/blogs/post/5445277-Kiberustojchivost-kiberzhivuchest.html#ixzz6QU4Yn2yY (дата обращения: 14.10.2020).
8. Скрыль С.В., Шелупанов А.А. Основы системного анализа в защите информации: учебное пособие для студентов высших учебных заведений. М.: Машиностроение, 2008. – 138 с.
9. Скрыль С.В., Никулин С.С., Сычев А.М., Пономарёв М.В., Ле Ву Хыонг Занг. Показатели адекватности структурированных систем оценки характеристик информационных процессов. / Промышленные АСУ и контроллеры. М: Научтехлитиздат, 2017. № 10. С. 31–37. URL: https://www.elibrary.ru/item.asp?id=30710941 (дата обращения: 14.10.2020).
10. Скрыль С.В., Сычев В.М., Астрахов А.В., Гайфулин В.В., Никитина Ю.С. Формальные аспекты представления математической модели характеристики киберустойчивости информационной среды. Промышленные АСУ и контроллеры, 2020. № 3. С. 40–46. DOI: http://dx.doi.org/10.25791/asu.3.2020.1169.
11. Сычев А.М., Коробец Б.Н., Смирнов С.Н. и др. Безопасность операционных систем: учеб. пособие для студ. учреждений высш. образования; под ред. С.В. Скрыля. М.: Издательский центр «Академия», 2021. – 256 с.
12. Скрыль С.В., Мещерякова Т.В., Голубков Д.А., Арутюнова В.И. Оценка защищенности информации от вирусных атак: существующий и перспективный методический аппарат. Промышленные АСУ и контроллеры. М: Научтехлитиздат, 2018. №9. С. 51–62. URL: https://www.elibrary.ru/item.asp?id=35648304 (дата обращения: 14.10.2020).
13. Багаев, Д.А.; Лаврухин, Ю.Н.; Скрыль, С.В. Показатели эффективности информационных процессов и их защищенности в системах реального времени. Безопасность информационных технологий, [S.l.]. Т. 16, № 3. С. 104–106, сен. 2009. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/858 (дата обращения: 14.10.2020).
14. Курило А.П. [и др.]. Оценка защищенности компьютерной информации: пути решения проблемы. // Интеллектуальные системы (INTELS’ 2010): труды девятого международного симпозиума. М.: МГТУ им. Н.Э. Баумана, 2010. С. 564–566.

15. Информационная безопасность открытых систем: учебник для вузов. В 2-х томах. Т. 1. Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников [и др.]. М.: Горячая линия–Телеком, 2006. – 536 с.
16. Макаренко С.И. Информационное оружие в технической сфере: терминология, классификация, примеры // Системы управления, связи и безопасности. 2016. № 3. С. 292–376. URL: https://sccs.intelgr.com/archive/2016-03/11-Makarenko.pdf (дата обращения: 14.10.2020).
17. Кондаков С.Е., Мещерякова Т.В., Скрыль С.В., Стадник А.Н., Суворов А.А. Вероятностное представление условий своевременного реагирования на угрозы компьютерных атак // Вопросы кибербезопасности. М.: АО «НПО «Эшелон», 2019. № 6. С. 59–68. DOI: http://dx.doi.org/10.21681/2311-3456-2019-6-59-68.
18. Skryl’ S. et al. Assessing the Response Timeliness to Threats as an Important Element of Cybersecurity: Theoretical Foundations and Research Model. In: Kravets A., Groumpos P., Shcherbakov M., Kultsova M. (eds) Creativity in Intelligent Technologies and Data Science. CIT&DS 2019. Communications in Computer and Information Science, vol. 1084. Springer, Cham. 2019. P. 258–269. DOI: http://dx.doi.org/10.1007/978-3-030-29750-3_20.

REFERENCES:

[1] Velichko V.V., Katunin G.P., Shuvalov V.P.; edited by professor Shuvalov V.P. Basics of infocommunication technologies: textbook for universities. M.: Gorjachaja linija –Telekom, 2009. – 712 p. (in Russian).
[2] Pjatibratov A.P., Gudyno L.P., Kirichenko A.A. Computing systems, networks and telecommunications: textbook. M.: Finansy i statistika, 2004. 512 p. (in Russian).
[3] Grinjaev S.N. The battlefield is cyberspace. Theory, techniques, means, methods and systems of information warfare. M.: Harvest, 2004. – 426 p. (in Russian).
[4] Gavdan, Grigory P., Ivanenko, Vitaliy G., Salkutsan, Alexei A. Security of significant objects of critical information infrastructure. IT Security (Russia), [S.l.]. V. 26, no. 4. P. 69–82, dec. 2019. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1232 (accessed: 14.10.2020). DOI: http://dx.doi.org/10.26583/bit.2019.4.05.
[5] Electronic dictionary: site. URL: https://ru.wiktionary.org/wiki/кибератака. (accessed: 14.10.2020) (in Russian).
[6] Kotsynyak M.A., Kuleshov I.A., Kudryavtsev A.M., Lauta O.S. Cyber resilience of the information and telecommunications network. SPb.: Boston-spectr, 2015. – 150 p.
[7] Lukackij A.V. Cyber resilience, cyber survivability, cyber reliability, cyber continuity. URL: http://www.iksmedia.ru/blogs/post/5445277-Kiberustojchivost-kiberzhivuchest.html#ixzz6QU4Yn2yY (accessed: 18.10.2017) (in Russian).
[8] Skryl’ S.V., Shelupanov A.A. Fundamentals of systems analysis in information security: a textbook for students of higher educational institutions. M.: Mashinostroenie, 2008. – 138 p. (in Russian).
[9] Skryl’ S.V., Nikulin S.S., Sychev A.M., Ponomarev M.V., Le Vu Huong Zang. Indicators of the adequacy of structured systems for assessing the characteristics of information processes. Promyshlennye ASU i kontrollery. M.: Nauchtekhlitizdat, 2017. no. 10. P. 31–37. URL: https://www.elibrary.ru/item.asp?id=30710941 (accessed: 14.10.2020) (in Russian).
[10] Skryl’ S.V., Sychev V.M., Astrakhov A.V., Gaifulin V.V., Nikitina Yu.S. Formal aspects of the representation of the mathematical model of the characteristics of the cyber stability of the information environment. Promyshlennye ASU i kontrollery. 2020. no. 3. P. 40–46. DOI: http://dx.doi.org/10.25791/asu.3.2020.1169 (in Russian).
[11] Sychev A.M., Korobets B.N., Smirnov S.N., edited by Skryl’ S.V. Operating system security: a textbook for students of higher educational institutions. M.: Akademija [publishing house academia], 2021. – 256 p. (in Russian).
[12] Skryl’ S.V., Meshcheryakova T.V., Golubkov D.A., Arutyunova V.I. Assessment of information security against virus attacks: existing and promising methodological apparatus. Promyshlennye ASU i kontrollery. M.: Nauchtekhlitizdat, 2018. no. 9. P. 51–62. URL: https://www.elibrary.ru/item.asp?id=35648304 (accessed: 14.10.2020) (in Russian).
[13] Bagaev, D.F., Lavruhin, Ju.N., Skril’ S.V. Indicators of the effectiveness of information processes and their security in real-time systems. IT Security (Russia), [S.l.]. V. 16, no. 3. P. 104–106, sep. 2009. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/858 (accessed: 14.10.2020) (in Russian).
[14] Kurilo A.P. Assessment of the security of computer information: ways to solve the problem. Intellektual'nye sistemy (INTELS’ 2010): trudy devjatogo mezhdunarodnogo simpoziuma. M.: MGTU im. N.Je. Baumana, 2010. P. 564–566 (in Russian).

[15] Zapechnikov S.V. Information security of open systems: a textbook for universities. In 2 volumes. V. 1. Threats, vulnerabilities, attacks and approaches to defense. M.: Gorjachaja linija–Telekom, 2006. – 536 p. (in Russian).

[16] Makarenko S.I. Information weapons in the technical sphere: terminology, classification, examples. Sistemy upravlenija, svjazi i bezopasnosti [Systems of Control, Communication and Security]. 2016. no. 3. P. 292–376 (in Russian).

[17] Kondakov S.E., Meshcheryakova T.V., Skryl' S.V., Stadnik A.N., Suvorov A.A. Probabilistic representation of conditions for timely response to threats of computer attacks. Voprosy kiberbezopasnosti. M.: AO "NPO "Eshelon", 2019. no. 6. P. 59–68. DOI: http://dx.doi.org/10.21681/2311-3456-2019-6-59-68.

[18] Skryl' S. et al. Assessing the Response Timeliness to Threats as an Important Element of Cybersecurity: Theoretical Foundations and Research Model. In: Kravets A., Groumpos P., Shcherbakov M., Kultsova M. (eds) Creativity in Intelligent Technologies and Data Science. CIT&DS 2019. Communications in Computer and Information Science, vol. 1084. Springer, Cham. 2019. P. 258–269. DOI: http://dx.doi.org/10.1007/978-3-030-29750-3_20.

Поступила в редакцию – 30 ноября 2020 г. Окончательный вариант – 01 февраля 2021 г.
Received – November 30, 2020. The final version – February 01, 2021.

Виктор А. Хвостов[1], Алексей В. Скрыпников[2], Евгений А. Рогозин[3],
Людмила А. Обухова[4], Дмитрий Г. Силка[5]
[1,2]ВГБОУ ВО «Воронежский государственный университет инженерных технологий»,
пр–т Революции, 19, Воронеж, 394036, Россия
[3,4,5]Воронежский институт МВД России,
пр–т Патриотов,53, Воронеж, 394065, Россия
[1]e-mail: hvahva1@mail.ru, https://orcid.org/0000-0002-9324-5415
[2]e-mail: skrypnikovvsafe@mail.ru, https://orcid.org/0000-0003-1073-9151
[3]e-mail: evgenirogozin@yandex.ru, https://orcid.org/0000-0002-4455-7535
[4]e-mail: obuhova.lyudmila@bk.ru, https://orcid.org/0000-0003-0198-4972
[5]e-mail: sdg.silka@gmail.com, https://orcid.org/0000-0001-5086-6433

АНАЛИЗ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ПРИ ОБРАБОТКЕ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ В МОБИЛЬНЫХ СИСТЕМАХ

DOI: http://dx.doi.org/10.26583/bit.2021.1.08

Аннотация. Проведен анализ мобильных технологий, используемых для повышения качества управления в банковской сфере, сервиса и государственном управлении. На основе анализа уязвимостей мобильных станций (смартфонов, планшетов, смарт устройств, различных периферийным устройств смартфонов и т.п.), технологий предоставления доступа к интернету для мобильных систем (используемые в сетях сотовой связи, беспроводного доступа), а также мобильных сервисов информационных систем предложена классификация угроз безопасности информации и проведен анализ возможностей по реализации этих угроз. Целью работы является разработка актуальной модели угроз безопасности мобильных технологий, проведение исследований по оценке полноты и непротиворечивости применяемых в настоящее время средств защиты мобильных систем, таких как менеджер мобильных устройств, менеджер мобильных приложений, магазин доверенных мобильных приложений, шлюз безопасности мобильных приложений и др. В статье рассматриваются источники угроз, уязвимости технологий мобильных систем, каналы воздействия угроз, объекты воздействия и возникающие ущербы от реализации угроз, характерные для мобильных систем и имеющие отличные от традиционной точки приложения реализаций угроз и векторы. Проведен анализ контекста применения мобильных технологий и влияния на процессы предоставления услуг.

Ключевые слова: мобильные системы, мобильная станция, шлюз безопасности, менеджер мобильных устройств.

Для цитирования: ХВОСТОВ, Виктор А. и др. АНАЛИЗ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ПРИ ОБРАБОТКЕ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ В МОБИЛЬНЫХ СИСТЕМАХ. Безопасность информационных технологий, [S.l.], v. 28, n. 1, p. 95–105, jan. 2021. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1324>. Дата доступа: 05 feb. 2021. DOI: http://dx.doi.org/10.26583/bit.2021.1.08.

Victor A. Khvostov[1], Alexey V. Skrypnikov[2], Evgeniy A. Rogozin[3],
Ludmila A. Obuhova[4], Dmitriy G. Silka[5]
[1,2]Voronezh State University of Engineering Technologies,
Revolution Avenue, 19, Voronezh, 394036, Russia
[3,4,5]Voronezh Institute of the Ministry of the Interior,
Prospekt Patriotov, 53, Voronezh, 394065, Russia
[1]e-mail: hvahva1@mail.ru, https://orcid.org/0000-0002-9324-5415
[2]e-mail: skrypnikovvsafe@mail.ru, https://orcid.org/0000-0003-1073-9151
[3]e-mail: evgenirogozin@yandex.ru, https://orcid.org/0000-0002-4455-7535
[4]e-mail: obuhova.lyudmila@bk.ru, https://orcid.org/0000-0003-0198-4972
[5]e-mail: sdg.silka@gmail.com, https://orcid.org/0000-0001-5086-6433

Analysis of information security threats when processing confidential data in mobile systems

DOI: http://dx.doi.org/10.26583/bit.2021.1.08

Abstract. The analysis of mobile technologies used to improve the quality of management in the banking sector, service and public administration is carried out. Based on the analysis of vulnerabilities of mobile stations (smartphones, tablets, smart devices, various peripheral devices of smart phones, etc.), technologies for providing Internet access for mobile systems (used in cellular networks, wireless access), as well as mobile services of information systems. A classification of information security threats is proposed and an analysis of the possibilities for implementing these threats is carried out. The aim of the work is to develop an up-to-date model of security threats to mobile technologies and to study the completeness and consistency of currently used mobile system protection tools, such as a mobile device manager, mobile application manager, trusted mobile application store, mobile application security gateway, etc. The paper discusses the sources of threats, vulnerabilities of technologies of mobile systems, the channels of exposure to threats, objects of exposure and the resulting damage from the implementation of threats that are characteristic of mobile systems and have different applications of threat implementations and vectors. The analysis of the context of the use of mobile medicine and the impact on the processes of providing medical services is carried out.

Keywords: mobile systems, mobile station, security gateway, mobile device manager.
For citation: KHVOSTOV, Victor A. et al. Analysis of information security threats when processing confidential data in mobile systems. IT Security (Russia), [S.l.], v. 28, n. 1, p. 95–105, jan. 2021. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1324>. Date accessed: 05 feb. 2021. DOI: http://dx.doi.org/10.26583/bit.2021.1.08.

Введение

Анализ современного состояния мобильных систем показал, что все большую популярность приобретает движение, известное сегодня как BYOD (BringYourOwnDevice), означающее применение личных станций в профессиональной деятельности специалистами различных сфер деятельности. По результатам исследования [1], около 60% офисных работников пользуются мобильными устройствами не только для личных целей, но и для выполнения тех или иных рабочих задач.

