ISSN 2225-5435

Вестник УрФО

БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ

№ 2(12) / 2014

Подписной индекс 73852 в каталоге «Почта России»

Журнал зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Свидетельство **ПИ № ФС77-44941** от 05.05.2011

Издатель: ООО «Южно-Уральский юридический вестник»

Адрес редакции: Россия, 454080, г. Челябинск, пр. Ленина, д. 76.

Тел./факс: (351) 267-90-65, 267-97-01.

Электронная версия журнала в Интернете: **www.info-secur.ru, e-mail: urvest@mail.ru**

В НОМЕРЕ

ENGINEERING AND TECHNICAL INFORMATION SECURITY

CRYPTOGRAPHIC INFORMATION SECURITY

PROGRAM AND HARDWARE INFORMATION SECURITY

LEGAL REGULATION OF INFORMATION SECURITY

THE PRACTICAL ASPECT

УКД 519.87 + 004.056

Булатов Д. К., Соколов А. Н.

ПРИМЕНЕНИЕ АЛГОРИТМА ВОЛНОВОЙ ТРАССИРОВКИ В ЗАДАЧАХ МОДЕЛИРОВАНИЯ ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Рассмотрен алгоритм волновой трассировки применительно к задачам, связанным с моделированием физической безопасности объекта как элемента инженерно-технической защиты информации. Описаны этапы работы алгоритма волновой трассировки и условия его применения в рассматриваемых задачах. Уточнен спектр решаемых задач. Проведен сравнительный анализ алгоритма с традиционно применяемыми графовыми алгоритмами и алгоритмами, основанными на поиске глобального минимума функционала. Проанализированы возможности развития и комплексного применения моделей информационной безопасности, построенных на основе алгоритма волновой трассировки.

Ключевые слова: *алгоритм волновой трассировки, графовый алгоритм, алгоритм поиска глобального минимума функционала, инженерно-техническая защита информации, информационная безопасность, физическая безопасность.*

Bulatov D. K., Sokolov A. N.

APPLYING THE ALGORITHM WAVE TRACE FOR MODELING TECHNICAL PROTECTION OF INFORMATION

The algorithm of the wave trace applied to the problems associated with modeling the physical security of the object as an element of technical protection of information. The stages of the algorithm wave tracing and conditions for its use in these problems. Clarified range of tasks. Carried out a comparative analysis of the algorithm with the traditionally used graph algorithms and algorithms based on finding the global minimum of the functional. The possibilities of development and comprehensive application of information security models that are based on the wave tracing algorithm.

Keywords: *wave tracing algorithm, graph algorithm, the algorithm search for the global minimum of the functional, technical information security, information security, physical security.*

Ввиду разнообразия и уникальности каждого объекта информатизации, информационной системы и, в общем случае, каждого информационного ресурса, проектирование системы защиты является сложным процессом, в котором преимущественно применяются экспертные знания, опыт специалистов при проектировании систем инженерно-технической защиты информации[1]. Поэтому моделирование процессов, объектов, информационных систем является важным аспектом обеспечения информационной безопасности. Однако необходимым условием обеспечения комплексной защиты информации является создание определенных критериев, позволяющих оценить защищенность и определить достаточность мер, предпринятых для защиты от угроз. Именно моделирование позволяет унифицировать систему защиты и установить критерии оценки (показатели) защищенности объекта. Непосредственный интерес представляют математические модели, позволяющие на основании выбранных критериев оценить систему защиты объекта на соответствие предъявляемым требованиям, – в частности, оценить физическую защищенность объекта[2] как элемент инженерно-технической защиты информации.

Основные задачи[3], которые ставятся при моделировании обеспечения физической безопасности объекта:

1) оценка эффективности систем безопасности;

2) оценка безопасности различных стратегий;

3) оптимизация систем безопасности, т. е. приведение в соответствие заданному критерию при минимальных расходах на их построение.

В задачах трассировки печатных плат и нахождении кратчайшего пути в двумерном лабиринте широко применяется алгоритм волновой трассировки[4] (волновой алгоритм, алгоритм Ли), основанный на поиске кратчайшего пути на планарном графе. Он принадлежит к алгоритмам, основанным на методах поиска в ширину. Применение его в задачах обеспечения информационной безопасности является новым.

Алгоритм волновой трассировки, как основа для моделирования физической защиты объекта, позволяет решать комплекс задач, связанных с локацией злоумышленника на объекте защиты. При этом множество реализуемых моделей предполагает рассмотрение физического передвижения злоумышленника по территории защищаемого объекта. В зависимости от реализации алгоритма возможна оценка:

1) нарушителя (внутреннего и внешнего);

2) стихийного бедствия (распространения пожара);

3) возможности размещения технических средств перехвата информации в границах периметра защищаемого объекта.

Классическое решение задачи основывается на алгоритмах нахождения кратчайшего пути в графах. Объект представляется совокупностью вершин, соответствующих элементам рубежей защиты, и ребер, характеризующих способность нарушителя переходить от одной вершины к другой с целью преступной акции. Ребрам (либо вершинам) присваивается определенный показатель, как, например, вероятность обнаружения на каждом рубеже, либо время задержки злоумышленника. Именно на таком графе решается задача нахождения кратчайшего пути. На основании значения пути оценивается надежность и эффективность системы защиты. Однако существенным недостатком такого метода является его избыточность при моделировании сложных объектов и учете всех возможных переходов злоумышленника от одного рубежа защиты к другому.

При моделировании физической защиты объекта маршрут злоумышленника (вне зависимости от его типа) обладает свойством последовательности: злоумышленник не может появиться «ниоткуда» на объекте защиты и исчезнуть в «никуда». Его маршрут непрерывен и в каждой точке характеризуется такими параметрами, как вероятность обнаружения и время задержки. Интегрированием этих параметров можно получить искомый показатель безопасности для системы с большей точностью, чем в графовом алгоритме. С другой стороны, рассматриваемый алгоритм является некоторым упрощением алгоритма, основанного на поиске глобального минимума функционала.

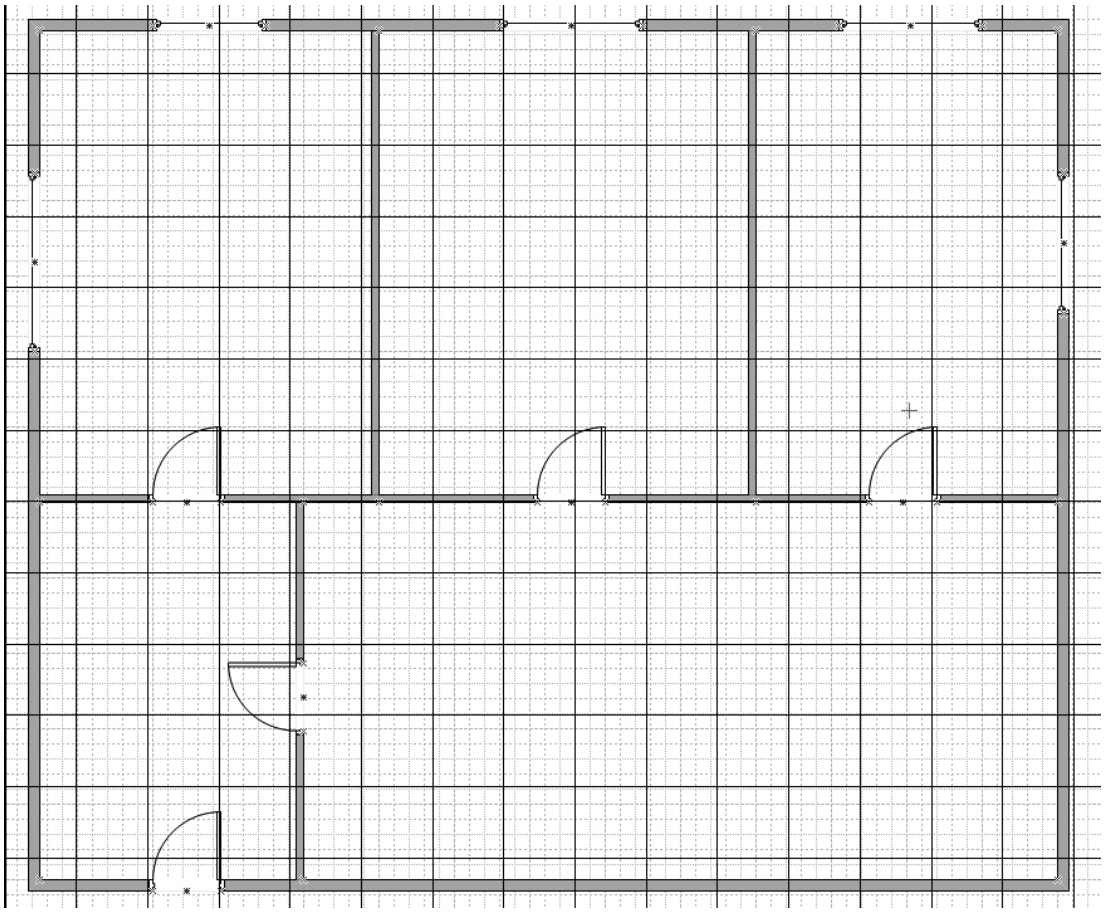

Рис. 1. План объекта с разбиением на ячейки

Алгоритм волновой трассировки реализуется в три этапа:

1) инициализация;
2) распространение волны;
3) восстановление пути.