При этом все многообразие мобильных технологий можно условно разделить на следующие направления [2–5]. Первая группа технологий используется для координации рабочих процессов, управления данными, доступа к корпоративным ресурсам. Технологии первой группы повышают эффективность работы пользователя, экономят его время, предоставляют оперативно справочную информацию, улучшают дистанционное взаимодействие внутри организаций и профессиональных групп. Вторая группа приложений используется для непосредственного взаимодействия с объектами физического мира (АСУ ТП – IndustrialControlSystems (ICS) или IndustrialAutomation and ControlSystems (IACS)). При этом организуется взаимодействие между элементами системы на разных уровнях представления. Третья группа технологий представляет собой информационно-справочные службы (в том числе экстренные). И четвертая группа представляет собой технологии для осуществления в терминальном режиме в качестве тонкого клиента с информационными системами (удаленное диагностирование, удаленное обслуживание и т.п.).

При организации функционирования мобильных технологий основной информацией, циркулирующей в технических средствах, является различная конфиденциальная информация (персональные данные, коммерческая тайна и др.), технологическая информация и ключевая информация криптографических протоколов различного вида.

Таким образом, использование мобильных технологий связано с организацией обработки конфиденциальной информации различного содержания и требует применения организации защиты информации[1,2,3].

Анализ нормативных и законодательных документов России в области защиты конфиденциальной информации и вопросов защиты информации (ЗИ), показал, что в настоящее время методических рекомендаций по ЗИ в информационных системах, использующих мобильные технологии, не существует. Применяемые в информационных системах средства ЗИ, обеспечивающие безопасность мобильных компонентов, применяются без законодательного и методического обоснования.

В соответствии со сложившимся методическим подходом обеспечения ЗИ[4,5], начальным этапом является разработка модели угроз безопасности информации (БИ), содержащей как классификацию угроз, так и краткое описание реализации наиболее актуальных угроз.

Таким образом, целью статьи является разработка модели угроз БИ для информационных систем, применяющим BYOD технологии.

Уязвимости мобильных технологий, новые векторы реализации угроз БИ, классификация угроз.

Под угрозой безопасности информации понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к конфиденциальной информации, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Угроза БИ может быть представлена в виде формальной записи следующего вида: угроза НСД в ИСПДн: = <источник угрозы>, <уязвимость ИСПДн>, <способ реализации угрозы>, <объект воздействия (программа, протокол, данные и др.)>, <деструктивное действие>.

Источником угрозы может выступать пользователь, вредоносная программа, аппаратная закладка.

По отношению к мобильным технологиям пользователей можно разделить на ряд категорий.

Сотрудники учреждения. Данная категория пользователей получает доступ к данным и услугам организации с мобильного устройства. Уровень доступа для пользователей этой категории основывается на требованиях, обусловленных их должностными обязанностями, уровнем конфиденциальности информации, к которой сотрудник должен получить доступ, и необходимости доступа к этим данным с

[1]Федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» //«Российская газета»№ 165 от 29.07.2006.

[2]Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды приказ директора ФСТЭК России от 14.03.2014 № 31.

[3]Стандарт Банка России СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации/ Общие положения» (принят и введен в действие распоряжением Банка России от 17.05.2014 № Р-399.

[4]ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения.

[5]Методический документ ФСТЭК России. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008.

использованием мобильного устройства. Для сотрудника учреждения необходим набор мобильных учетных данных, которые используются для доступа к внутренним ресурсам информационной системы.

Партнеры – это сотрудники сторонних организаций, которые сотрудничают с организацией при выполнении определенных задач, включая технический персонал, поддерживающий работоспособность технических средств. Пользователям-партнерам может потребоваться доступ к системе, приложениям и инфраструктуре для выполнения назначенных технического обслуживания и регламентных работ, но им не предоставляется доступ и права, как для сотрудников. Пользователям-партнерам обычно предоставляется ограниченный набор мобильных учетных данных, которые используются для доступа к внутренним системам организации.

Внешние пользователи – это лица, которые не связаны с организацией, но которым необходим доступ к общедоступным данным организации через предоставляемые и поддерживаемые организацией интерфейсы. Этими интерфейсами обычно являются WEB-приложения или другие приложения для мобильных устройств. Внешние пользователи обычно не указывают свои учетные данные в мобильной информационной системе. Интерфейсы данных организации могут иметь набор локально используемых учетных записей, которые действительны только для ресурса, к которому осуществляется доступ.

Поставщики компонентов, сборок и аксессуаров мобильных устройств. Данная категория источников угроз ИБ имеет возможность физически вмешиваться в работу мобильного устройства перед его поставкой и устанавливать вредоносное программное обеспечение.

Поставщики услуг сервисов беспроводных технологий. Эта категория источников угроз опасна возможностью установки вредоносного программного обеспечения, направленного как на воздействие на данные пользователей, так и на процессы управления мобильным устройством. Поставщик услуг сервисов беспроводных технологий имеет возможность перенастройки мобильного устройства, получения доступа к информационному ресурсу мобильной станции, кэширования данных пользователя на носителе. При этом могут использоваться не только каналы передачи информации, использующие IP транспорт (MMS/SMS), но и каналы управления мобильной сети.

Наиболее опасным источником угроз БИ для мобильных технологий является вредоносный код (эксплойты, руткиты и др.). Это программное обеспечение, созданное с целью выполнить несанкционированное действие, которое может поставить под угрозу конфиденциальность, целостность или доступность мобильного устройства. Вредоносное ПО может быть прикреплено к мгновенным сообщениям, добавлено в электронную почту или загружено в интернет как зараженный файл. Вредоносное ПО также может быть встроено в загруженные приложения. Эта категория источников угроз БИ может повлиять на работу операционной системы мобильного устройства, компрометировать данные или приложения на мобильном устройстве или и то, и другое.

1. Основные уязвимости БИ мобильных технологий.

В качестве основных уязвимостей БИ мобильных технологий необходимо рассмотреть следующие:

– уязвимости беспроводных технологий, обеспечивающих доступ в интернет мобильных устройств;

– уязвимости мобильных устройств;

– уязвимости сервисов мобильного доступа информационных систем.

Уязвимости беспроводных технологий – это уязвимости, которые могут использоваться источником угрозы через сеть на уровне приложений или в приложениях, файлах документов или данных (как протоколов передачи данных, так и протоколы управления), как, а также с использованием протоколов управления мобильных устройств. Сетевые угрозы безопасности связаны с уязвимостями внутри сети и сетевых протоколов, а также устройств, приложений и данных, которые находятся в сети. Использование мобильных устройств актуализируют проблему анализа угроз безопасности на основе сети, поскольку для передачи цифрового потока используются сотовая связь, технологии WiFi, Bluetooth, InfraredCommunication (IR), NearFieldCommunication (NFC), имеющие ряд специфических уязвимостей и имеющих достаточно низкий уровень защищенности.

Мобильные устройства передают цифровой поток через сотовые сети. Соответственно, им свойственны уязвимости глобальной системы мобильной связи GSM [6–8], обеспечиваемой провайдером, цифровой технологии беспроводной передачи данных для мобильной связи, функционирующей как надстройка над 2G и 2.5G EDGE, универсальной системы мобильной связи (UMTS), технологии высокоскоростного пакетного доступа HSDPA и ее варианта HSUPA. Также могут быть рассмотрены уязвимости технологий сотовой связи с множественным доступом с кодовым разделением CDMA, в которых используются протоколы Evolution-Data Optimized (EV-DO) и Long-Term Evolution (LTE).

Передача данных и голоса по управляемой сети мобильных операторов может быть перехвачена, а конфигурация, а также основные компоненты могут быть скомпрометированы через каналы управления.

Мобильные устройства используют беспроводную сетевую связь Wi-Fi, основанную на семействе стандартов IEEE 802.11a/b/g/n. Эти устройства могут подключаться к любой мобильной точке доступа, персональным или корпоративным точкам доступа или аналогичным устройствам для одноранговой связи. Устройства, использующие связь Wi-Fi, уязвимы для перехвата другими устройствами Wi-Fi и беспроводными программными средствами, а также анализаторами сигналов[6]. Нелегитимные точки доступа (несанкционированные мошенники в административно управляемом домене) также представляют потенциальную угрозу, подвергая мобильные устройства угрозам «человек посередине».

Bluetooth[7]. Беспроводная технология малого радиуса действия Bluetooth, обеспечивает стандартный протокол замены проводов для подключения. Технология используется как для передачи данных между устройствами в персональной сети, так и для команд, а также для голосовой связи между устройством и гарнитурой. Bluetooth обеспечивает собственные механизмы шифрования и аутентификации, но также имеет известные уязвимости и угрозы БИ, такие как атака с перехватом ключей во время инициализации сеанса.

Инфракрасный порт (InfraRed Data Association – IrDA)[8,9]. Технология IrDA предоставляет спецификации для реализации передачи данных на физическом и канальном уровнях с использованием в качестве среды передачи инфракрасный диапазон световых

[6]K. Scarfone, D. Dicoi Wireless Network Security for IEEE 802.11a/b/g and Bluetooth (Draft). Recommendations of the National Institute of Standards and Technology. Special Publication 800-48 Revision 1 (Draft)
[7]NIST SP 800 121 Guide to Bluetooth Security. Published Date: May 2017.
[8]IrDA Marketing Requirements – Basis for the IrDA Technical Standards, Version 3.2 The Infrared Data Association, November 23, 1993.
[9]LAN Access Extensions for Link Management Protocol (IrLAN), Proposal, Version 1.0 The Infrared Data Association, January 1, 1996.

волн, но также имеет известные уязвимости спецификаций IrLAP, IrLMP, IrCOMM, Tiny TP, IrOBEX, IrLAN, IrSimple и IrFM, которые необходимо учитывать.

Инфракрасное излучение используется как для передачи данных между устройствами внутри локальной сети (PAN), так и для команд (односторонняя передача). Инфракрасный порт не предоставляет механизмов шифрования и аутентификации и, следовательно, имеет известные уязвимости. Большинство угроз БИ, связанные с уязвимостями IrDA зависят от поставщика, например, из-за переполнения буфера в принимающем коде инфракрасной связи.

Near field communication, NFC[10] («коммуникация ближнего поля», «ближняя бесконтактная связь») – технология беспроводной передачи данных малого радиуса действия, которая даёт возможность обмена данными между устройствами на расстоянии порядка 10 см. Данная технология представляет собой набор стандартов для маломощного, миниатюрного подключения для замены проводов для двухточечной связи, мобильных устройств.

Уязвимости NFC связаны с тем, что стек протоколов технологии не предусматривает использования криптографических протоколов при передаче. Стандарты хранения данных в метках и картах, а также их эмуляции – не предусматривают криптографической защиты при хранении.

В NFC сервисах традиционно закладывается излишнее доверие к информации, хранящейся в мобильном устройстве, в результате фактически не выполняется фильтрация данных. Подключение NFC в первую очередь подвержено атакам физического уровня, таким как перехват и внедрение сигналов, но конкретные реализации могут содержать дополнительные уязвимости.

Уязвимости мобильных систем. Уязвимости мобильных систем можно классифицировать по признаку принадлежности к элементу мобильной системы. При этом можно выделить уязвимости аппаратной составляющей мобильной станции, уязвимость мобильной операционной системы, уязвимость мобильного приложения.

Уязвимости аппаратной составляющей мобильной станции в основном связаны с ошибками или с преднамеренно установленными аппаратными люками при прошивке мобильной станции. Кроме того, в мобильных станциях могут быть установлены дополнительные несанкционированные аппаратные закладки, различные функции слежения и перехвата информации.

Уязвимость мобильной операционной системы и мобильных приложений аналогичны тем, что существуют для традиционных ЭВМ и постоянно обнаруживаются [9, 10]. Уязвимости операционной системы могут быть использованы аналогично уязвимым приложениям. Уязвимости операционной системы представляют большую угрозу, поскольку операционная система работает с более высоким уровнем привилегий, чем приложения. Мобильные приложения, как и приложения на других устройствах, также могут быть плохо написаны и уязвимы для атак и эксплуатации. Многие приложения уязвимы из-за ошибок программирования, ошибок проектирования или выбора конфигурации в возможностях обеспечения безопасности.

Кроме того, пользователи отключают встроенные функции безопасности ОС, обычно известные как «джейлбрейк» или «рутинг». Отключение встроенных функций безопасности ОС позволяет пользователям устанавливать приложения и усовершенствования системы, которые в противном случае были бы ограничено.

[10]ISO/IEC 18092 / ECMA-340 Near Field Communication Interface and Protocol-1 (NFCIP-1).

Существует высокий уровень риска, связанный с использованием измененных устройств с отключенными функциями безопасности мобильной ОС.

2. Основные каналы воздействия угроз БИ мобильных технологий

К основным каналам воздействия угроз БИ мобильных технологий относятся:

– физический доступ к мобильной станции;

– доступ к радиоканалу передачи цифрового потока от мобильной станции к базовой станции;

– доступ к высокоскоростным магистральным каналам передачи цифрового потока, используемым операторами сотовой связи;

– доступ к внутренней инфраструктуре информационной системы организации.

Основная уязвимость физического доступа к мобильной станции связана с доступом злоумышленника к данным при потере смартфона. Потеря мобильного устройства ставит под угрозу конфиденциальность, целостность и доступность информации. Кроме того, устройство может содержать учетные данные для доступа к информационной системе организации, что создает дополнительный риск для нее. Также, данные на мобильном устройстве могут быть потеряны, если устройство не выполняется резервное копирование.

Дополнительно, при возможности доступа злоумышленника к мобильной станции, возможна установка вредоносного аппаратного или программного обеспечения, которое может собирать или повреждать данные, как на устройстве, так и в информационной системе организации. Злоумышленник может использовать внешние интерфейсы для подключения мобильного устройства к USB и Bluetooth-модему. Кроме того, злоумышленник может подключить компьютер или внешний жесткий диск для клонирования, копирования, уничтожения, удаления или изменения содержимого мобильного устройства.

Существующие уязвимости встроенных функций мобильного устройства, таких как камера и микрофон, создают повышенную угрозу безопасности, создавая средства для сбора конфиденциальных изображений или разговоров. Также угрозу безопасности повышают уязвимости периферийных устройств, физически взаимодействующих с мобильной станцией (док-станции, гарнитуры, дополнительное оборудование).

Канал реализации угрозы БИ при доступе к радиоканалу передачи цифрового потока от мобильной станции к базовой станции представляет собой электронное прослушивание через беспроводную сеть (Wi-Fi или GSM), цифровой поток или речевые сигналы могут изменяться, ими можно манипулировать или выборочно блокировать во время передачи.

Канал побочных электромагнитных излучений. Мобильные станции основаны на работе различных дискретных электрических компонентов внутри самого устройства. Также они излучают внеполосные и кратные сигналы, соответствующие их основным радиоинтерфейсам, таким как сотовая связь, Bluetooth, NFC или Wi-Fi. Это излучение находится в пределах радиочастотного спектра и может быть захвачено и декодировано, поскольку информация, излучаемая ЦП и его подсистемами, в основном не зашифрована. И, следовательно, канал побочных электромагнитных излучений является уязвимым для наблюдения третьей стороной как в непосредственной близости, так и на расстоянии (например, 100 м).

Кроме перехвата сигналов мобильных станций дополнительной угрозой БИ являются подавление приемников мобильных станций (любой беспроводной протокол, используемый на мобильном устройстве, подвержен помехам, включая GPS, сотовую связь, Wi-Fi и Bluetooth). Кроме того, специфической угрозой, воздействующей по радиоканалу,

является угроза наводнения (flood) при реализации которой в систему направляется большее количество информации, чем она может обработать.

Большинство мобильных устройств обеспечивают возможность определения реального географического местоположения электронного устройства (геолокации) в своих приложениях. Такие приложения могут быть использованы для отображения текущей позиции на карте, поиска близлежащих ресурсов или отслеживания пути пользователя. Еще более популярным среди пользователей является возможность приложений указывать маршруты движения. Эти службы определения местоположения могут разгласить местоположение устройства (или предоставить неточную информацию о местоположении пользователя устройства из-за внешних помех или манипуляций).

Канал реализации угрозы БИ со стороны сети провайдера сотовой связи приводит к возможности нарушения конфиденциальности и целостности информации, т.к. для работы используются высокоскоростные магистральные сети, являющиеся составной частью сетей связи общего пользования страны [11].

3. Объекты воздействия угроз БИ мобильных технологий

Объектами воздействия угроз БИ являются информационные ресурсы, содержащие персональные данные, конфиденциальную служебную информацию организации, а также технологическая информация, программно-технические средства обработки информации, средства защиты персональных данных (ПДн), каналы информационного обмена и телекоммуникации информационной системы. В зависимости от места нахождения объектов воздействия угроз их можно классифицировать на следующие виды:

– информационный ресурс, содержащийся в мобильной станции;

– цифровой поток, передаваемый по радиоканалу «мобильная станция – базовая – станция провайдера сотовой связи»;

– цифровой поток, передаваемый по радиоканалу «мобильная станция – точка – доступа Wi-Fi»;

– цифровой поток, передаваемый по сети провайдера сотовой связи;

– цифровой поток, передаваемый по высокоскоростным магистральным сетям, являющийся составной частью сетей связи общего пользования страны;

– цифровой поток, обрабатываемый в сети организации.

В зависимости от вида объекты воздействия угроз можно разделить на:

– открытые данные;

– данные, зашифрованные симметричным шифром (DES, AES);

– данные, зашифрованные ассиметричным шифром (A5) [6–8].

4. Классификация угроз БИ мобильных технологий

По виду деструктивных действий, воздействующих на конфиденциальную информацию в мобильных технологиях, традиционно выделяют следующие классы угроз БИ:

– приводящие к нарушению конфиденциальности;

– приводящие к нарушению целостности;

– приводящие к нарушению доступности.

При этом, необходимо рассмотреть ряд специфических угроз БИ, обусловленных применением мобильных станций и непосредственно не нарушающих состояние безопасности ПДн.

Состав элементов описания угроз БИ мобильных технологий представлен на рис. 1.

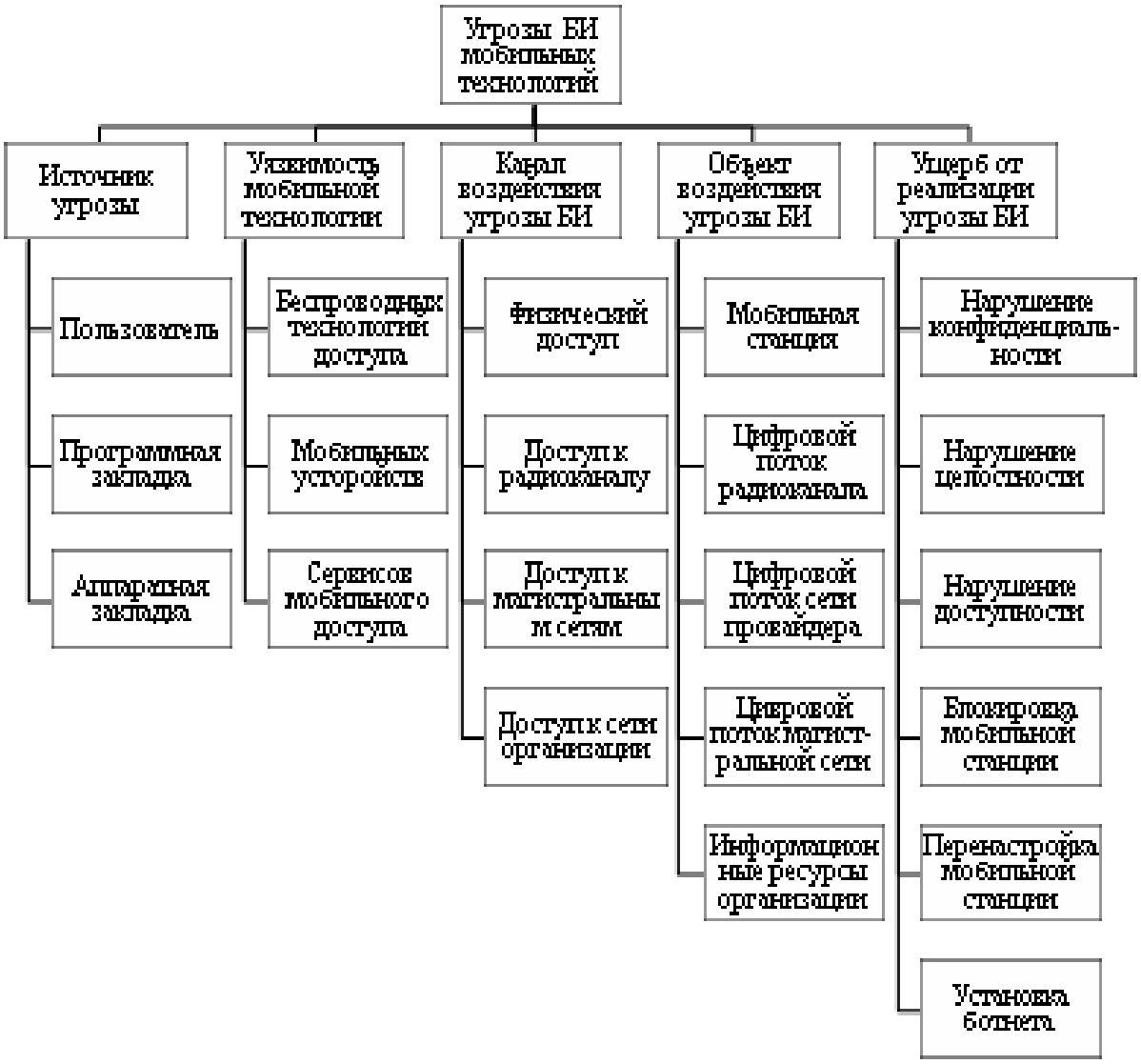


Рис. 1. Классификация угроз БИ мобильных технологий
Fig. 1. Classification of information security threats in mobile technologies

Мобильная станция в ходе функционирования передаёт в базовую станцию сервисную информацию (LAC, CellID, IMSI, NetworkIdentity and TimeZone и т.п.). Переданные мобильной станцией сервисные данные могут быть использованы для анализа поведения пользователя или организации (например, локальные и удаленные журналы). Также широко применяется специальное программное обеспечение и сервисы провайдеров мобильной связи для объединения данных геолокации с информацией SSID для сбора информации о местоположении определенных беспроводных сетей, которые совместно используются их клиентами. Известны примеры программного обеспечения, установленного поставщиком услуг сотовой связи, использующиеся для отслеживания поведения пользователя, а также показателей производительности мобильной станции или мобильного сервиса. Эти данные также могут быть отправлены непосредственно поставщику или третьей стороне.

В ходе использования мобильной станции пользователь может установить приложение, содержащее вредоносный код, позволяющий перенастроить мобильное

устройство (прямо или косвенно) или предлагать услугу непосредственно или через стороннее устройство.

Вредоносные программы, требующие выкуп, стали крайне распространенным классом злонамеренных программ для мобильных систем. Как правило, блокируется работа мобильной станции, требуя с жертвы выкуп, после выплаты которого возвращают пользователю контроль над смартфоном или планшетом. Также преступники выбирают в качестве целей истории звонков, контакты, фотографии или сообщения, что практически всегда вынуждает пользователя заплатить затребованную сумму.

Ботнеты, состоящие из взломанных мобильных станций – еще одна актуальная угроза БИ. Зараженные устройства, являющиеся частью ботнетов, находятся под контролем злоумышленников, которые в любой момент могут приказать им инициировать DDoS-атаку на какой-либо ресурс, либо начать массовую рассылку спам писем.

Заключение

Проведенный в статье анализ угроз БИ аппаратных и программных средств мобильных технологий, используемых в сфере сервиса, АСУ ТП и банковской сфере, показал значительное усложнение проблемы обеспечения БИ при существенном повышении эффективности функционирования при использовании этой технологии. Применение мобильных станций в качестве основного инструмента в сфере сервиса, АСУ ТП и банковской сфере, участие третьей стороны в процессах обработки конфиденциальной информации (провайдер услуг сотовой связи, провайдер услуг беспроводного доступа, организации, эксплуатирующие высокоскоростные магистральные каналы передачи цифрового потока) привело к существенному усложнению традиционной модели угроз БИ сформированной ФСТЭК России. Новые угрозы БИ, обусловленные использованием мобильных технологий и новые векторы реализации угроз, рассмотренные в статье, позволили доработать модель угроз БИ и разработать классификационную схему угроз БИ, представленную на рис. 1.

СПИСОК ЛИТЕРАТУРЫ:

1. Исследование мобильного интернета в России. URL: https://www.shopolog.ru/news/mail-ru-group-issledovanie-mobilnogo-interneta-v-rossii/ (дата обращения: 10.11.2020).
2. Никитин П.В., Мурадянц А.А., Шостак Н.А. Мобильное здравоохранение: возможности, проблемы, перспективы // Клиницист. 2015, № 4. С. 13–21. URL: https://www.elibrary.ru/item.asp?id=25672591 (дата обращения: 10.11.2020).
3. Яненко М.Б., Яненко М.Е. Мобильные технологии в маркетинге услуг: новые возможности и проблемы // Проблемы современной экономики. 2014. № 2. С. 227–230. URL: https://www.elibrary.ru/item.asp?id=21981140 (дата обращения: 10.11.2020).
4. Банковское обслуживание будущего: мобильные технологии стимулируют развитие инноваций. URL: https://www.intel.ru/content/www/ru/ru/financial-services-it/article/banking-on-the-future.html (дата обращения: 10.11.2020).
5. АСУ ТП с использованием мобильного телефона. URL: http://www.adastra.ru/products/overview/mobile/ (дата обращения: 10.11.2020).
6. Попов В.И. Основы сотовой связи стандарта GSM М.: Эко-Трендз, 2005. – 296 с.
7. Интеллектуальные сети связи. / Лихтциндер Б.Я. [и др.] М.: ЭКО-ТРЕНДЗ, 2000. – 205 с.
8. Шиллер Й. Мобильные коммуникации. М.: Вильямс, 2002. – 384 с.
9. Zhu X., Zhu Y. (2019) Extension of ISO/IEC27001 to Mobile Devices Security Management. In: Yun X. et al. (eds) Cyber Security. CNCERT 2018. Communications in Computer and Information Science. Vol. 970. Springer, Singapore. DOI: https://doi.org/10.1007/978-981-13-6621-5_3.
10. Gkioulos, Vasileios; Wangen, Gaute; Katsikas, Sokratis K.; Kavallieratos, George; Kotzanikolaou, Panayiotis. 2017. "Security Awareness of the Digital Natives" Information 8, no. 2: 42. DOI: https://doi.org/10.3390/info8020042.

11. Гольдштейн Б.С., Соколов Н.А., Яновский Г.Г. Сети связи. Учебник для ВУЗов. СПб.: БХВ-Петербург. 2011. – 400 с.

REFERENCES:

[1] Research of the mobile Internet in Russia. URL: https://www.shopolog.ru/news/mail-ru-group-issledovanie-mobilnogo-interneta-v-rossii/ (accessed: 10.11.2020) (in Russian).
[2] Nikitin P.V., Muradyants A.A., Shostak N.A. Mobile health care: opportunities, problems, prospects. Clinician. 2015, no. 4. P. 13–21. URL: https://www.elibrary.ru/item.asp?id=25672591 (accessed: 10.11.2020) (in Russian).
[3] Yanenko M.B., Yanenko M.E. Mobile technologies in marketing services: new opportunities and problems. Problems of modern economics. 2014, no. 2. P. 227–230. URL: https://www.elibrary.ru/item.asp?id=21981140 (accessed: 10.11.2020) (in Russian).
[4] Banking services of the future: mobile technologies stimulate the development of innovations. URL: https://www.intel.ru/content/www/ru/ru/financial-services-it/article/banking-on-the-future.html (accessed: 10.11.2020) (in Russian).
[5] ACS TP using a mobile phone. URL: http://www.adastra.ru/products/overview/mobile/ (accessed: 10.11.2020) (in Russian).
[6] Popov V.I. Fundamentals of cellular communication of the GSM standard M.: Eco-Trends, 2005. – 296 p. (in Russian).
[7] Intelligent communication networks. Likhtzinder B.Ya. [and others] M.: EKO-TRENDZ, 2000. – 205 p. (in Russian).
[8] Schiller J. Mobile communications. M.: Williams, 2002. – 384 p. (in Russian).
[9] Zhu X., Zhu Y. (2019) Extension of ISO/IEC27001 to Mobile Devices Security Management. In: Yun X. et al. (eds) Cyber Security. CNCERT 2018. Communications in Computer and Information Science. Vol 970. Springer, Singapore. DOI: https://doi.org/10.1007/978-981-13-6621-5_3.
[10] Gkioulos, Vasileios; Wangen, Gaute; Katsikas, Sokratis K.; Kavallieratos, George; Kotzanikolaou, Panayiotis. 2017. "Security Awareness of the Digital Natives" Information 8, no. 2: 42. DOI: https://doi.org/10.3390/info8020042.
[11] Goldstein B.S., Sokolov N.A., Yanovskiy G.G. Communication networks. Textbook for universities. SPb.: BHV-Petersburg. 2011. – 400 p. (in Russian).