На первом этапе объект, представленный в виде плана или схемы, разбивается на ячейки, размер которых должен обеспечивать различимость элементов инженерных конструкций и средств защиты (рис. 1).

С учетом разбиения создаются маски объекта:

1) маска физической доступности элементов объекта, которая характеризует физический маршрут злоумышленника, его возможность либо невозможность преодоления физических ограждений, а также характер преграждающих конструкций: дверей, окон, турникетов и т. д.;

2) маска системы безопасности, которая задает для каждой ячейки параметры вероятности фиксации либо обнаружения злоумышленника.

В общем случае применения алгоритма волновой трассировки достаточно двух масок, но модель может быть расширена путем добавления новых, например, маски огнеустойчивости среды, маски зон возможного снятия ПЭМИН, маски акустической разведки и т. д. На первом этапе также выбираются ячейки цели и исходные ячейки выдвижения злоумышленника.

Второй этап включает непосредственную реализацию волнового метода: на каждом шаге алгоритма рассчитывается новый фронт волны, то есть множество ячеек, в которые может переместиться злоумышленник из множества ячеек предыдущего шага (рис. 2). При этом происходит расчет параметров по маскам в зависимости от искомого параметра моделирования.

В ситуации, когда нас интересует исключительно параметр системы, как, например, показатель вероятности обнаружения на наиболее оптимальном маршруте, либо минимальная вероятность обнаружения, алгоритм может закончить свою работу.

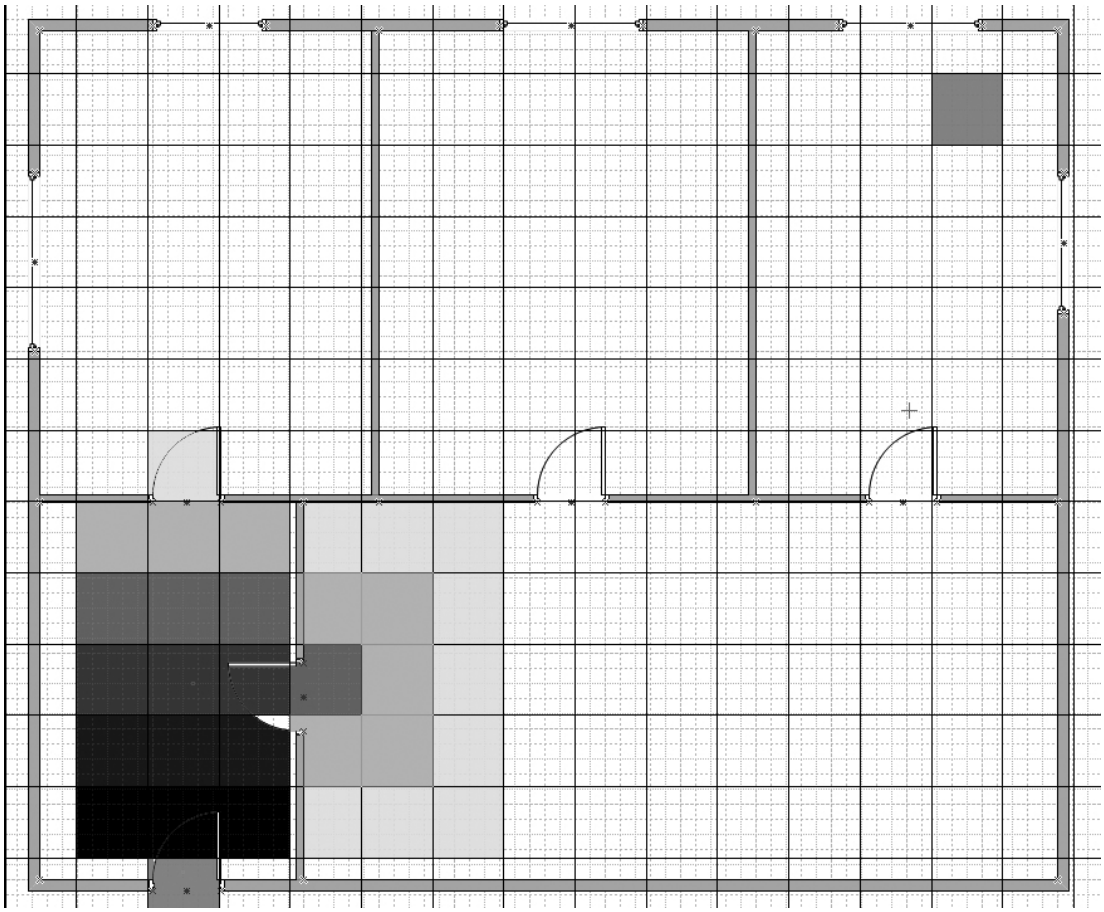

Рис. 2. Распространение фронта волны

Третий этап предполагает восстановление пути злоумышленника: методом обратного прохода от ячейки цели нарушителя восстанавливается маршрут, обусловленный заданными параметрами.

Алгоритм волновой трассировки используется в моделях, занимающих промежуточное положение между классическими графовыми моделями и моделями, основанными на поиске глобального минимума функционала, и обладает определенными преимуществами:

1) по сравнению с графовыми алгоритмами позволяет получить более точные результаты моделирования и использует более простую систему исходных данных;

2) по сравнению с алгоритмами, основанными на поиске глобального минимума функционала, более прост в реализации.

Рассмотренный алгоритм имеет высокий потенциал применения при моделировании различных аспектов обеспечения информационной безопасности.

Примечания

[1] Инженерно-техническая защита информации [текст]/А.А. Торокин. – М.: Гелиос АРВ, 2005. – 958 с.

[2] Проектирование и оценка систем физической защиты [текст]/ М.Гарсиа. – М.: Мир, 2003. – 386 с.

[3] Математические модели безопасности [текст]/ Вл. Вит. Башуров, Т. И. Филимоненкова. – Новосибирск: Наука, 2009 – 87 с.

[4] Графы в программировании: обработка, визуализация и применение [текст]/ В. Н. Касьянов, В. А. Евстигнеев – СПб.: БХВ-Петербург, 2003. – 1104 с.

References

[1] Engineering and Technical Information Security [text]/A.A. Torokin. – Moscow: Gelios ARV Publ., 2005. – 958 p. (In Russ.)

[2] Design and Assessment of the Systems of Physical Security [text]/ M.Garsia. – Moscow: Mir Publ., 2003. – 386 p. (In Russ.)

[3] Mathematical Models of Security [text]/ Vl.Vit. Bashurov, T.I. Filimonenkova. – Novosibirsk: Nauka Publ., 2009 – 87 p. (In Russ.)

[4] Graphs in Programming: Processing, Visualization, and Application [text]/ V.N. Kas'yanov, V.A. Evstigneev – St. Petersburg: BKhV-Peterburg Publ., 2003. – 1104 p.

Булатов Данил Кабирович, студент кафедры безопасности информационных систем ФГБОУ ВПО «Южно-Уральский государственный университет» (национальный исследовательский университет). E-mail: DANILDAZ@mail.ru

Соколов Александр Николаевич, кандидат технических наук, доцент, зав. кафедрой безопасности информационных систем ФГБОУ ВПО «Южно-Уральский государственный университет» (национальный исследовательский университет). E-mail: ANSokolov@inbox.ru

Danil Kabirovich Bulatov, student of the Department of Information System Security of the Federal State Budgetary Educational Institution of Higher Professional Education 'South Ural State University'. E-mail: DANILDAZ@mail.ru

Sokolov Aleksandr Nikolaevich, candidate if engineering sciences, associate professor, head of Information Systems Security Department, South Ural State University (national research university). E-mail: ANSokolov@inbox.ru

УДК 342.843:003.26:004.056

Яркова О. Н., Осипова А. А.