Поступила в редакцию –26 ноября 2020 г. Окончательный вариант – 05 февраля 2021 г.
Received –November 26, 2020. The final version – February 05, 2021.

Андрей Е. Краснов[1], Александр С. Мосолов[2], Наталия А. Феоктистова[3]
[1]Российский государственный социальный университет,
ул. Вильгельма Пика, 4, стр. 1, Москва,129226, Россия
[2]Российский химико-технологический университет им. Д.И. Менделеева,
Миусская пл., 9, Москва, Россия
[3]Российская академия образования,
ул. Погодинская, 8, Москва, 119121, Россия
[1]e-mail: krasnovmgutu@yandex.ru, https://orcid.org/0000-0002-4075-4427
[2]e-mail: asmosolov@yandex.ru, https://orcid.org/0000-0002-3266-9505
[3]e-mail: feofamilynat@yandex.ru, https://orcid.org/0000-0002-0030-7390

ОЦЕНИВАНИЕ УСТОЙЧИВОСТИ КРИТИЧЕСКИХ ИНФОРМАЦИОННЫХ ИНФРАСТРУКТУР К УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

DOI: http://dx.doi.org/10.26583/bit.2021.1.09

Аннотация. Цель настоящей статьи заключается в описании методологии комплексного оценивания уязвимости критической информационной инфраструктуры (КИИ) и ее критических элементов на опасных производственных объектах, в том числе на объектах топливно-энергетического комплекса. К элементам КИИ на таких предприятиях в первую очередь следует отнести автоматизированные системы управления технологическими процессами. От нормального функционирования КИИ зависит бесперебойная работа сложных производственно-технологических процессов на критических элементах. Поэтому оценка уязвимостей в системе информационной безопасности, а также исследование стабильности системы безопасности объекта в целом позволит принять превентивные меры в отношении различного вида угроз. В рамках исследования применялись методы системного анализа (декомпозиция и синтез): при оценивании устойчивости информационной системы в целом ее иерархическая структура рассмотрена на примере графа с возможными структурными связями компонентов (активов) системы. Рассмотрены четыре вида отношений активов – полная независимость, слабая зависимость, сильная зависимость, обратная связь. Оценивание устойчивости системы в целом основано на вычислении устойчивости ее парных активов и информационной технологии рекуррентного пересчета при подключении новых компонентов. Метод имитационного моделирования применен для моделирования влияния рисков информационной безопасности на КИИ в условиях неполных и неоднозначных данных об их составляющих, логико-вероятностные методы – для оценки влияния рисков как на составляющие (активы) информационной системы, так и систему в целом с учетом иерархической связи этих активов. Для оценивания влияния базовой угрозы «технического воздействия» (информационной безопасности и системы физической защиты) на риски системы безопасности производственных объектов использовался метод Монте-Карло. Проведение мероприятий по оценке устойчивости информационных систем и стабильности систем безопасности ориентировано на критически важные объекты в медицине, образовании, промышленности, структурах государственного управления.

Ключевые слова: угроза, риск, устойчивость, стабильность, граф, отношения, независимость, слабая зависимость, сильная зависимость, обратная связь.

Для цитирования: КРАСНОВ, Андрей Е.; МОСОЛОВ, Александр С.; ФЕОКТИСТОВА, Наталия А. ОЦЕНИВАНИЕ УСТОЙЧИВОСТИ КРИТИЧЕСКИХ ИНФОРМАЦИОННЫХ ИНФРАСТРУКТУР К УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Безопасность информационных технологий, [S.l.], v. 28, n. 1, p. 106–120, jan. 2021. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1328>. Дата доступа: 18 feb. 2021. DOI: http://dx.doi.org/10.26583/bit.2021.1.09.

Andrey E. Krasnov[1], Alexander S. Mosolov[2], Nataliya A. Feoktistova[3]
[1]Russian State Social University,
Wilhelm Pik str., 4 Building 1, Moscow, 129226, Russia,
[2]D. Mendeleev University of Chemical Technology of Russia,
Miusskaya square, 9, Moscow, 125047
[3]Russian Academy of Education,
Pogodinskaya str., 8, Moscow, 119121, Russia
[1]e-mail: krasnovmgutu@yandex.ru, https://orcid.org/0000-0002-4075-4427
[2]e-mail: asmosolov@yandex.ru, https://orcid.org/0000-0002-3266-9505
[3]e-mail: feofamilynat@yandex.ru, https://orcid.org/0000-0002-0030-7390

Assessing the resilience of critical information infrastructures to information security threats

DOI: http://dx.doi.org/10.26583/bit.2021.1.09

Abstract. This paper describes the methodology for comprehensive assessment of the vulnerability of critical information infrastructure (CII) and its critical elements at hazardous production facilities, including those of the fuel and energy production. The elements of CII at such enterprises, first of all, include automated control systems for technological processes. The smooth operation of complex technological and production processes based on critical elements depends on the normal functioning of the CII. Therefore, the assessment of vulnerabilities in the information security system, as well as the study of the security system stability at the facilities as a whole, will allow taking preventive measures against various types of threats. The following methods were used in this study. Methods of system analysis (decomposition and synthesis): when assessing the resilience of an information system as a whole, its hierarchical structure is considered using the example of a graph with possible structural connections of the components (assets) of the system. Four types of asset relationships are considered (their complete independence, weak dependence, strong dependence, feedback). Assessing the resilience of the system as a whole is based on calculating the resilience of its paired assets and information technology of recurrent recalculation when new components are connected. The method of simulation modeling, in particular, for modeling the impact of information security risks on CII in conditions of incomplete and ambiguous data on their components, logical and probabilistic methods - for assessing the impact of risks both on the components (assets) of the information system, and the system as a whole, taking into account the hierarchical relationship of these assets. The Monte Carlo method was used to assess the impact of the basic threat of "technical impact" (information security and physical protection systems) on the security risks of production facilities. The implementation of measures to assess the resilience of information systems and the security systems stability is focused on critical objects in medicine, education, industry, and public administration.
Keywords: threat, risk, resilience, stability, graph, relationships, independence, weak dependence, strong dependence, feedback.
For citation: KRASNOV, Andrey E.; MOSOLOV, Alexander S.; FEOKTISTOVA, Nataliya A. Assessing the resilience of critical information infrastructures to information security threats. IT Security (Russia), [S.l.], v. 28, n. 1, p. 106–120, jan. 2021. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1328>. Date accessed: 18 feb. 2021. DOI: http://dx.doi.org/10.26583/bit.2021.1.09.

Введение

В управлении безопасностью как больших организационно-экономических и организационно-технических систем, так и систем безопасности категорируемых предприятий топливно-энергетического комплекса ключевую роль играет управление рисками, и, в первую очередь, модели оценивания рисков (Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 № 187-ФЗ, последняя редакция). Риски рассматривают как функции от вероятностей и опасностей событий, вызванных множеством угроз, а также уровней уязвимости к этим угрозам [1, 2]. Риск угрозы «технического воздействия» системе

безопасности – возможность того, что данная угроза сможет воспользоваться уязвимостью актива или группы активов и нанести ущерб организации (ГОСТ Р ИСО/МЭК 27005:2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. – М.: Стандартинформ, 2011. – 94 с. NIST SP 800-30 Revision 1. Guide for Conducting Risk Assessments, 2012). Традиционно риски рассчитывают, как произведение вероятности наступления неблагоприятного события на величину его последствий [2–5]. Следует также отметить, что даже во многих внедренных системах информационной безопасности величины вероятностей наступления неблагоприятных событий рассчитывают, как произведение оценок вероятностей реализации каждой из угроз, считая их независимыми событиями, что совершенно не верно для общего случая.

В последнее время весьма плодотворными оказались подходы, в которых риски рассматривают как нечеткие категории, а их оценивание предлагают проводить на основе функций принадлежности теории нечетких множеств [6, 7], а также смешанного нечетко-вероятностного анализа [8].

Развиваются также гибридные модели информационной безопасности систем, включающие как факторный анализ рисков, так и особенности управленческих и технических решений в области противодействия [9].

Тем не менее, еще в работе [2] отмечалась важность агрегирования оценок рисков различной природы для сложных систем, а также возрастание сложности контроля безопасности в системах с разнородными рисками из-за увеличения взаимозависимости различных системных структурных составляющих и утраты контроля за их безопасностью. Поэтому независимо от того, как рассчитывается риск (на основе вероятностного подхода, или на основе теории нечетких множеств), главным является оценивание его связи с иерархией информационной системы, относящейся к критической информационной инфраструктуре (КИИ) в соответствии с 187-ФЗ от 26.07.2017.

Основная гипотеза настоящего исследования состоит в том, что для оценивания влияния угроз на системообразующие составляющие защищаемой информационной системы, а также систему в целом эффективным будет новое вводимое понятие – устойчивость к угрозам информационной безопасности. Это позволяет воспользоваться результатами, полученными в работах по формализации синдромной диагностики заболеваний [10], привлечь нейросетевые технологии агрегирования для оценивания качества функционирования многопараметрических объектов и процессов [11], а также – эффективности функционирования организации по ключевым показателям ее деятельности [12, 13].

Целью настоящей статьи является создание методологии, позволяющей оценивать влияние рисков информационной безопасности на КИИ в условиях неполных и неоднозначных данных об их составляющих, а главное – влияние рисков как на составляющие (активы) информационной системы, так и систему в целом с учетом иерархической связи этих активов. Конкретными активами могут быть серверы и локальные сети, подключенные к компьютерам лабораторные установки.

1. Постановка задачи исследования

Рассмотрим трехуровневую иерархическую структуру отношений (связей) составляющих (активов, ресурсов) $\boldsymbol{A}_1$, $\boldsymbol{A}_2$, $\boldsymbol{A}_3$, $\boldsymbol{A}_4$, $\boldsymbol{A}_5$ информационной системы (ИС), представленных в виде однонаправленного графа (рис. 1).

Из приведенного на рис. 1 графа видно, что каждый последующий уровень ИС агрегирует подсистемы предыдущего уровня. Естественно, что отношения активов могут быть более сложными, включая и обратные связи. Такие связи рассмотрим позже.

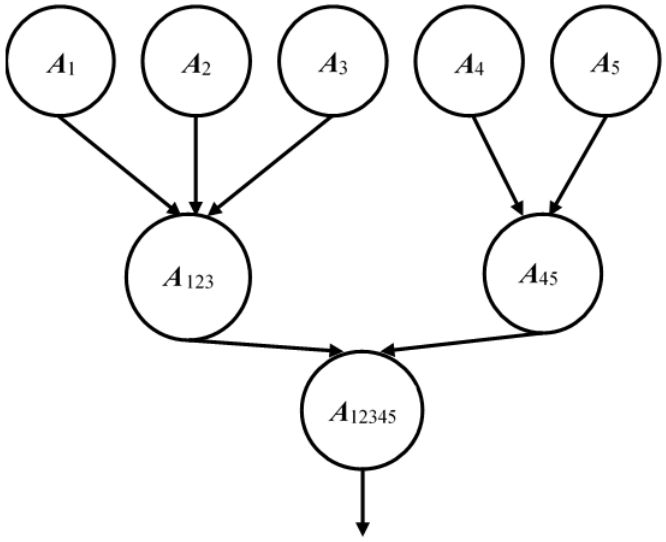


Рис. 1. Граф иерархических уровней связей активов ИС
Fig. 1. Graph of hierarchical levels of links between IS assets

Пусть заданы коэффициенты $K_c(\boldsymbol{A}_n)$, $K_i(\boldsymbol{A}_n)$ и $K_a(\boldsymbol{A}_n)$ («важности») критериев *конфиденциальности* (*confidentiality*), *целостности* (*integrity*) и *доступности* (*availability*) каждого актива $\boldsymbol{A}_n$ (n = 1, 2, …, N) в произвольных балльных шкалах (3-х балльной, 5-ти балльной). Пусть также экспертно заданы:

$\mu_c(T|\boldsymbol{A}_n)$ и $\mu_c(V|\boldsymbol{A}_n)$ – мера (степень) реализации *угрозы безопасности* (*security threat*) и мера (степень) *уязвимости* (*vulnerability*) конфиденциальности актива $\boldsymbol{A}_n$ соответственно;

$\mu_i(T|\boldsymbol{A}_n)$ и $\mu_i(V|\boldsymbol{A}_n)$ – мера (степень) реализации *угрозы безопасности* и мера (степень) *уязвимости* целостности актива $\boldsymbol{A}_n$ соответственно;

$\mu_a(T|\boldsymbol{A}_n)$ и $\mu_a(V|\boldsymbol{A}_n)$ – мера (степень) реализации *угрозы безопасности* и мера (степень) *уязвимости* доступности актива $\boldsymbol{A}_n$ соответственно.

Значения всех мер μ заданы в интервале $(0 \div 1)$.

Определим меры *риско*в (*risk*) конфиденциальности, целостности и доступности актива $\boldsymbol{A}_n$ (n = 1, 2, …, N) в виде нечеткого И:

$$\mu_c(R|\boldsymbol{A}_n) = k_c(\boldsymbol{A}_n)\ \mu_c(T|\boldsymbol{A}_n)\ \mu_c(V|\boldsymbol{A}_n); \quad (1)$$

$$\mu_i(R|\boldsymbol{A}_n) = k_i(\boldsymbol{A}_n)\ \mu_i(T|\boldsymbol{A}_n)\ \mu_i(V|\boldsymbol{A}_n);$$

$$\mu_a(R|A_n) = k_a(\boldsymbol{A}_n)\ \mu_a(T|\boldsymbol{A}_n)\ \mu_a(V|\boldsymbol{A}_n),$$

где

$$k_c(\boldsymbol{A}_n) = K_c(\boldsymbol{A}_n)/[K_c(\boldsymbol{A}_n) + K_i(\boldsymbol{A}_n) + K_a(\boldsymbol{A}_n)]; \quad (2)$$

$$k_i(\boldsymbol{A}_n) = K_i(\boldsymbol{A}_n)/[K_c(\boldsymbol{A}_n) + K_i(\boldsymbol{A}_n) + K_a(\boldsymbol{A}_n)];$$

$$k_a(\boldsymbol{A}_n) = K_a(\boldsymbol{A}_n)/[K_c(\boldsymbol{A}_n) + K_i(\boldsymbol{A}_n) + K_a(\boldsymbol{A}_n)],$$

а меры угроз безопасности и меры уязвимости будем считать независимыми.