ЗАЩИЩЕННАЯ СИСТЕМА ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ НА ОСНОВЕ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ

В статье рассматривается актуальная проблема внедрения дистанционного голосования в существующий избирательный процесс. Авторами разработана система электронного голосования, защита которой построена на основе криптографических алгоритмов. Предложенная система подходит для проведения референдумов, а также выборов с большим количеством кандидатов.

Ключевые слова: *система электронного голосования; интернет-голосование.*

Yarkova O. N., Osipova A. A.

SECURE ELECTRONIC VOTING SYSTEM BASED CRYPTOGRAPHIC ALGORITHMS

The article deals with the actual problem of implementation distance voting in the existing electoral process. The authors have developed an electronic voting system with protection which based on cryptographic algorithms. The proposed system is suitable for holding elections with two or more candidates.

Keywords: *electronic voting system; Internet voting.*

Информатизация коснулась всех сфер общественной жизни и стала визитной карточкой XXI века. Переход процессов производства в автоматизированный режим, создание электронных ресурсов, развитие средств вычислительной техники свидетельствуют о научно-техническом прогрессе и позволяют называть современное общество информационным.

В развитых странах стали осуществляться целевые программы по автоматизации работы государственных служб. Одной из наиболее актуальных проблем является организация выборов через глобальную сеть Интернет. В США, Великобритании, Ирландии, Швейцарии и Эстонии для избрания членов центральных и местных органов власти используются системы электронного голосования (СЭГ), позволяющие избирателям дистанционно сделать свой выбор.

В России существует государственная автоматизированная система «Выборы», в рам-

ках которой реализуется процесс электронного голосования с помощью сенсорных устройств. Но на данный момент эти технологии используются только для проведения муниципальных выборов некоторых регионов страны; в большинстве случаев применяется система бумажно-электронного голосования. Развитие системы интернет-голосования только начинает набирать обороты.

Преимущества проведения выборов через сеть общего пользования очевидны. Среди них можно выделить:

• отсутствие необходимости появления на избирательном участке;

• осуществление подсчета голосов в более короткие сроки;

• увеличение явки на выборы «молодого» электората, пользующегося мобильными устройствами.

Наряду с достоинствами СЭГ возникают трудности ее внедрения. Так, для внедрения удаленного электронного голосования в России необходимо[1]:

• внедрение электронных удостоверений личности и соответствующей инфраструктуры открытых ключей;

• разработка надежного протокола голосования на основе криптографических алгоритмов;

• разработка ПО и аппаратуры;

• тестирование СЭГ на различном уровне (муниципальный, региональный, федеральный).

По различным экспертным оценкам внедрение системы интернет-голосования в Российской Федерации возможно через 8–10 лет.

Основная цель при организации избирательного процесса – гарантия получения достоверного результата. Поэтому на всех этапах проведения выборов необходимо обеспечить защиту сведений от модификации и уничтожения.

Отличием СЭГ от системы бумажно-электронного голосования является наличие канала передачи данных (КПД) между избирателем и счетной комиссией. При бумажном голосовании нарушению целостности информации препятствуют наблюдатели и система видеоконтроля на избирательном участке. Проведение дистанционного голосования должно сопровождаться иными мерами безопасности, направленными на защиту КПД. Наиболее эффективным методом защиты информации при передаче по каналу связи является шифрование.

Целью создания СЭГ является повышение уровня защищенности информации, циркулирующей при организации и проведении дистанционных выборов.

Для достижения поставленной цели в ходе работы решены следующие задачи:

• определение общих требований к СЭГ;

• определение этапов избирательного процесса и разработка схемы работы СЭГ;

• проведение анализа СЭГ, защита которой реализована на основе криптографиче-

Рис. 1. Упрощенная схема системы электронного голосования

Рис. 2. – Алгоритм работы системы электронного голосования

ских алгоритмов, предлагаемых источником[2], выделение достоинств и недостатков;

• предложение варианта модификации защищенной СЭГ для устранения выявленных недостатков.

В различных источниках можно найти перечни требований к интернет-выборам, отличающиеся формулировкой, но схожие по смыслу. Проанализировав сведения из[2-4], выделим основные свойства, которыми должна обладать система электронного голосования (СЭГ):

1) Контроль над избирателями (голосовать имеют право только уполномоченные избиратели; один человек имеет лишь один голос);

2) анонимность, тайна голосования (нельзя узнать выбор конкретного избирателя);

3) индивидуальный контроль (каждый избиратель может убедиться, что его голос учтен);

4) универсальный контроль (каждый из участников способен проверить, что результат подсчитан правильно, что не были вброшены лишние бюллетени);

5) устойчивость (некорректные действия избирателей или злоумышленные действия организаторов не должны сорвать выборы);

6) неподтверждаемость (после выборов нельзя доказать, что избиратель проголосовал определенным образом).

Руководствуясь представленными требованиями, были разработаны упрощенная схема работы СЭГ (рис. 1), а также подробный алгоритм функционирования (рис. 2). Участниками выборов являются кандидаты, голосующие и счетные комиссии, сведения о ко-

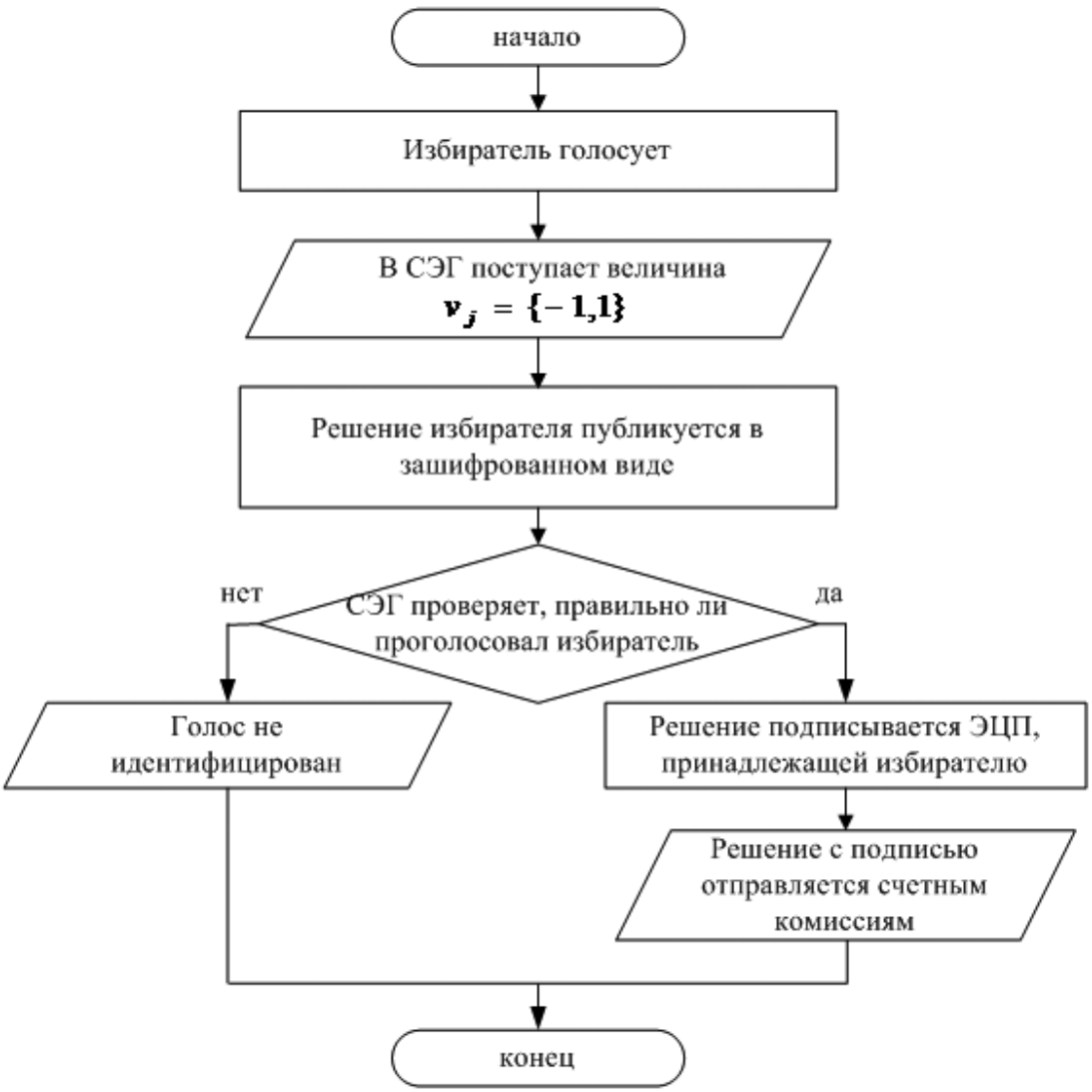

Рис. 3. Алгоритм заполнения бюллетеня в оригинальном варианте СЭГ

торых хранятся в базе данных с подсистемой обработки данных. Избирательный процесс в СЭГ включает в себя четыре этапа: заполнение электронного бюллетеня избирателем; передача бюллетеня счетным комиссиям; проверка достоверности и целостности полученной информации; определение результатов голосования.

Система электронного голосования, предложенная авторами источника[2], работает согласно представленным схемам. На всех этапах избирательного процесса для защиты канала передачи данных и циркулирующей информации применяются криптографические алгоритмы (электронная цифровая подпись (ЭЦП), протоколы идентификации и аутентификации и др.). Подробно они описаны в литературе[2,5].

Достоинством описанной СЭГ является соответствие всем вышеперечисленным требованиям. Но имеется недостаток, препятствующий внедрению данной системы: она применима только на референдумах, т. е. избирательных процессах, где голосующему предлагается выбрать одного кандидата из двух.

Предложим модификацию рассмотренной системы голосования для расширения круга кандидатов. Для этого определим исходные данные и обратимся к первому этапу избирательного процесса.

Пусть в голосовании участвуют m лиц с правом голоса, n счетных комиссий и k кандидатов ($k = 2$). Процедура заполнения бюллетеня избирателем в оригинальном варианте СЭГ представлена на рис. 3.

Как видно из схемы алгоритма заполнения бюллетеня (рис. 3), в СЭГ поступает величина $v = \{-1,1\}$, где $\{-1,1\}$ – множество кандидатов, включающее два элемента.

Увеличим количество кандидатов k ($k \geq 2$). На этапе голосования избирателя с $ID = j, j = \overline{1,m}$ предлагается отправлять в СЭГ вектор (1). Назовем вектор V_j бюллетенем j-ого избирателя:

$$V_j = (v_1, v_2, ..., v_{k+1}) \quad (1)$$

где $v_1 \in \{0,1\}$ – отметка о голосовании избирателя: «0» – не голосовал, «1» – голосовал;

Таблица 1. Бюллетени избирателей в незашифрованном виде и подведение итогов голосования

Номер избирателя	Отметка о факте голосования	Выбор избирателя относительно конкретного кандидата				
		k=1	k=2	k=3	k=4	k=5
1	1	-1	1	-1	-1	-1
2	1	1	-1	-1	-1	-1
3	1	-1	-1	1	-1	-1
4	1	1	-1	-1	-1	-1
5	1	-1	-1	-1	-1	1
6	0	-	-	-	-	-
7	1	1	-1	-1	-1	-1
8	1	1	-1	-1	-1	-1
9	1	1	-1	-1	-1	-1
10	1	-1	1	-1	-1	-1
11	0	-	-	-	-	-
12	1	-1	-1	1	-1	-1
13	1	-1	-1	-1	-1	1
14	1	1	-1	-1	-1	-1
15	1	-1	-1	-1	1	-1
Сумма голосов	13	6	2	2	1	2
Итоги выборов (%)		46,14	15,39	15,39	7,69	15,39

$v_2,...,v_{k+1} \in \{-1,1\}$ – выбор избирателя относительно конкретного кандидата: «-1» – против, «1» – за;

k – количество кандидатов.

Подсчет голосов за кандидата k будет производиться по формуле (2)

$$U_k = \frac{\sum_{j=1}^{m} v_{jk} + \sum_{j=1}^{m} v_{j1}}{2}, \quad (2)$$

где U_k – сумма голосов за кандидата k;

$j = \overline{1,m}$ - порядковый номер избирателя;

$\sum_{j=1}^{m} v_{j1}$ - общее количество проголосовавших.

Несложно подсчитать процент голосов за каждого кандидата:

$$U_{k\%} = \frac{\sum_{j=1}^{m} v_{j1}}{U_k} * 100\%. \quad (3)$$

Проверим работу предложенного алгоритма. Пусть количество избирателей $m = 15$, количество кандидатов $k = 5$. Результат представлен в табл. 1.

Следует отметить, что бюллетени представлены в таблице в открытом виде для наглядности; в процессе работы СЭГ они передаются в виде затемненного обязательства[5].

Как видно из табл. 1, подсчет результатов при обработке незашифрованных бюллетеней корректен. Проблема заключается во внедрении предложенных изменений в СЭГ. Необходима проверка соответствия модифицированной системы требованиям, представленным выше. Особое внимание следует обратить на устойчивость СЭГ (п. 5 требований). Остальные условия будут выполнены, если каждая компонента вектора (1) будет шифроваться своим уникальным ключом в соответствии с алгоритмом, представленным на рис. 3.

Таким образом, в предложенной системе дистанционного голосования, защищенной с помощью криптографических алгоритмов, можно выделить следующие характеристики:

• регистрация пользователей и формирование ЭЦП обеспечивают участие в выборах уполномоченных лиц;

• избиратель не может проголосовать более одного раза, и его голос никто не может дублировать;

• отправка бюллетеня в виде затемненного обязательства гарантирует верифицируемость (позволяет проверить, что данные получены от уполномоченного избирателя, скрывая при этом его личность);

• протокол идентификации совместно с затемненным обязательством обеспечивают соблюдение тайны голосования;

• система обеспечивает корректный подсчет результата.

Реализация аналогичной системы на языках веб-программирования может стать основой защищенного интернет-ресурса для голосования.

Примечания

[1] Гребнев, С. В. Электронное голосование и криптография: проблемы, решения и перспективы. М.: 2011. 17 с.

[2] Смарт, Н. Криптография. М.: Техносфера. 2005. 528 с.

[3] Лифшиц, Ю. Электронные выборы. СПб.: 2005. 9 с.

[4] Алехова Е. Ю. Система тайного электронного голосования на базе локальной сети // Электронное научно-техническое издание «Наука и образование». 2004. URL: http://technomag.edu.ru/doc/44988.html/ (дата обращения: 22.04.2014).

[5] См.: Осипова, А. А. Яркова, О. Н. Модель интерактивной системы электронного голосования // Естественные и математические науки в современном мире. № 11 (11). сборник статей по материалам XII международной научно-практической конференции. Новосибирск: Изд. «СибАК». 2013. 226 с.

References

[1] Grebnev, S.V. Elektronnoe golosovanie i kriptografiya: problemy, resheniya i perspektivy [Electronic Voting and Cryptography: Problems, Solutions, and Perspectives]. Moscow: 2011. 17 p.

[2] Smart, N. Kriptografiya [Cryptography]. Moscow: Tekhnosfera Publ.. 2005. 528 p.

[3] Lifshits, Yu. Elektronnye vybory [Electronic Elections]. St. Petersburg: 2005. 9 p.

[4] Alekhova E.Yu. Sistema tainogo elektronnogo golosovaniya na baze lokal'noi seti [System of Secret Electronic Voting on the Basis of Local Network]// Electronic scientific and technical publication «Science and Education». 2004. URL: http://technomag.edu.ru/doc/44988.html/ (Date of Access: 22.04.2014).

[5] Sm. Osipova, A.A. Yarkova, O.N. Model' interaktivnoi sistemy elektronnogo golosovaniya [Model of Interactive System of Electronic Voting]// Estestvennye i matematicheskie nauki v sovremennom mire. No. 11 (11) sbornik statei po materialam XII mezhdunarodnoi nauchno-prakticheskoi konferentsii. Novosibirsk: «SibAK» Publ., 2013. 226 p.