Тем самым в (1) все три меры $\mu_c(R|\boldsymbol{A}_n)$, $\mu_i(R|\boldsymbol{A}_n)$ и $\mu_a(R|A_n)$ рисков R (конфиденциальности, целостности и доступности) для актива $\boldsymbol{A}_n$ (n = 1, 2, …, N) определены произведением нормированных коэффициентов (2) важности этих критериев

на меры реализации соответствующих угроз и меры уязвимости конфиденциальности, целостности и доступности.

Задача заключается в том, чтобы оценить влияние рисков на агрегаты ($\boldsymbol{A}_{123}$, A_{45}, $\boldsymbol{A}_{12345}$) всех уровней, формируемых из соответствующих ресурсов с учетом однонаправленных связей графа, представленного на рис. 1.

2. Устойчивости агрегатов информационной системы к угрозам информационной безопасности

2.1. Устойчивости активов

Будем считать, что риски конфиденциальности, целостности и доступности не являются независимыми, и будем рассчитывать значение риска для каждого актива $\boldsymbol{A}_n$ (n = 1, 2, …, N), используя рекурсию [12]:

$$\mu_{ci}(R|\boldsymbol{A}_n) = \mu_c(R|\boldsymbol{A}_n) + \mu_i(R|\boldsymbol{A}_n) - \mu_c(R|\boldsymbol{A}_n)\,\mu_i(R|\boldsymbol{A}_n)]; \quad (3)$$

$$\mu_{cia}(R|\boldsymbol{A}_n) = \mu_{ci}(R|\boldsymbol{A}_n) + \mu_a(R|\boldsymbol{A}_n) - \mu_{ci}(R|\boldsymbol{A}_n)\,\mu_a(R|\boldsymbol{A}_n).$$

Тогда из (3) получим выражение для расчета совокупной меры риска для каждого актива $\boldsymbol{A}_n$:

$$\mu_{cia}(\boldsymbol{A}_n) = \mu_c(\boldsymbol{A}_n) + \mu_i(\boldsymbol{A}_n) + \mu_a(\boldsymbol{A}_n) - \quad (4)$$

$$- \mu_c(\boldsymbol{A}_n)\,\mu_i(\boldsymbol{A}_n) - \mu_c(\boldsymbol{A}_n)\,\mu_a(\boldsymbol{A}_n) - \mu_i(\boldsymbol{A}_n)\,\mu_a(\boldsymbol{A}_n) + \mu_c(\boldsymbol{A}_n)\,\mu_i(\boldsymbol{A}_n)\,\mu_a(A_n).$$

Полученное выражение имеет простой физический смысл: первые три слагаемых оценивают результирующую степень риска конфиденциальности, целостности и доступности без учета их зависимости, вторые три слагаемые учитывают вклад их двойных корреляций, а последнее слагаемое – вклад тройной корреляции.

Предположим, что динамика реализации одиночной угрозы безопасности конфиденциальности, целостности и доступности, связанных с динамикой активности *ACT(t) (activity)* угроз и противодействия *C(t) (counteraction)* им, описывается для каждой составляющей актива $\boldsymbol{A}_n$ простейшей кинетической зависимостью, которая согласуется с качественной моделью, предложенной в [5]:

$$\frac{d\mu}{dt} = -\frac{\mu}{\tau} + AVT(t) - C(t) = -\frac{\mu}{\tau} + \Delta ACT(t),\ \mu(t_0) = 0,\ \Delta ACT_{max} = \frac{1}{\tau}, \quad (5)$$

где τ – время релаксации угрозы в отсутствии ее активности, t_0 – случайное время начала реализации угрозы, ΔACT – скомпенсированная активность угрозы за счет принятия мер противодействия.

Заметим, что среди базовых угроз, законодательно закрепленных регулятором (Министерство энергетики РФ) в структуре процедуры категорирования объектов топливно-энергетического комплекса (ТЭК), угроза «технического воздействия» встречается в более чем 75% случаев («Методические рекомендации по анализу уязвимости производственно-технологического процесса и выявлению критических элементов объекта, оценке социально-экономических последствий совершения на объекте террористического акта и антитеррористической защищенности объекта при проведении категорирования и составлению паспорта безопасности объекта топливно-энергетического комплекса». Минэнерго России. М.: 2012). При этом речь идет о воздействии на автоматизированные системы управления технологическими процессами (АСУ ТП) критических элементов. В качестве потенциального нарушителя рассматривается и руководитель установки, который действует совместно с представителем соответствующей службы.

Поэтому можно предположить, что динамика активности угроз зависит от субъекта, участвующего в технологическом информационном процессе.

Рассмотрим случай, когда характерное время изменения активности много меньше времени τ, а активность угрозы изменяется «скачком» (от 0 до ΔACT) и продолжается некоторое характерное время, большее τ. Тогда (5) имеет аналитическое решение:

$$\mu(t) = \tau \Delta ACT \left[1 - \exp\left(-\frac{t-t_0}{\tau}\right)\right], \quad (6)$$

где $\mu(t)$ – мера риска для составляющей актива.

Из (6) следует, что при $\Delta ACT = \Delta ACT_{max}$:

$$\mu(t) = \left[1 - \exp\left(-\frac{t-t_0}{\tau}\right)\right], \text{ а } \mu_{max} = 1. \quad (7)$$

Исходя из (7), величину $1 - \mu(t) = \exp\left(-\frac{t-t_0}{\tau}\right)$ будем рассматривать, как *степень устойчивости* к угрозам – с ростом степени реализации угрозы (от 0 до 1) степень устойчивости падает (от 1 до 0).

Далее, по аналогии с (7) и используя (4) введем степени $s_{cia}(\boldsymbol{A_n})$ устойчивости (*sustainability, resilience*) к угрозам каждого актива $\boldsymbol{A}_n$ (n = 1, 2, …, N):

$$s_{cia}(\boldsymbol{A}_n) = 1 - \mu_{cia}(\boldsymbol{A}_n). \quad (8)$$

2.2. Устойчивости агрегатов активов

Рассмотрим возможные методы оценивания степеней устойчивости к угрозам агрегатов всех иерархических уровней графа информационной системы, представленного на рис. 2.

Для расчёта введем для всех активов $\boldsymbol{A}_n$ (n = 1, 2, …, N) коэффициенты $K(\boldsymbol{A}_n)$ их «весомости», а нормированные коэффициенты их значимости пересчитаем по аналогии с (2):

$$k(\boldsymbol{A}_n) = K(\boldsymbol{A}_n) / \sum_{n=1}^{N} K(\boldsymbol{A}_n). \quad (9)$$

При расчетах будем учитывать случаи отношений элементов агрегатов из [11].

2.3. Устойчивость агрегата при полностью независимых активах

Определим степень устойчивости агрегата $\boldsymbol{A}_{123}$, как:

$$s_{cia}(\boldsymbol{A}_{123}) = k(\boldsymbol{A}_1)\, s_{cia}(\boldsymbol{A}_1) + k(\boldsymbol{A}_2)\, s_{cia}(\boldsymbol{A}_2) + k(\boldsymbol{A}_3)\, s_{cia}(\boldsymbol{A}_3), \quad (10)$$

$$k(\boldsymbol{A}_1) + k(\boldsymbol{A}_2) + k(\boldsymbol{A}_3) = 1,$$

$$s_{cia}(\boldsymbol{A}_{45}) = k(\boldsymbol{A}_4)\, s_{cia}(\boldsymbol{A}_4) + k(\boldsymbol{A}_5)\, s_{cia}(\boldsymbol{A}_5),$$

$$k(\boldsymbol{A}_4) + k(\boldsymbol{A}_5) = 1.$$

В этом случае выход из строя одного из элементов агрегата (обнуление его устойчивости) не приведет к потере устойчивости всего агрегата.

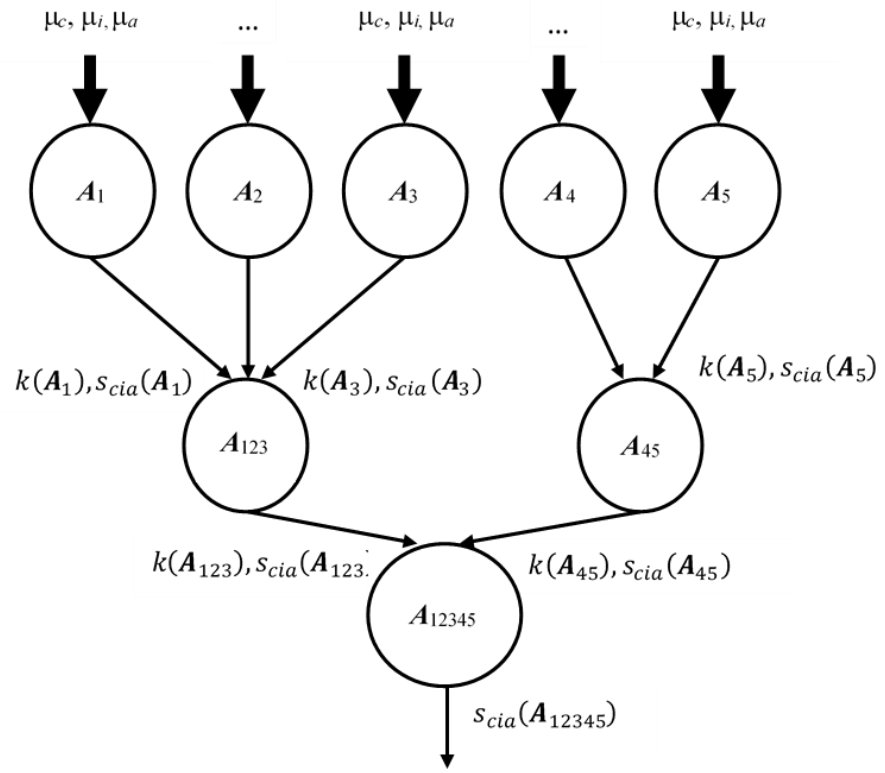


Рис. 2. Граф расчета устойчивости агрегатов ИС
Fig. 2. Graph for calculating the stability of IS aggregates

2.4. Устойчивость агрегата при слабой зависимости активов

Определим степень устойчивости таких агрегатов на основе рекурсии парных взаимодействий (корреляций) их элементов. Так, для агрегата $\boldsymbol{A}_{123}$ (рис. 2):

$$s_{cia}(\boldsymbol{A}_{12}) = \frac{k(\boldsymbol{A}_1)\, s_{cia}(\boldsymbol{A}_1) + k(\boldsymbol{A}_2)\, s_{cia}(\boldsymbol{A}_2) - k(\boldsymbol{A}_1)k(\boldsymbol{A}_2)s_{cia}(\boldsymbol{A}_1)s_{cia}(\boldsymbol{A}_2)}{k(\boldsymbol{A}_1) + k(\boldsymbol{A}_2) - k(\boldsymbol{A}_1)k(\boldsymbol{A}_2)}, \tag{11}$$

$$k(\boldsymbol{A}_{12}) = k(\boldsymbol{A}_1) + k(\boldsymbol{A}_2) - k(\boldsymbol{A}_1)k(\boldsymbol{A}_2), k(\boldsymbol{A}_1) + k(\boldsymbol{A}_2) + k(\boldsymbol{A}_3) = 1.$$

$$s_{cia}(\boldsymbol{A}_{123}) = \frac{k(\boldsymbol{A}_{12})\, s_{cia}(\boldsymbol{A}_{12}) + k(\boldsymbol{A}_3)\, s_{cia}(\boldsymbol{A}_3) - k(\boldsymbol{A}_{12})k(\boldsymbol{A}_3)s_{cia}(\boldsymbol{A}_{12})s_{cia}(\boldsymbol{A}_3)}{k(\boldsymbol{A}_{12}) + k(\boldsymbol{A}_3) - k(\boldsymbol{A}_{12})k(\boldsymbol{A}_3)} =$$

$$= \frac{k(\boldsymbol{A}_1)\, s_{cia}(\boldsymbol{A}_1) + k(\boldsymbol{A}_2)\, s_{cia}(\boldsymbol{A}_2) + k(\boldsymbol{A}_3)\, s_{cia}(\boldsymbol{A}_3)}{k(\boldsymbol{A}_1) + k(\boldsymbol{A}_2) + k(\boldsymbol{A}_3) - k(\boldsymbol{A}_1)k(\boldsymbol{A}_2) - k(\boldsymbol{A}_1)k(\boldsymbol{A}_3) - k(\boldsymbol{A}_2)k(\boldsymbol{A}_3) + k(\boldsymbol{A}_1)\, k(\boldsymbol{A}_2)\, k(\boldsymbol{A}_3)} - \tag{12}$$

$$- \frac{k(\boldsymbol{A}_1)k(\boldsymbol{A}_2)s_{cia}(\boldsymbol{A}_1)s_{cia}(\boldsymbol{A}_2) + k(\boldsymbol{A}_1)k(\boldsymbol{A}_3)s_{cia}(\boldsymbol{A}_1)s_{cia}(\boldsymbol{A}_3) + k(\boldsymbol{A}_2)k(\boldsymbol{A}_3)s_{cia}(\boldsymbol{A}_2)s_{cia}(\boldsymbol{A}_3)}{k(\boldsymbol{A}_1) + k(\boldsymbol{A}_2) + k(\boldsymbol{A}_3) - k(\boldsymbol{A}_1)k(\boldsymbol{A}_2) - k(\boldsymbol{A}_1)k(\boldsymbol{A}_3) - k(\boldsymbol{A}_2)k(\boldsymbol{A}_3) + k(\boldsymbol{A}_1)\, k(\boldsymbol{A}_2)\, k(\boldsymbol{A}_3)} +$$

$$+ \frac{k(\boldsymbol{A}_1)k(\boldsymbol{A}_2)k(\boldsymbol{A}_3)s_{cia}(\boldsymbol{A}_1)s_{cia}(\boldsymbol{A}_2)s_{cia}(\boldsymbol{A}_3) +}{k(\boldsymbol{A}_1) + k(\boldsymbol{A}_2) + k(\boldsymbol{A}_3) - k(\boldsymbol{A}_1)k(\boldsymbol{A}_2) - k(\boldsymbol{A}_1)k(\boldsymbol{A}_3) - k(\boldsymbol{A}_2)k(\boldsymbol{A}_3) + k(\boldsymbol{A}_1)\, k(\boldsymbol{A}_2)\, k(\boldsymbol{A}_3)}.$$

Первое слагаемое в (12) соответствует отсутствию зависимости активов, второе – их парным корреляциям, а третье – тройным корреляциям.

Корреляция или слабое взаимодействие дает значительный синергетический эффект повышения устойчивости агрегата. Рассмотрим этот синергетический эффект $\Delta s_{cia}(\boldsymbol{A}_{45})$, например, для агрегата $\boldsymbol{A}_{45}$:

$$\Delta s_{cia}(\boldsymbol{A}_{45}) = \frac{k(\boldsymbol{A}_4)\, s_{cia}(\boldsymbol{A}_4) + k(\boldsymbol{A}_5)\, s_{cia}(\boldsymbol{A}_5) - k(\boldsymbol{A}_4)k(\boldsymbol{A}_5)s_{cia}(\boldsymbol{A}_4)s_{cia}(\boldsymbol{A}_5)}{k(\boldsymbol{A}_4) + k(\boldsymbol{A}_5) - k(\boldsymbol{A}_4)k(\boldsymbol{A}_5)} -$$

$$- \frac{k(\boldsymbol{A}_4)\, s_{cia}(\boldsymbol{A}_4) + k(\boldsymbol{A}_5)\, s_{cia}(\boldsymbol{A}_5)}{k(\boldsymbol{A}_4) + k(\boldsymbol{A}_5)} . \quad (13)$$

Максимальный синергетический эффект – увеличение площади под поверхностью $\Delta s_{cia}(\boldsymbol{A}_{45})$ достигается при $k(\boldsymbol{A}_4) = k(\boldsymbol{A}_5) = 0.5$.

При слабом взаимодействии потеря устойчивости одним из активов также не приводит к потере устойчивости агрегата.

2.5. Устойчивость агрегата при сильной зависимости активов

На содержательном уровне сильное взаимодействие активов обусловлено их полной взаимозависимостью. Определим степень устойчивости агрегатов при сильном взаимодействии их парных элементов, как:

$$s_{cia}(\boldsymbol{A}_{12}) = \frac{k(\boldsymbol{A}_1)k(\boldsymbol{A}_2)s_{cia}(\boldsymbol{A}_1)s_{cia}(\boldsymbol{A}_2)}{k(\boldsymbol{A}_1) + k(\boldsymbol{A}_2) - k(\boldsymbol{A}_1)k(\boldsymbol{A}_2)}. \quad (14)$$

Тогда для агрегата $\boldsymbol{A}_{123}$ получим:

$$s_{cia}(\boldsymbol{A}_{123}) = \quad (15)$$

$$= \frac{k(\boldsymbol{A}_1)k(\boldsymbol{A}_2)s_{cia}(\boldsymbol{A}_1)s_{cia}(\boldsymbol{A}_2) + k(\boldsymbol{A}_1)k(\boldsymbol{A}_3)s_{cia}(\boldsymbol{A}_1)s_{cia}(\boldsymbol{A}_3) + k(\boldsymbol{A}_2)k(\boldsymbol{A}_3)s_{cia}(\boldsymbol{A}_2)s_{cia}(\boldsymbol{A}_3)}{k(\boldsymbol{A}_1) + k(\boldsymbol{A}_2) + k(\boldsymbol{A}_3) - k(\boldsymbol{A}_1)k(\boldsymbol{A}_2) - k(\boldsymbol{A}_1)k(\boldsymbol{A}_3) - k(\boldsymbol{A}_2)k(\boldsymbol{A}_3) + 2\,k(\boldsymbol{A}_1)\,k(\boldsymbol{A}_2)\,k(\boldsymbol{A}_3)} -$$

$$\frac{2\,k(\boldsymbol{A}_1)k(\boldsymbol{A}_2)k(\boldsymbol{A}_3)s_{cia}(\boldsymbol{A}_1)s_{cia}(\boldsymbol{A}_2)s_{cia}(\boldsymbol{A}_3)}{k(\boldsymbol{A}_1) + k(\boldsymbol{A}_2) + k(\boldsymbol{A}_3) - k(\boldsymbol{A}_1)k(\boldsymbol{A}_2) - k(\boldsymbol{A}_1)k(\boldsymbol{A}_3) - k(\boldsymbol{A}_2)k(\boldsymbol{A}_3) + 2\,k(\boldsymbol{A}_1)\,k(\boldsymbol{A}_2)\,k(\boldsymbol{A}_3)}.$$

Так, при $k(\boldsymbol{A}_1) = k(\boldsymbol{A}_2) = k(\boldsymbol{A}_3)$ и $s_{cia}(\boldsymbol{A}_1) = s_{cia}(\boldsymbol{A}_2) = s_{cia}(\boldsymbol{A}_3) = 1$ получим $s_{cia}(\boldsymbol{A}_{123}) \cong 1$. При $s_{cia}(\boldsymbol{A}_1) = 0$, $s_{cia}(\boldsymbol{A}_2) = s_{cia}(\boldsymbol{A}_3) = 1$ получим $s_{cia}(\boldsymbol{A}_{123}) \cong 0.02$.

Тем самым, выход из строя одного актива приводит к потере устойчивости агрегата.

2.6. Устойчивость подсистем с обратной связью.

На рис. 3 приведен граф элементарной подсистемы с обратной связью (*feedback*).

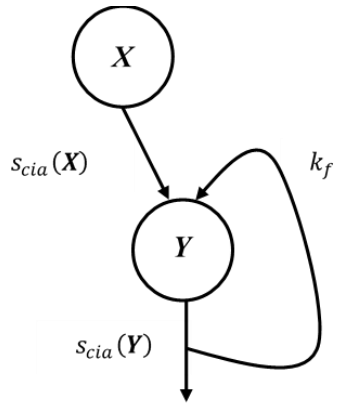


Рис. 3. Граф элементарной подсистемы с обратной связью
Fig. 3. Elementary Subsystem Graph with Feedback

В соответствии с (12) выход подсистемы $s_{cia}(\boldsymbol{Y})$ связан с ее входом $s_{cia}(\boldsymbol{X})$ уравнением:

$$s_{cia}(\boldsymbol{Y}) = \frac{s_{cia}(\boldsymbol{X})}{1 - k_f[1 - s_{cia}(\boldsymbol{X})]}, \quad (16)$$

где k_f – коэффициент обратной связи ($k_f \leq 1$).

Из (16) следует, что обратная связь увеличивает устойчивость подсистемы. На рис. 4 приведен пример отклика $s_{cia}(\boldsymbol{Y})$ данной подсистемы на входное воздействие $s_{cia}(\boldsymbol{X})$ при разных коэффициентах k_f обратной связи.

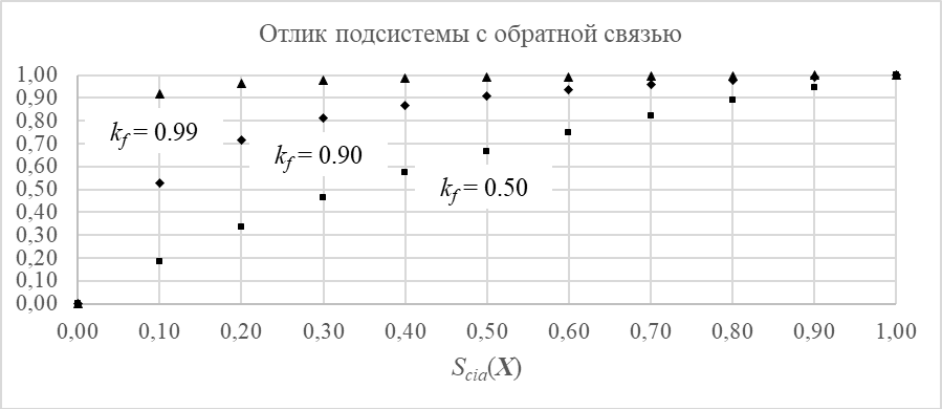


Рис. 4. Увеличение устойчивости подсистемы за счет обратной связи
Fig. 4. Increasing the stability of the subsystem due to feedback

На рис.5 приведен граф подсистемы $\boldsymbol{A}_{45}$, агрегирующей два актива и имеющей обратную связь с коэффициентом k_f. При этом активы могут быть связаны как слабой, так и сильной зависимостями.

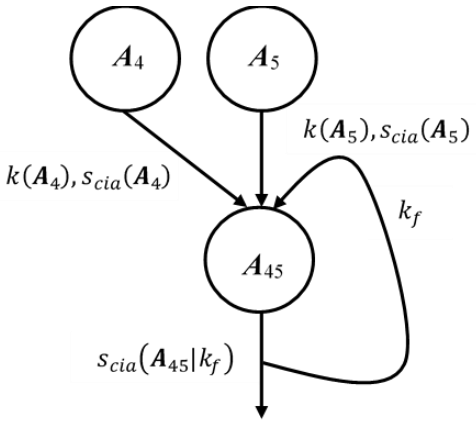


Рис. 5. Граф парной подсистемы с обратной связью
Fig. 5. The graph of the paired subsystem with feedback

В соответствии с (11) и (15) выход $s_{cia}(\boldsymbol{A}_{45})$ подсистемы $s_{cia}(\boldsymbol{A}_{45})$ связан с ее входами $s_{cia}(A_4)$ и $s_{cia}(A_5)$ уравнением:

$$s_{cia}(\boldsymbol{A}_{45}|k_f) = \frac{s_{cia}(\boldsymbol{A}_{45})}{1 - k_f[1 - s_{cia}(\boldsymbol{A}_{45})]}, \quad (17)$$

где устойчивость парного агрегата рассчитывается в соответствии с (12).

Как видно из (17) обратная связь увеличивает устойчивость агрегированной подсистемы наряду с синергизмом (12), обусловленным взаимодействием ее элементов. На рис. 6 приведена поверхность синергетического эффекта, обусловленного обратной связью (для случая слабой зависимости, $k_f = k(A_4) = k(A_5) = 0.5$), описываемая уравнением:

$$\Delta s_{cia}(\boldsymbol{A}_{45}|k_f) = s_{cia}(\boldsymbol{A}_{45}|k_f) - s_{cia}(\boldsymbol{A}_{45}|k_f = 0). \quad (18)$$

Обратная связь увеличивает синергетический эффект дополнительно к парному взаимодействию.

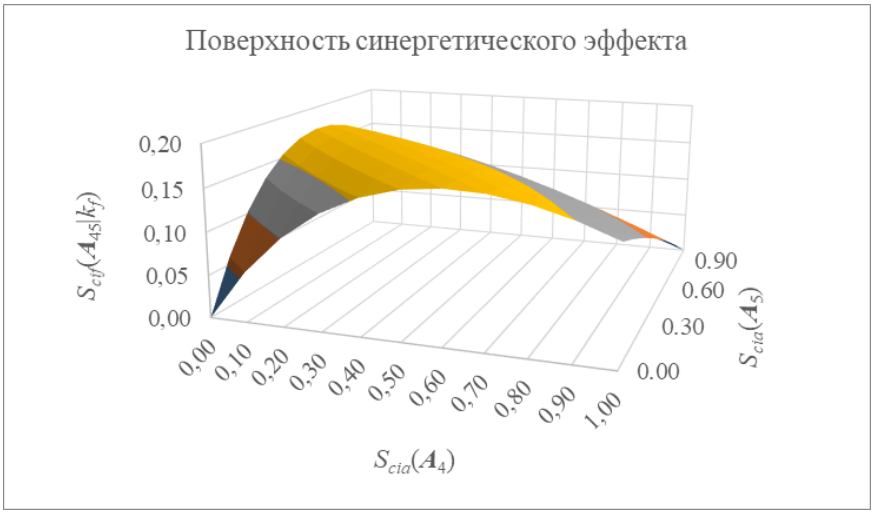


Рис. 6. Поверхность синергетического эффекта устойчивости для парной агрегированной подсистемы с обратной связью.
Fig. 6. Surface of the synergistic effect of resistance for paired aggregated subsystem with feedback.

3. Обсуждение результатов

Из приведенного рассмотрения следует, что наиболее подвержены риску взаимозависимые активы ИС, у которых потеря устойчивости хоты бы одного из них приводит к потере устойчивости всех подсистем или агрегатов, состоящих их этих активов. Поэтому в практическом отношении необходимо хотя бы дублирование таких подсистем.

Так, например, безмасштабные сети очень устойчивы к случайным повреждениям или внешним случайным воздействиям [14]. Однако, у таких сетей существует своеобразная «Ахиллесова пята» – целенаправленное повреждение одного или нескольких узлов с большим числом связей ведет к дезинтеграции сети [15]. Например, хакер может существенно повредить WWW, если выведет из строя один или несколько сайтов с большим числом связей.

При определении приоритетной комбинации отказов в результате развития аварийной ситуации, предполагается проектирование физических барьеров, которые будут «караулить» возможную аварийную ситуация.

Поэтому дублирование в информационных системах является «зеркальным» мероприятием для обеспечения информационной безопасности и безопасности объекта в целом.

Независимые активы ИС, или ресурсы, связанные слабой зависимостью, устойчивы к рискам, приводящим к потерям устойчивости хоты бы одного из активов, или даже

нескольких активов. В то же время, слабая зависимость активов дает синергетический эффект – эффект повышения ее устойчивости.

Зависимости активов, формируемые в ИС с помощью обратных связей, наряду с их слабыми зависимостями также повышают устойчивость систем.

Полученные результаты согласуются с работами в области новой парадигмы, отражающей, в отличие от редукционизма, важность рассмотрения современных сетевых систем [16] и проблем безопасности сложных технических объектов [17] на системном уровне. Основной вывод – необходимо изучать не только отдельные составляющие таких объектов, но, главным образом, их связи.

Рассмотренный материал можно аппроксимировать применительно к критическим элементам объектов ТЭК (Методические рекомендации Минэнерго России от 10.10.2012). В соответствии с методикой определения категории потенциальной опасности, по каждому объекту ТЭК в результате анализа уязвимости производственно-технологических процессов выделяются критические элементы (КЭ).

Очевидно, что к выделенным критическим элементам ТЭК специалисты вправе отнести объекты КИИ по ФЗ 187 от 26.07.2017, в частности, автоматизированные системы управления технологическими процессами, которые обеспечивают функционирование КЭ.

Устойчивость агрегатов информационной системы к угрозам информационной безопасности в каждый конкретный момент времени позволяет сделать вывод о стабильности информационной системы на исследуемом интервале времени.

Аналогично понятию устойчивости системы информационной безопасности будет полезно ввести понятие «стабильности»: взаимосвязь мер уязвимости системы информационной безопасности со «стабильностью» внешнего контура системы безопасности очевидна. Рассмотрим эту аналогию.

Под «стабильностью», в числовом выражении (в интервале от 0 до 1), подразумевается степень безопасности системы, характеризующая способность элементов системы безопасности штатно реагировать на воздействия внешних факторов, направленных на разрушение системы. Рассмотрим понятие стабильности ИС на примере элемента КИИ, описываемого графом на рис. 1, связывающего активы или ресурсы $\boldsymbol{A}_1$, $\boldsymbol{A}_2$, $\boldsymbol{A}_3$, $\boldsymbol{A}_4$, $\boldsymbol{A}_5$.