Яркова Ольга Николаевна, кандидат экономических наук, доцент кафедры математических методов и моделей в экономике Оренбургского государственного университета. E-mail: yarkova_on@mail.ru

Осипова Александра Александровна, студент кафедры вычислительной техники и защиты информации Оренбургского государственного университета. E-mail: sandrenok92@mail.ru

Olga Nikolaevna Yarkova, Cand. Sc. Economics, Associate Professor, Associate Professor of the Department of mathematical Methods and Models in Economics of Orenburg State University. E-mail: yarkova_on@mail.ru

Aleksandra Aleksandrovna Osipova, Student of the Department of Computational Machinery and Information Security of Orenburg State University. E-mail: sandrenok92@mail.ru

УДК 578.087.1+004.383.8+612.087.1

Иванов А. И., Сомкин С. А., Андреев Д. Ю., Малыгина Е. А.

О МНОГООБРАЗИИ МЕТРИК, ПОЗВОЛЯЮЩИХ НАБЛЮДАТЬ РЕАЛЬНЫЕ СТАТИСТИКИ РАСПРЕДЕЛЕНИЯ БИОМЕТРИЧЕСКИХ ДАННЫХ «НЕЧЕТКИХ ЭКСТРАКТОРОВ» ПРИ ИХ ЗАЩИТЕ НАЛОЖЕНИЕМ ГАММЫ

Проведен анализ возможностей «нечетких экстракторов» и нейросетевых преобразователей биометрия-код. Показано, что для «нечетких экстракторов» переход в пространство метрики расстояний Хэмминга и/или использование метрики среднего значения показателей стабильности разрядов биокода приводит к автоматическому снятию защиты от наблюдения статистик распределения биоданных. Использование свойств нейросетевых преобразователей биометрия-код позволяет решить данные проблемы.

Ключевые слова: *метрика расстояний Хэмминга, метрика среднего показателя стабильности состояний разрядов биокода, биометрические данные, преобразователь биометрия-код.*

Ivanov A., Somkin S., Andreev D., Malygina E.

DIVERSITY METRICS TO WATCH ACTUAL BIOMETRIC DATA DISTRIBUTION STATISTICS «FUZZY EXTRACTORS» IN THEIR PROTECTION OF A RANGE

The analysis of the «fuzzy extractors» and converters biometrics-neural network code. It is shown, that for «fuzzy extractors» transition to the Hamming distance metrics and/or use the metric average indicators stability level bio-code will automatically remove the protection from bio-data distribution statistics. Use the properties of neural network converters biometrics-code allows you to solve these problems.

Keywords: *Hamming distance metric, metric, the average State-level bio-security, biometrics, converters biometrics-neural network code.*

1. Классификация преобразователей биометрия-код

Все преобразователи биометрии в код делятся на «нечеткие экстракторы» и нейросетевые преобразователи биометрия-код. Отличие между ними только в положении квантователя непрерывных биометрических данных. В «нечетких экстракторах» квантователь преобразует в код «сырые» биометрические данные, а далее эти данные исправляются за счет избыточности самокорректирующегося кода.

В нейросетевых преобразователях «сырые» биометрические данные первоначально обогащаются сумматорами нейронов, а далее уже обогащенные сигналы на выходах сумматоров квантуются выходным нелинейным элементом. Структурные схемы, отражающие положение квантователей в преобразователях биометрия-код, отображены на рис. 1.

В «нечетких экстракторах» может быть использован любой классический код, способный обнаруживать и исправлять ошибки. Обычно используются коды БЧХ (Боуза – Чоухуры – Хоквингема) с примерно 10 кратной избыточностью, способные править до 15% ошибок. То есть при 512 контролируемых биометрических параметров длина выходного кода «нечеткого экстрактора» составит 51 бит.

Нейронные сети осуществляют обогащение данных в непрерывной форме, и обычно для корректировки всех входных ошибок оказывается достаточно двукратной избыточности, то есть 512 входных биопараметров нейронная сеть преобразует в 256 бит выходного кода практически без ошибок.

С точки получения биометрических свойств нейросетевые преобразователи биометрия-код всегда лучше «нечетких экстракторов». Этот тезис никто не оспаривает. Это легко продемонстрировать на примере плохих биометрических данных, дающих ошибки в 50% и более разрядах биокода, скорректировать больше 50% ошибок классические самокорректирующиеся коды не способны, нейронные сети с этой проблемой справляются, если избыточность их становится трехкратной (входов в три раза больше, чем выходов).

2. Нечеткие экстракторы

Основным преимуществом «нечетких экстракторов» англоязычная криптографическая общественность считала их относитель-

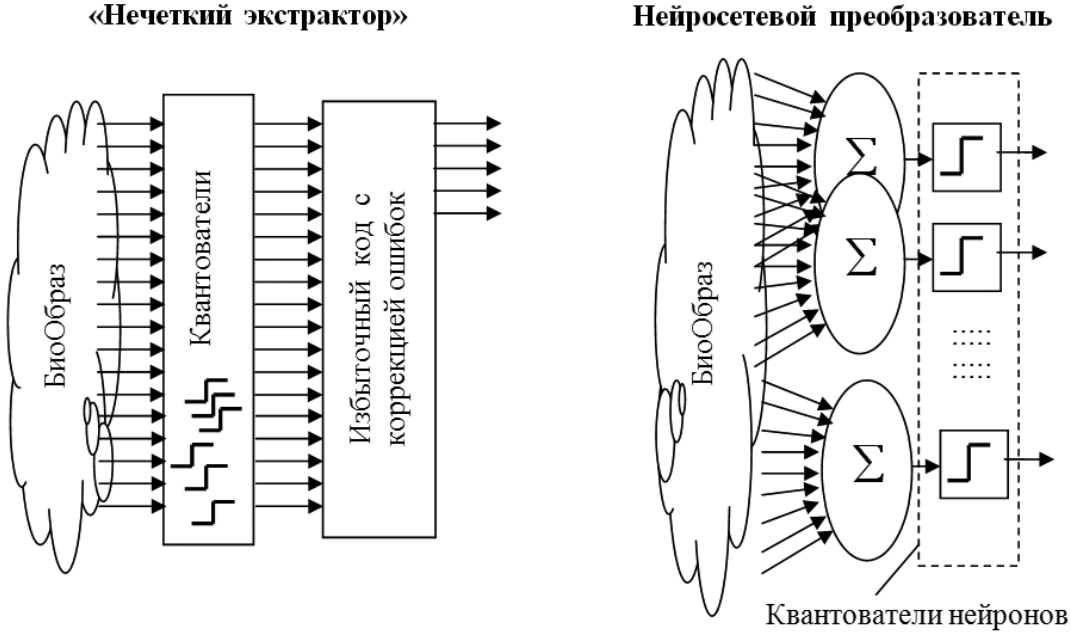

Рис. 1. «Нечеткие экстракторы» и нейросетевые преобразователи отличаются положением нелинейных элементов, квантующих непрерывные данные в код с конечным числом состояний

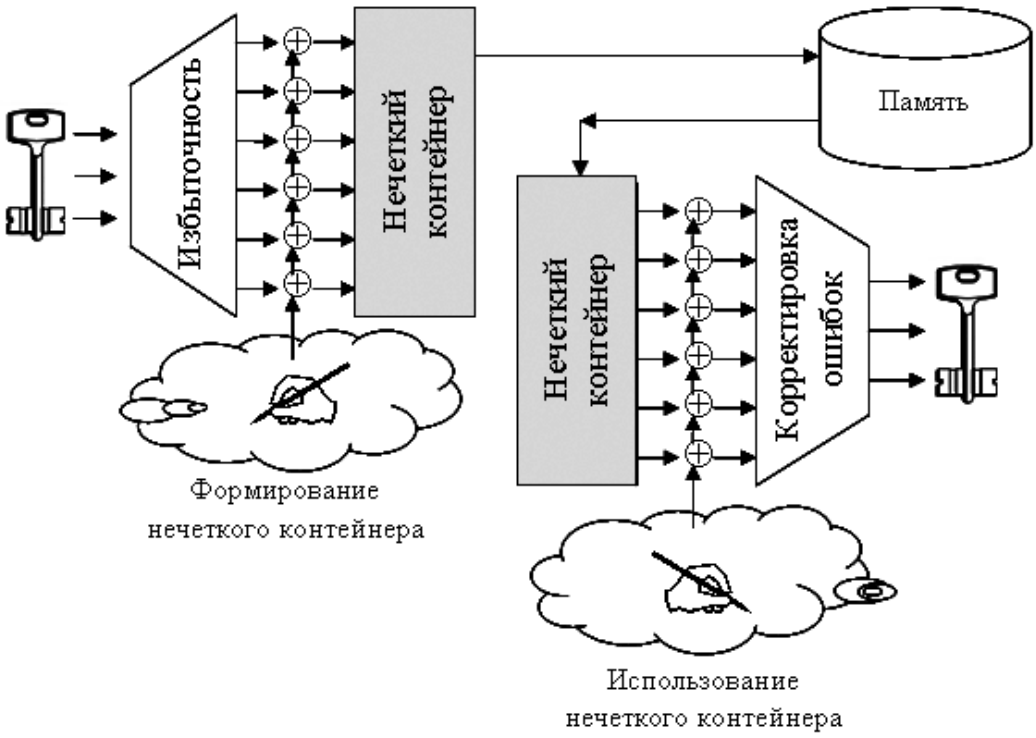

Рис. 2. Формирование и использование нечетких контейнеров

но высокий уровень защищенности и простоту (прозрачность) используемой защиты. Принцип защиты данных «нечетких экстракторов» иллюстрируется рис. 2.

Для защиты «сырых» биокодов используют секретный ключ. Этот ключ накрывают избыточным самокорректирующимся кодом (например, БЧХ), тем самым получают гамму в 10 раз длиннее кода секретного ключа. Далее накрывают «сырой» биокод гаммой, получая тем самым «нечеткий контейнер». «Нечеткий контейнер» хранят в памяти средств биометрической аутентификации. В США и странах НАТО такой способ считается относительно безопасным, и именно эта ветвь технологий за рубежом активно развивается. Конструкции «нечетких экстракторов» даны в ряде англоязычных публикаций[1-12], в работах[13-15] отражены усилия русскоязычных исследователей этого технологического направления.

В процессе аутентификации «нечеткий контейнер» извлекают из памяти и складывают его данные по модулю два с введенным и оцифрованным биометрическим образом. При этом восстанавливается избыточный самокорректирующийся код криптографического ключа, содержащий ошибки, унаследованные от двух биокодов (биокоде формирования нечеткого контейнера и биокоде аутентификации). Если таких ошибок меньше исправляющей способности самокорректирующегося кода, то они правятся.

3. Уязвимость защиты «нечетких контейнеров» в пространстве метрик расстояний Хэмминга

Если бы гаммой был защищен неизвестный текст, то такая защита сегодня считается надежной. Распространять этот тезис о безопасности на защиту «сырых» биокодов нельзя. Это иной объект защиты. Атакующий может подать на вход преобразователя 1000 образов «Чужой» и получить выборку из 1000 «сырых» биокодов «Чужой», накрытых одинаковой гаммой - "$\overline{g}$".

Если мы из пространства обычных кодов перейдем в пространство расстояний Хэмминга между кодами, то при вычислениях мы фактически снимаем одну и ту же гамму:

$$h("\overline{x}", "\overline{c}") = \sum_{i=1}^{512} "x_i" \oplus "c_i" = \sum_{i=1}^{512} ("g_i" \oplus "x_i") \oplus ("g_i" \oplus "c_i"), \qquad (1)$$

где "g_i" – состояния «0» или «1» *i*-го разряда, маскирующей биокод гаммы;

"c_i" – состояния «0» или «1» *i*-го разряда биокода «Свой»;

"x_i" – состояния «0» или «1» *i*-го разряда биокода «Чужой»,

512 – длина сравниваемых кодов.

В метрике расстояний Хэмминга защищающая биокод гамма неизвестного ключа исчезла, то есть биокоды «нечетких экстракторов» оказываются без защиты от наблюдения статистик распределений расстояний Хэмминга. Анализируя статистики распределения расстояний Хэмминга, удается выявить то направление, куда следует двигаться при направленном подборе биометрических данных неизвестного биометрического образа «Свой». Задача направленного подбора распределений биометрических данных образа «Свой» имеет полиномиальную сложность как для «нечетких экстракторов», так и для «нейросетевых контейнеров».

4. Уязвимость защиты «нечетких контейнеров» в пространстве метрики показателей стабильности био-кодов

Следует отметить, что метрика расстояний Хэмминга не единственная метрика, в которой защищающая «нечеткие контейнеры» гамма снимается. Точно такой же эффект снятия защитной гаммы наблюдается в метрике показателей стабильности разрядов биокода.

Показатель стабильности *i*-го разряда определяется через вероятности появления в разряде состояний «1» или «0»:

$$\gamma_i = 2 \cdot \left|0.5 - P("1_i")\right| = 2 \cdot \left|0.5 - P("0_i")\right|. \quad (2)$$

В предельной ситуации $P(«0_i»)=P(«1_i»)=0.5$ показатель стабильности оказывается нулевым. Если же значение разряда не меняется $P(«0_i»)=1$ или $P(«1_i»)=1$, то показатель стабильности оказывается единичным. Примеры гистограмм распределения показателей стабильности образа «Свой» и образов «Чужой» приведены на рис. 3.

Из данных рис. 3 видно, что по мере увеличения расстояния Хэмминга образа «Чужой» от образа «Свой» стабильность разрядов биокодов падает. Такой показатель, как средняя стабильность всех разрядов биокода – $E(\gamma)$, может использоваться для определения направления движения в сторону образа «Свой». При таком направленном переборе следует стремиться увеличивать по-

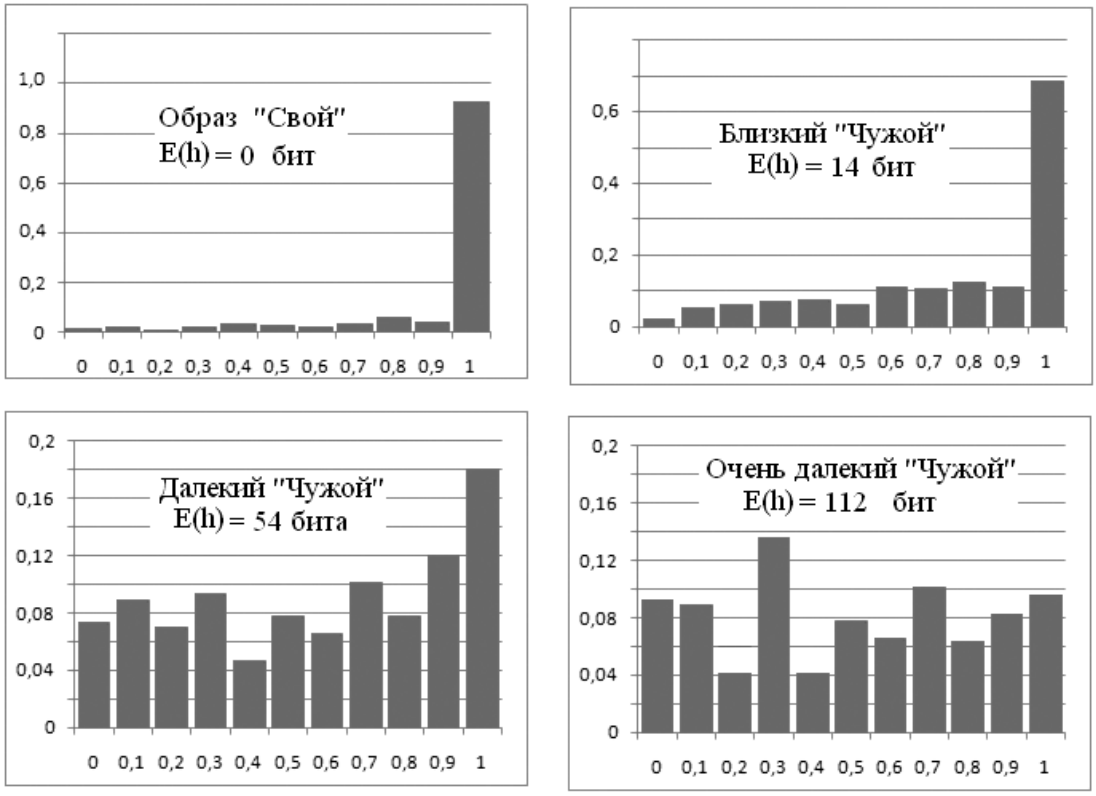

Рис. 3. Падение стабильности разрядов кодов «Чужой» по мере удаления образа «Чужой» от образа «Свой»

казатель стабильности разрядов при генетической селекции образов «Чужой», приближающихся к образу «Свой».