Для каждого ресурса $\boldsymbol{A}_n$ (n = 1, 2, …, N) можно определить степень его стабильности, оценив критерии КД($\boldsymbol{A}_n$), КЦ($\boldsymbol{A}_n$) и КЗ($\boldsymbol{A}_n$) стабильности, как показатели достаточности, целостности и значимости, и их важности *Imp*(КД($\boldsymbol{A}_n$)), *Imp*(КЦ($\boldsymbol{A}_n$)) и *Imp*(КЗ($\boldsymbol{A}_n$)), соответственно. При этом физический смысл критериев КД, КЦ и КЗ стабильности определяются как:

КД – критерий достаточности (набор функциональных возможностей ресурса достаточен для того, чтобы соответствовать заданному уровню оценки эффективности системы при наличии необходимого перечня таких возможностей). Определяется с использованием программного продукта САПР «Амулет» [18–19];

КЦ – критерий целостности (условия существования и степень надежности ресурса). Определяется экспертами в интервале от 0 до 1, где 0 – не надежно, а 1 – надежно;

КЗ – критерий значимости (важность функционирования данного ресурса для функционирования системы в целом). Чем выше степень зависимости системы от данного элемента, тем более уязвимым является данная область контроля.

Тогда, определив значения каждого критерия и их важности, вычислим степень стабильности (*stability*) ресурса по формуле:

$$St(\boldsymbol{A}_n) = Imp\big(\text{КД}(\boldsymbol{A}_n)\big)\cdot \text{КД}(\boldsymbol{A}_n) + Imp\big(\text{КЦ}(\boldsymbol{A}_n)\big)\cdot \text{КЦ}(\boldsymbol{A}_\text{n}) + \\ + Imp\big(\text{КЗ}(\boldsymbol{A}_n)\big)\cdot\big(1-\text{КЗ}(\boldsymbol{A}_n)\big). \quad (19)$$

Для данного определения также вводятся ограничения типа (2) на сумму важностей критериев КД(R_n), КЦ(R_n) и КЗ(R_n): $Imp(\text{КД}(\boldsymbol{A}_n)) + Imp(\text{КЦ}(\boldsymbol{A}_n)) + Imp(\text{КЗ}(\boldsymbol{A}_n)) = 1$.

Степень стабильности системы должна быть не менее 0,95, т.е. допускается отклонение от полной стабильности не больше, чем на 5%.

Пример. Определим степень стабильности ресурса $\boldsymbol{A}_n$. Для этого экспертным методом назначим важность критериев, как приведено в табл. 1.

Таблица 1. Важность критериев стабильности

Обозначение	**Значение**
$Imp(\text{КД}(\boldsymbol{A}_n))$	0,40
$Imp(\text{КЦ}(\boldsymbol{A}_n))$	0,35
$Imp(\text{КЗ}(\boldsymbol{A}_n))$	0,25

Затем с помощью программного продукта САПР «Амулет» определим значение КД($\boldsymbol{A}_n$), как 0,95. С помощью метода экспертной оценки [20] определим надежность КЦ($\boldsymbol{A}_n$) данного ресурса, как 0,65. Проанализировав систему в целом, оценим значение КЗ($\boldsymbol{A}_n$) ресурса, как 0,85. Полученные данные приведены в табл. 2.

Таблица 2. Результаты оценки важности и значений критериев стабильности

Важность критериев		**Значения критериев**	
Обозначение	**Значение**	**Обозначение**	**Значение**
$Imp(\text{КД}(\boldsymbol{A}_n))$	0,40	КД($\boldsymbol{A}_n$)	0,95
$Imp(\text{КЦ}(\boldsymbol{A}_n))$	0,35	КЦ($\boldsymbol{A}_n$)	0,65
$Imp(\text{КЗ}(\boldsymbol{A}_n))$	0,25	КЗ($\boldsymbol{A}_n$)	0,85

Затем, оценим степень стабильности ресурса:

$$St(\boldsymbol{A}_n) = 0{,}40 \cdot 0{,}95 + 0{,}35 \cdot 0{,}65 + 0{,}25 \cdot (1 - 0{,}85) = 0{,}65.$$

Как видно, полученное значение стабильности ниже допустимого. Поэтому необходимо обеспечить наибольшую безопасность данному ресурсу.

Логично, что, исходя из важности критериев, разумно вносить изменения на те активы системы, которые увеличат значения критериев с наибольшей важностью (в рассматриваемом примере – коэффициент КД) [21, 22].

После анализа системы и увеличения ее безопасности были получены следующие значения коэффициентов (табл. 3).

Таблица 3. Результаты оценки важности и значений коэффициентов с увеличенной безопасностью

Важность коэффициентов		**Значения коэффициентов**	
Обозначение	**Значение**	**Обозначение**	**Значение**
$Imp(\text{КД}(\boldsymbol{A}_n))$	0,40	КД($\boldsymbol{A}_n$)	0,98
$Imp(\text{КЦ}(\boldsymbol{A}_n))$	0,35	КЦ($\boldsymbol{A}_n$)	0,95
$Imp(\text{КЗ}(\boldsymbol{A}_n))$	0,25	КЗ($\boldsymbol{A}_n$)	0,08

При этом степень стабильности ресурса равна 0,95: (0,4*0,98+0,35*0,95+0,25*(1-0,08) = 0,9545).

Заметим, что степень стабильности системы в целом, с учетом всех ресурсов и их связей возможно также рассчитывать по вышеизложенной методике оценивания устойчивости системы.

Заключение

Предложенный подход не является методикой организации связей ресурсов ИС для обеспечения ее информационной безопасности. Однако, при наличии установленных связей между активами системы, он позволяет провести оценивание устойчивости как ее информационных подсистем, так и системы в целом к всевозможным угрозам информационной безопасности. Хотя в работе и рассмотрены простейшие примеры структур связей активов ИС, показано, что четыре вида их отношений (независимость, слабая зависимость, сильная зависимость, обратная связь) позволяют рекуррентно вычислять устойчивость систем при любых структурах связей. Поскольку в основе устойчивости находятся модели рисков и угроз, то полученная модель устойчивости может быть применена к их различным модификациям.

Предложенный подход, связывающий устойчивость элементов системы информационной безопасности с ее устойчивостью для разных видов связей элементов, позволяет также оценивать и стабильность как отдельных элементов системы, так и системы в целом.

Кроме того, оценивание стабильности системы способно повлиять на формирование дополнительно к комплексу компенсационных мероприятий средств и систем физической защиты таблицы результатов предпроектных расчетов устойчивости в границах АСУ ТП соответствующего критического элемента КИИ.

СПИСОК ЛИТЕРАТУРЫ:

1. Wawrzyniak D. (2006) Information Security Risk Assessment Model for Risk Management. In: Fischer-Hübner S., Furnell S., Lambrinoudakis C. (eds) Trust and Privacy in Digital Business. TrustBus 2006. Lecture Notes in Computer Science. Vol. 4083. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/11824633_3.
2. Кононов А.А., Котельников А.П., Черныш К.В. Оценка защищенности критически важных объектов на основе построения моделей событий рисков. Труды ИСА РАН. Т. 62, Вып. 4, 2012. С. 69–75. URL: http://www.isa.ru/proceedings/images/documents/2012-62-4/t-4-12_69-75.pdf. (дата обращения: 01.11.2020).
3. Liu S., Kuhn R., Rossman H. Understanding insecire IT: Practical risk assessment. IT Professional Magazine. V. 11, no. 3, 2009. P. 57–59. DOI: https://doi.org/10.1109/MITP.2009.62.
4. Shukla N., Kumar S. A comparative study on information security risk analysis practices // Special Issue of International Journal of Computer Applications. P. 28–33, 2012.
5. Bandopadhyay S., Sengupta A., Mazumdar C. A quantitative methodology for information security control gap analysis," Proceedings of the 2011 International Conference on Communication, Computing & Security – ICCCS '11, 2011. DOI: https://doi.org/10.1145/1947940.1948051.
6. Shapiro Arnold F., Koissi Marie-Claire. Risk Assessment Applications of Fuzzy Logic. Casualty Actuarial Society, Canadian Institute of Actuaries, Society of Actuaries, 2015. – 112 p. URL: https://www.soa.org/globalassets/assets/Files/Research/Projects/2015-risk-assess-apps-fuzzy-logic.pdf (дата обращения: 01.11.2020).
7. Ana Paula Henriques de Gusmão, Lúcio Camara e Silva, Maisa Mendonça Silva, Thiago Poleto, Ana Paula Cabral Seixas Costa. Information security risk analysis model using fuzzy decision theory // International Journal of Information Management. V. 36, Issue 1, 2016. P. 25–34. DOI: https://doi.org/10.1016/j.ijinfomgt.2015.09.003.
8. Abdo H., Flaus J-M. A mixed fuzzy probabilistic approach for risk assessment of dynamic systems //IFAC-PapersOnLine. V. 48, Issue 3, 2015. P. 960–965. DOI: https://doi.org/10.1016/j.ifacol.2015.06.207.
9. Sami Haji, Qing Tan, Rebeca Soler Costa. A Hybrid Model for Information Security Risk Assessment. International Journal of Advanced Trends in Computer Science and Engineering. Vol. 8, no. 1, 2019. P. 100–106. DOI: https://doi.org/10.30534/ijatcse/2019/1981.12019.
10. Krasnova T.N., Kryukova I.P., Krasnov A.E. et al. Principles of formalization of the syndrome diagnosis used in an automated system of management of patients. Biomed Eng. V. 32, 1998. P. 140–147. DOI: https://doi.org/10.1007/BF02369144.
11. Краснов А.Е., Сагинов Ю.Л., Феоктистова Н.А. Количественное оценивание качества многопараметрических объектов и процессов на основе нейросетевой технологии. В сб. научных трудов Всероссийской конференции «Информационные технологии, менеджмент качества, информационная

безопасность» (IT&MQ&IS-2015) - (20–25 мая 2015 г.). Учебно-научная база КБГУ в Приэльбрусье (п. Эльбрус). Приложение к журналу «Качество. Инновации. Образование». Т. 2, № 5, 2015. С. 97–108. URL: http://quality-journal.ru/wp-content/uploads/2016/07/ITMQIS-2015.pdf. (дата обращения: 01.11.2020).

12. Краснов А.Е., Надеждин Е.Н., Никольский Д.Н., Калачев А.А. Нейросетевой подход к проблеме оценивания эффективности функционирования организации на основе агрегирования показателей ее деятельности. Информатизация образования и науки, № 1 (33), 2017. С. 141–154. URL: https://informika.ru/pechatnye-izdaniya/zhurnal-informatizaciya-obrazovaniya-i-nauki/arhiv-vypuskov/2017/vypusk-n33/. (дата обращения: 01.11.2020).
13. Krasnov A., Pivneva S. (2021) Hierarchical Quasi-Neural Network Data Aggregation to Build a University Research and Innovation Management System. In: Murgul V., Pukhkal V. (eds) International Scientific Conference Energy Management of Municipal Facilities and Sustainable Energy Technologies EMMFT 2019. EMMFT 2019. Advances in Intelligent Systems and Computing. V. 1259. Springer, Cham. P. 12–15. DOI: https://doi.org/10.1007/978-3-030-57453-6_2.
14. Albert R., Barabasi A.-L. Statistical mechanics of complex networks. Rev. Mod. Phys. V. 74, Issue 1, 2002. P. 47–97. DOI: https://doi.org/10.1103/RevModPhys.74.47.
15. Barabási A.-L. The network takeover. Nature Phys. V. 8, 2012. P. 4–16. DOI: https://doi.org/10.1038/nphys2188.
16. Евин И.А. Введение с теорию сложных сетей. Компьютерные исследования и моделирование. Т. 2, № 2, 2010. С. 121–141. DOI: https://10.20537/2076-7633-2010-2-2-121-141.
17. Мосолов А.С. Универсальная технология проектирования систем инженерно-физической защиты «АМУЛЕТ» с заданным уровнем эффективности. М.: НИЯУ «МИФИ». 2013. – 200 с.
18. Мосолов А.С., Беляева Е.А., Бадиков А.В. Изучение универсального метода проектирования систем инженерно-технической защиты объектов. М.: НИЯУ «МИФИ». 2010. – 84 с.
19. Беляева Е.А., Кузоятов О.П., Мосолов А.С., Новиков Ю.В. Способ проектирования системы комплексной безопасности объекта. Патент RU 2219576 C2. Заявка RU 2002105932, 05.03.2002. Опубликовано 20.12.2003. Бюл. № 35. МПК G06F 17/00.
20. Саати Т. Принятие решений. Метод анализа иерархий. М.: Радио и связь, 1993. – 278 с.
21. Акинин Н.И., Губина Т.А., Мосолов А.С. Алгоритм метода определения приоритетного сценария развития аварийной ситуации на объекте защиты. Кокс и химия: журнал. М.: Металлургиздат, 2019. С. 41–49.
22. Губина Т.А., Мосолов А.С., Мосолов А.А. Система оценки безопасности опасного производственного объекта. Патент RU 2709155 C1. Заявка RU 2019107954, 02.04.2019. Опубликовано 16.12.2019. Бюл. № 35. МПК G06Q 10/06.

REFERENCES:

[1] Wawrzyniak D. (2006) Information Security Risk Assessment Model for Risk Management. In: Fischer-Hübner S., Furnell S., Lambrinoudakis C. (eds) Trust and Privacy in Digital Business. TrustBus 2006. Lecture Notes in Computer Science. Vol. 4083. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/11824633_3.
[2] Kononov A. A., Kotelnikov A. P., Chernysh K. V. Security assessment of critical objects based on the construction of risk event models. Trudy ISA RAN. V. 62, Issue 4, 2012. P. 69–75. URL: http://www.isa.ru/proceedings/images/documents/2012-62-4/t-4-12_69-75.pdf (accessed: 01.11.2020) (in Russian).
[3] Liu S., Kuhn R., Rossman H. Understanding insecire IT: Practical risk assessment. IT Professional Magazine. Vol. 11, no. 3, 2009. P. 57–59. DOI: https://doi.org/10.1109/MITP.2009.62.
[4] Shukla N., Kumar S. A comparative study on information security risk analysis practices. Special Issue of International Journal of Computer Applications. P. 28–33, 2012.
[5] Bandopadhyay S., Sengupta A., Mazumdar C. A quantitative methodology for information security control gap analysis," Proceedings of the 2011 International Conference on Communication, Computing & Security – ICCCS '11, 2011. DOI: https://doi.org/10.1145/1947940.1948051.
[6] Shapiro Arnold F., Koissi Marie-Claire. Risk Assessment Applications of Fuzzy Logic. Casualty Actuarial Society, Canadian Institute of Actuaries, Society of Actuaries, 2015. – 112 p. URL: https://www.soa.org/globalassets/assets/Files/Research/Projects/2015-risk-assess-apps-fuzzy-logic.pdf (accessed: 01.11.2020).
[7] Ana Paula Henriques de Gusmão, Lúcio Camara e Silva, Maisa Mendonça Silva, Thiago Poleto, Ana Paula Cabral Seixas Costa. Information security risk analysis model using fuzzy decision theory // International Journal of Information Management. V. 36, Issue 1, 2016. P. 25–34. DOI: https://doi.org/10.1016/j.ijinfomgt.2015.09.003.