Очевидным является то, что гаммирование биокода не может повлиять на показатели стабильности разрядов кода. Гаммирование – это детерминированная операция, которая приводит только к смене наиболее вероятного состояния (состояние «0» может смениться на состояние «1»). Это никак не влияет на значение показателя стабильности (2), так как его можно вычислять и через вероятность $P(«0_i»)$, и через вероятность $P(«1_i»)$. Результат вычислений будет одинаковым.

5. Уязвимость защиты «нечетких контейнеров» в пространстве комбинированной метрики Хэмминга, взвешенной показателями стабильности разрядов био-кодов

Одним из важных теоретических моментов является то, что обе рассмотренные выше метрики могут быть объединены. Из них получается более сильная комбинированная метрика:

$$h("\overline{x}", "\overline{c}", \overline{\gamma}("x"), \overline{\gamma}("c")) = \sum_{i=1}^{512} ("x_i" \oplus "c_i") \cdot \gamma("x_i") \cdot \gamma("c_i") = \\ = \sum_{i=1}^{512} \left[("g_i" \oplus "x_i") \oplus ("g_i" \oplus "c_i")\right] \gamma("x_i") \cdot \gamma("c_i") \quad . \quad (3)$$

Эта метрика наследует лучшие свойства своих метрик-родителей, она одновременно учитывает и расхождения между разрядами сравниваемых биокодов «Чужой» и «Свой», и стабильность появления состояний в этих разрядах. Она учитывает то, что сравнивать между собой совершенно не стабильные разряды нет смысла. В этом случае расчет метрики Хэмминга полностью утрачивает физический смысл.

Практика применения взвешенной метрики Хэмминга показала, что она значительно увеличивает скорость направленного подбора биометрических данных. Комбинирование двух разных по содержанию метрик позволяет сократить адресное пространство направленного подбора от 20% до 40%.

6. Метрика среднего модуля коэффициентов корреляции и метрика энтропии биокодов

Еще одной метрикой, способной «видеть» реальные статистики данных, накрытых неизвестной гаммой, является метрика среднего модуля коэффициентов корреляции между случайно выбранными парами разрядов биокода. Очевидно, что для разрядов биокода «Свой» модуль коэффициентов корреляции оказывается близок к единице. Для кодов «Чужой» корреляционные связи всегда оказывается много меньше:

$$\left|r("c_i", "c_j")\right| \approx 1 \;\rangle\rangle\; \left|r("x_i", "x_j")\right|. \quad (4)$$

Это является следствием, того, что энтропия биокодов «Свой» оказывается практически нулевой, тогда как энтропия кодов «Чужой» оказывается крайне высокой:

$$H("\overline{c}") \approx 0 \langle\langle H("\overline{x}"). \quad (5)$$

Значение энтропии биокодов функционально связано с математическим ожиданием модулей коэффициентов парной корреляции (4), номограмма связи дана в монографии[16]. Легко показать, что наложение одной и той же гаммы на исследуемые биокоды не влияет на корреляционную и энтропийную метрики. В итоге получается, что мы можем наблюдать реальные статистики биокодов в 4 разных метриках (1), (2), (4), (5) и их комбинациях. Простое гаммирование данных «нечетких экстракторов» нельзя рассматривать как эффективную защиту биометрических данных. В пространствах описанных выше метрик легко строится атака направленного подбора данных биометрического образа «Свой».

7. Защита от атак направленного подбора данных образа «Свой»

Обычно атака направленного подбора данных неизвестного биометрического образа «Свой» ведется до момента подбора ключа аутентификации (рис. 2). При реализации атаки осуществляют подстановку образов «Чужой» из заранее созданной базы, осуществляя попутно их генетическую селекцию и скрещивание. При этом направление верного движения определяется тем вернее, чем длиннее оказываются наблюдаемые биокоды. Фактически атака направленного подбора выполня-

ется за счет возможности многомерной статистической обработки дынных в пространствах метрик (1), (2), (4), (5) и их комбинаций. Как было показано выше, для длинных биокодов нечетких экстракторов защита простым гаммированием не помогает. При этом исправить ситуацию для «нечетких экстракторов» нельзя, так как они нуждаются в длинных самокорректирующихся кодах, содержащих значительную избыточность. Пока биокод не исправлен, нельзя перемешивать его разряды, их последовательность должна полностью повторять заранее заданную структуру самокорректирующегося кода.

Совершенно иная ситуация возникает при использовании нейросетевых преобразователей биометрия-код. Их выходной биокод практически не содержит ошибок. То есть его можно защищать не только гаммированием, но и перемешиванием данных. Как только мы включаем в средство защиты механизмы перемешивания (механизмы размножения ошибок), наблюдать реальные статистики биометрических кодов в пространстве метрик (1), (2), (4), (5) уже не удается (структурные статистические связи разрушаются). Получается, что нейросетевые преобразователи биометрия-код вполне могут быть защищены от наблюдения реальных многомерных статистик в пространствах расстояний Хэмминга (1), средней стабильности разрядов (2), модулей корреляции (4), энтропии (5) и их комбинаций. Более того, ГОСТ Р 52633.3-201117 содержит прямые рекомендации того, как определить, в каком режиме находится «нейросетевой контейнер» (включен или нет защитный механизм размножения биометрических ошибок). То, что является непреодолимой угрозой для «нечетких экстракторов», достаточно просто отражается при использовании нейросетевых преобразователей биометрия-код[16].

Примечания

[1] Y. Dodis, L. Reyzin, A. Smith Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy, Data April 13, In EUROCRYPT, pages 523-540, 2004.

[2] F. Monrose, M. Reiter, Q. Li, S. Wetzel. Cryptographic key generation from voice. In Proc. IEEE Symp. on Security and Privacy, 2001.

[3] Arakala A., Jeffers J., Horadam K.J. Fuzzy Extractors for Minutiae-Based Fingerprint Authentication. // Advances in Biometrics (LNCS 4642), Springer, pp. 760-769, 2007.

[4] Balakirsky V.B., Ghazaryan A.R., Han Vinck A.J. Constructing Passwords from Biometrical Data. // Advances in Biometrics (LNCS 5558), Springer, pp. 889-898, 2009.

[5] Cauchie S., Brouard T., Cardot H. From features extraction to strong security in mobile environment: A new hybrid system. //On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops, Springer, pp. 489-498, 2006.

[6] Juels A., Wattenberg M. A Fuzzy Commitment Scheme // Proc. ACM Conf. Computer and Communications Security, 1999, p. 28–36.

[7] Juels A., Sudan M. A Fuzzy Vault Scheme // IEEE International Symposium on Information Theory, 2002.

[8] Kanade S., Petrovska-Delacretaz D., Dorizzi B. Multi-Biometrics Based Cryptographic Key Regeneration Scheme. //Proceedings of the 3rd IEEE international conference on Biometrics: Theory, applications and systems, p. 333-339, 2009.

[9] Lee Y.J., Bae K., Lee S.J., Park K.R., Kim J. Biometric Key Binding: Fuzzy Vault Based on Iris Images. // Proceedings of 2nd International Conference on Biometrics, p. 800–808, Seoul, South Korea, August 2007.

[10] Nandakumar K., Jain A.K., Pankanti S. Fingerprint-Based Fuzzy Vault: Implementation and Performance. //IEEE Transactions on Information Forensics and Security 2(4), pp. 744–757, 2007.

[11] Ramírez-Ruiz J., Pfeiffer C., Nolazco-Flores J. Cryptographic Keys Generation Using FingerCodes.// Advances in Artificial Intelligence - IBERAMIA-SBIA 2006 (LNCS 4140), p. 178-187, 2006.

[12] Yang S., Verbauwhede I. Automatic Secure Fingerprint Verification System Based on Fuzzy Vault Scheme // Proc. IEEE ICASSP 2005, p.609-612.

[13] Чморра А. Л. Маскировка ключа с помощью биометрии // Проблемы передачи информации. 2011. № 2(47). С. 128–143.

[14] Чморра А. Л., Уривский А. В. «Биометрическая система аутентификации», описание к патенту № RU2316120, 27.01.2008. Бюл. № 3.

[15] Ушмаев О. В., Кузнецов В. В. Алгоритмы защищенной верификации на основе бинарного представления топологии отпечатка пальцев // Информатика и ее применения. 2012. № 6(1). С. 132–140.

[16] Язов Ю. К. и др. Нейросетевая защита персональных биометрических данных. М.: Радиотехника. 2012. –160 с.

[17] ГОСТ Р 52633.3-2011 «Защита информации. Техника защиты информации. Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора». М.: Стандартинформ, 2012. – 16 с.