[8] Abdo H., Flaus J-M. A mixed fuzzy probabilistic approach for risk assessment of dynamic systems //IFAC-PapersOnLine. V. 48, Issue 3, 2015. P. 960–965. DOI: https://doi.org/10.1016/j.ifacol.2015.06.207.
[9] Sami Haji, Qing Tan, Rebeca Soler Costa. A Hybrid Model for Information Security Risk Assessment. International Journal of Advanced Trends in Computer Science and Engineering. V. 8, no. 1, 2019. P. 100–106. DOI: https://doi.org/10.30534/ijatcse/2019/1981.12019.
[10] Krasnova T.N., Kryukova I.P., Krasnov A.E. et al. Principles of formalization of the syndrome diagnosis used in an automated system of management of patients. Biomed Eng. V. 32, 1998. P. 140–147. DOI: https://doi.org/10.1007/BF02369144.
[11] Krasnov A.E., Saginov Yu.L., Feoktistova N.A. Quantitative assessment of the quality of multiparameter objects and processes based on neural network technology. Sbornik nauchnyh trudov Vserossijskoj konferencii «Informacionnye tekhnologii, menedzhment kachestva, informacionnaya bezopasnost'» (IT&MQ&IS-2015) - (20–25 maya 2015 g.). Uchebno-nauchnaya baza KBGU v Priel'brus'e (p. El'brus). Prilozhenie k zhurnalu «Kachestvo. Innovacii. Obrazovanie». T. 2, no. 5, 2015. S. 97–108. URL: http://quality-journal.ru/wp-content/uploads/2016/07/ITMQIS-2015.pdf (accessed: 01.11.2020) (in Russian).
[12] Krasnov A.E., Nadezhdin E.N., Nikolsky D.N., Kalachev A.A. A neural network approach to the problem of assessing the efficiency of an organization's functioning based on the aggregation of its performance indicators. Informatizaciya obrazovaniya i nauki, № 1 (33), 2017. S. 141–154. URL: https://informika.ru/pechatnye-izdaniya/zhurnal-informatizaciya-obrazovaniya-i-nauki/arhiv-vypuskov/2017/vypusk-n33/ (accessed: 01.11.2020) (in Russian).
[13] Krasnov A., Pivneva S. (2021) Hierarchical Quasi-Neural Network Data Aggregation to Build a University Research and Innovation Management System. In: Murgul V., Pukhkal V. (eds) International Scientific Conference Energy Management of Municipal Facilities and Sustainable Energy Technologies EMMFT 2019. EMMFT 2019. Advances in Intelligent Systems and Computing. V. 1259. Springer, Cham. P. 12–15. DOI: https://doi.org/10.1007/978-3-030-57453-6_2.
[14] Albert R., Barabasi A.-L. Statistical mechanics of complex networks. Rev. Mod. Phys. V. 74, Issue 1, 2002. P. 47–97. DOI: https://doi.org/10.1103/RevModPhys.74.47.
[15] Barabási A.-L. The network takeover. Nature Phys. V. 8, 2012. P. 14–16. DOI: https://doi.org/10.1038/nphys2188.
[16] Evin I.A. Introduction to complex network theory (in Russian). Kompyuternye issledovaniya I modelirovanie. V. 2, no. 2, 2010. P. 121–141. DOI: https://10.20537/2076-7633-2010-2-2-121-141 (in Russian).
[17] Mosolov A.S. Universal technology for designing systems of engineering and physical protection "AMULET" with a given level of efficiency. M.: NIYAU «MIFI», 2013. – 200 p. (in Russian).
[18] Mosolov A.S., Belyaeva E.A., Badikov A.V. Study of a universal method for designing systems for engineering and technical protection of objects. M.: NIYAU «MIFI», 2010. – 84 p. (in Russian).
[19] Belyaeva E.A., Kuzoyatov O.P., Mosolov A.S., Novikov Yu.V. A method for designing an integrated security system for an object. Patent RU 2219576 C2. Application RU 2002105932, 05.03.2002. Published 20.12.2003, bull. No. 35. IPC G06F 17/00 (in Russian).
[20] Saati T. Decision-making. Hierarchy analysis method. M.: Radio i svyaz', 1993. – 278 s. (in Russian).
[21] Akinin N.I., Gubina T.A., Mosolov A.S. Algorithm of the method for determining the priority scenario for the development of an emergency at the protected object (in Russian). Koks i himiya: zhurnal. M.: Metallurgizdat, 2019. S. 41–49 (in Russian).
[22] Gubina T.A., Mosolov A.S., Mosolov A.A. Safety assessment system for a hazardous production facility. Patent RU 2709155 C1. Application RU 2019107954, 02.04.2019. Published 16.12.2019, bull. No. 35. IPC G06Q 10/06 (in Russian).

Поступила в редакцию – 16 ноября 2020 г. Окончательный вариант – 12 февраля 2021 г.
Received – November 16, 2020. The final version – February 12, 2021.

Рукописи, предоставляемые в редакцию, должны соответствовать следующим требованиям:

– тема статьи должна быть актуальной, иметь научное или практическое значение и публиковаться авторами впервые;

– рукопись должна быть оформлена только в формате *.doc или *.docx, полоса А4, кегль 12, шрифт TimesNewRoman, интервал одинарный;

– в начале статьи идут сведения о статье **на русском языке**: Имя О. Фамилия авторов (по центру, строчными буквами, кегель 12); далее сведения об авторах – организация с почтовым адресом, адрес электронной почты и личный идентификатор ORCID (по центру, строчными буквами, курсив, кегель 11); затем название статьи (по центру, ПРОПИСНЫМИ буквами, кегель 12), в случае выполнения статьи в рамках НИР, гранда и пр. возможно оформление сноски на благодарность; благодарность (курсивом, кегель 11) - пишутся сведения об источнике финансирования; ключевые слова (не более шести, по ширине, курсив, кегель 11); аннотация (100 – 250 слов, по ширине, строчными буквами – см. **правила оформления аннотации**);

– далее повторяются все сведения о статье **на английском языке.**

– название статьи на английском оформляется по центру, строчными буквами, полужирно с подчеркиванием;

– в статью включают **Введение** и **Заключение**, а также вводятся **Разделы** с их нумерацией (прописные по центру, полужирно, кегль 12);

– затем идет текст статьи на русском или английском языке, кегль 12, интервал одинарный, рекомендуемый общий объем статьи не должен превышать 10 страниц, включая таблицы, иллюстрации; подписи под иллюстрациями на русском языке дублируются на английском языке;

– в конце статьи приводится СПИСОК ЛИТЕРАТУРЫ, в котором указан библиографический список источников литературы литературы (по ширине, строчные, кегль 10), оформленный в соответствии с действующими стандартами и указанием идентификатора DOI (как правило, не менее 15 наименований в научной статье и 50 в обзорной статье);

– после списка литературы идет REFERENCES, в котором указанные библиографические данные авторов и название статьи должны быть на английском языке, исходные данные русскоязычного издания и издательства должны быть представлены в транслитерации на латиницу.

Правила оформления аннотации

Аннотация является источником информации о содержании статьи и изложенных в ней результатах исследований и дает возможность установить основное содержание статьи, определить его релевантность и решить, следует ли обращаться к полному тексту статьи. Аннотация используется в информационных, в том числе автоматизированных, системах для поиска документов и информации (на английский язык переводятся: название, аннотация и ключевые слова, и по ним зарубежный читатель судит о содержании статьи).

Структура аннотации должна соответствовать структуре статьи и должна быть объемом не менее 100 слов, но не более 250 слов.

Аннотация включает следующие аспекты содержания статьи**:**

- предмет, цель статьи;
- метод или методологию проведения научной работы, описываемой в статье;
- результаты научной работы;
- область применения результатов;
- выводы.

Аннотация к статье должна быть информативной (не содержать общих слов) и оригинальной. Сведения, содержащиеся в заглавии статьи, не должны повторяться в тексте аннотации. Текст аннотации не должен содержать интерпретацию содержания статьи, критические замечания и точку зрения автора, а также информацию, которой нет в статье. Следует избегать лишних вводных фраз (например, «автор статьи рассматривает...»).

Исторические справки, если они не составляют основное содержание статьи, описание ранее опубликованных работ и общеизвестные положения в аннотации не приводятся.

В тексте аннотации следует употреблять синтаксические конструкции, свойственные языку научных и технических документов, избегать сложных грамматических конструкций.

В тексте аннотации следует применять значимые (ключевые) слова из текста статьи.

Метод или методологию проведения работы целесообразно описывать в том случае, если они отличаются новизной или представляют интерес с точки зрения данной работы. В аннотации статьи, описывающей экспериментальные работы, указывают источники данных и характер их обработки.

Результаты работы описывают предельно точно и информативно. Приводятся основные теоретические и экспериментальные результаты, фактические данные, обнаруженные взаимосвязи

и закономерности. При этом отдается предпочтение новым результатам и данным долгосрочного значения, важным открытиям, выводам, которые опровергают существующие теории, а также данным, которые, по мнению автора, имеют практическое значение.

Выводы могут сопровождаться рекомендациями, оценками, предложениями, гипотезами, описанными в статье.

Правила оформления текстов для публикации

1. Статьи необходимо подавать в электронном виде (файл *.doc) с распечаткой (или файлом в формате *.pdf) – во избежание неточностей прочтения формул.
2. Рисунки, графики, фотографии и другие виды иллюстраций следует предоставлять не только включенными в текст, но и отдельными файлами в исходном формате (не интегрированными в документ Word). Подписи под иллюстрациями делать на русском и английском языках.
3. Сокращения и аббревиатуры, которых нет в списке сокращений, необходимо раскрывать (в скобках или в сноске).
4. Давая в тексте статьи ссылки на формулы, выражения или ограничения, пожалуйста, убедитесь в том, что соответствующие объекты в статье есть и пронумерованы.
5. Ссылки на литературу следует давать в тексте в квадратных скобках, в случае цитирования – с указанием страниц.
6. При оформлении списка литературы обязательно проверить наличие и корректность выходных данных работ и исключить повторные указания одной и той же работы под разными номерами.
7. В список литературы не рекомендуется помещать источники старше 5 лет (рекомендация ВАК), а также источники, которых нет научных электронных базах (российские - это Elibrary, Ciberleninka).
8. Не надо помещать в список литературы анонимные источники - законы, нормативные акты, инструкции и пр. Их, при необходимости, помещать в постраничной ссылке или прямо по тексту.
9. Нельзя ссылаться на справочно-поисковые системы типа «Консультант» вместо ссылок на оригиналы.
10. Недопустимо в научной статье ссылаться на учебники и учебные пособия (на учебники допустимо ссылаться только в обзорных статьях).
11. Иноязычные слова, термины и фамилии, написание которых допускает варианты, просьба писать в пределах одной статьи одинаково.

Условия опубликования статьи:

– статья должна быть выслана по электронной почте, загружена самостоятельно на сайте журнала или представлена в редакцию на электронном носителе;

– редакционная коллегия журнала следует этическим нормам, принятым в международном научном сообществе, опираясь на рекомендации Комитета по этике научных публикаций, не противоречащим нормам российского законодательства в областях регулирования деятельности средств массовой информации и авторского права;

– статьи, не соответствующие установленным требованиям представления и оформления, не рассматриваются и не публикуются;

– в одном номере журнала публикуется, как правило, только одна статья автора, в том числе с соавторами;

– авторы должны предоставлять только оригинальные работы, при использовании текстовой или графической информации, полученной из работ других лиц, необходимы ссылки на соответствующие публикации или письменное разрешение автора;

– решение о публикации рукописи принимается редакционной коллегией на основании результата двойного слепого рецензирования и экспертной оценки квалифицированными специалистами в области ИБ, срок рецензирования не превышает 30 дней;

– в случае приема рукописи к публикации автор должен оперативно давать ответы на вопросы редакции, связанные с замечаниями по статье;

– в случае отказа в публикации редакционная коллегия должна предоставить автору копию рецензии и обоснование отказа в публикации;

– подача статьи в более чем в один журнал одновременно расценивается как неэтичное поведение и является неприемлемой;

– статьи публикуются бесплатно.

Заранее спасибо,
редакционная коллегия

СПИСОК СОКРАЩЕНИЙ, ПРИНЯТЫХ В ЖУРНАЛЕ

АБИ – администратор безопасности информации
АнД – аналоговый документ
АРМ АБИ – автоматизированное рабочее место администратора безопасности информации
АС – автоматизированная система
БД – база данных
БИС – большая интегральная схема
БЧ – блокчейн
ИБ – информационная безопасность
ИКТ – информационно-коммуникационные технологии
ИП – информационные продукты
ИПС – изолированная программная среда
ИР – информационные ресурсы
КПО – комплекс программного обеспечения
КСЗ – комплекс средств защиты
КТЭ – компьютерно-техническая экспертиза
ЛВС – локальная вычислительная сеть
МЭ – межсетевой экран
НД – нормативный документ
НСД – несанкционированный доступ
ОИ – объект информатизации
ОКСО – Общероссийский классификатор специальностей по образованию
ОС – операционная система
ПАК – программно-аппаратный комплекс
ПО – программное обеспечение
ПРД – правила разграничения доступа
ПСКЗИ – персональное средство криптографической защиты информации
РД – руководящий документ
РКБ – резидентный компонент безопасности
РПВ – разрушающее программное воздействие
СБЧ – система блокчейн
СВТ – средство вычислительной техники
СЗИ – средство защиты информации
СЗИ НСД – средство защиты информации от несанкционированного доступа
СКЗИ – система криптографической защиты информации
СРД – система разграничения доступа
СУБД – система управления базами данных
ЭлД – электронный документ
ЭЦП – электронная цифровая подпись
ФГОС – федеральный государственный образовательный стандарт
ФУМО ИБ – федеральное учебно-методическое объединение по образованию в области информационной безопасности