References

[1] Y. Dodis, L. Reyzin, A. Smith Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy, Data April 13, In EUROCRYPT, pages 523-540, 2004.

[2] F. Monrose, M. Reiter, Q. Li, S. Wetzel. Cryptographic key generation from voice. In Proc. IEEE Symp. on Security and Privacy, 2001.

[3] Arakala A., Jeffers J., Horadam K.J. Fuzzy Extractors for Minutiae-Based Fingerprint Authentication. // Advances in Biometrics (LNCS 4642), Springer, pp. 760-769, 2007.

[4] Balakirsky V.B., Ghazaryan A.R., Han Vinck A.J. Constructing Passwords from Biometrical Data. // Advances in Biometrics (LNCS 5558), Springer, pp. 889-898, 2009.

[5] Cauchie S., Brouard T., Cardot H. From features extraction to strong security in mobile environment: A new hybrid system. //On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops, Springer, pp. 489-498, 2006.

[6] Juels A., Wattenberg M. A Fuzzy Commitment Scheme // Proc. ACM Conf. Computer and Communications Security, 1999, p. 28–36.

[7] Juels A., Sudan M. A Fuzzy Vault Scheme // IEEE International Symposium on Information Theory, 2002.

[8] Kanade S., Petrovska-Delacretaz D., Dorizzi B. Multi-Biometrics Based Cryptographic Key Regeneration Scheme. //Proceedings of the 3rd IEEE international conference on Biometrics: Theory, applications and systems, p. 333-339, 2009.

[9] Lee Y.J., Bae K., Lee S.J., Park K.R., Kim J. Biometric Key Binding: Fuzzy Vault Based on Iris Images. // Proceedings of 2nd International Conference on Biometrics, p. 800–808, Seoul, South Korea, August 2007.

[10] Nandakumar K., Jain A.K., Pankanti S. Fingerprint-Based Fuzzy Vault: Implementation and Performance. //IEEE Transactions on Information Forensics and Security 2(4), pp. 744–757, 2007.

[11] Ramírez-Ruiz J., Pfeiffer C., Nolazco-Flores J. Cryptographic Keys Generation Using FingerCodes.// Advances in Artificial Intelligence - IBERAMIA-SBIA 2006 (LNCS 4140), p. 178-187, 2006.

[12] Yang S., Verbauwhede I. Automatic Secure Fingerprint Verification System Based on Fuzzy Vault Scheme // Proc. IEEE ICASSP 2005, p.609-612.

[13] Chmorra A.L. Maskirovka klyucha s pomoshch'yu biometrii [Concealement of the Key with the Help of Biometrics] // Problemy peredachi informatsii. 2011 No. 2(47). p. 128-143.

[14] Chmorra A.L., Urivskii A.V. «Biometrical System of Authentication», description to the patent №No. RU2316120, 27.01.2008. No. 3. (In Russ.)

[15] Ushmaev O.V., Kuznetsov V.V. Algoritmy zashchishchennoi verifikatsii na osnove binarnogo predstavleniya topologii otpechatka pal'tsev [Algorithms of Secure Verification on the Basis of Binary Representation of the Topology of Fingerprints] //Informatika i ee primeneniya. 2012. No. 6(1). p. 132-140.

[16] Yazov Yu.K. and others. Neirosetevaya zashchita personal'nykh biometricheskikh dannykh [Neural Network Security of Personal Biometrical Data]. Moscow: Radiotekhnika Publ.. 2012. – 160 p.

[17] All-Union State Standard R 52633.3-2011 «Information Security. Technology of Information Security. Testing of Survivability of Means of High-Reliable Biometrical Security to Brute-Force Attacks». Moscow: Standartinform Publ.. 2012. –16 p.

Иванов Александр Иванович, доктор технических наук, доцент, начальник лаборатории биометрических и нейросетевых технологий ОАО «Пензенский научно-исследовательский электротехнический институт». E-mail: ivan@pniei.penza.ru.

Сомкин Сергей Александрович, зам. начальника научно-исследовательского отдела ОАО «Пензенский научно-исследовательский электротехнический институт». E-mail: somkin@pniei.penza.ru.

Андреев Дмитрий Юрьевич, научный сотрудник лаборатории биометрических и нейросетевых технологий ОАО «Пензенский научно-исследовательский электротехнический институт». E-mail: mail.stray@gmail.com.

Малыгина Елена Александровна, аспирант кафедры «Информационная безопасность систем и технологий» ФБГОУ ВПО «Пензенский государственный университет». E-mail: mal890@yandex.ru.

Ivanov Alexander, doctor of technical sciences, Associate Professor, head of the laboratory of biometric and neural network technology «Penza research Electrotechnical Institute» E-mail: ivan@pniei.penza.ru

Somkin Sergei, Deputy Head of the Research Department, «Penza research Electrotechnical Institute». E-mail: somkin@pniei.penza.ru.

Andreev Dmitry, a researcher at the laboratory of biometric and neural network technology «Penza research Electrotechnical Institute». E-mail: mail.stray@gmail.com

Malygina Elena, graduate student «Security of information systems and technology» Penza State University. E-mail: mal890@yandex.ru

УДК 004.056+004.45.056+004.946

Тыщенко С. В., Соловьев Н. А.

СИСТЕМНЫЙ АНАЛИЗ ДОСТУПНОСТИ РЕСУРСОВ ИНФОРМАЦИОННЫХ СИСТЕМ В ГЕТЕРОГЕННОЙ ВИРТУАЛЬНОЙ СРЕДЕ

В статье рассмотрены особенности виртуализации физических серверов и введено понятие гетерогенной виртуальной среды. На примере возрастания угрозы отказа в обслуживании информационных систем при их размещении в гетерогенной виртуальной среде рассмотрена проблема доступности ресурсов как одного из аспектов безопасности информационных систем. Проведен системный анализ, выявлен источник проблемы и намечены пути решения. Выполнено формальное описание задачи автоматизации проблемного участка и определены основные требования к программным системам.

Ключевые слова: *виртуализация, гетерогенная виртуальная среда, информационная безопасность, отказ в обслуживании.*

Tyschenko S. V., Soloviev N. A.

SYSTEM ANALYSIS OF INFORMATION SYSTEM RESOURCE AVAILABILITY IN THE HETEROGENEOUS VIRTUAL ENVIRONMENT

The paper deals with aspects of physical server virtualization and introduces notion of heterogeneous virtual environment. Case of increased denial of service threat for information system in heterogeneous virtual environment has been used to demonstrate the problem of resource availability as an aspect of information system security. System analysis of the problem has led to detection of the problem source, and development of solution approach. Formal description of the problem area automation has been provided and basic requirements to the software systems established.

Keywords: *virtualization, heterogeneous virtual environment, information security, denial of service.*

Описание проблемы

В связи с активным развитием технологий виртуализации все больше организаций стремятся использовать виртуальные платформы при построении своей IT-инфраструктуры. Наиболее часто переносятся в виртуальную среду физические сервера, входящие в состав корпоративных информационных систем. Это объясняется высокой эффективностью подобной виртуализации при достаточно низкой стоимости решения.

Основным инструментом виртуализации стандартных серверов являются гипервизоры – мониторы виртуальных машин. Программные продукты, включающие в себя гипервизор и средства управления, составляют платформу виртуализации от конкретного производителя. Примерами современных платформ виртуализации являются: VSphere от компании VMware; Hyper-V от Microsoft; CitrixXen от Citrix[1].

Каждая из представленных на рынке платформ виртуализации имеет свои особенности: архитектуру гипервизора; используемый тип виртуализации; перечень совместимого оборудования; перечень поддерживаемых операционных систем. Эти особенности могут послужить причиной для параллельной эксплуатации нескольких виртуальных платформ в рамках виртуальной среды одного предприятия. Такая виртуальная среда называется гетерогенной. Гетерогенная виртуальная среда может образоваться в результате объединения компаний, в которых были развернуты разные виртуальные платформы. Также гетерогенность возникает в результате развертывания дополнительной виртуальной платформы с целью получения новой функциональности виртуальной среды или снижения стоимости решений виртуализации[2].

По результатам исследований, проведенных в 2012 году аналитической компанией Gartner Inc, – только 5% организаций на момент проведения исследования использовали единственную виртуальную платформу. В 2009 году абсолютное большинство организаций использовали только одну VMware[3]. Это означает, что гетерогенные виртуальные среды на текущий момент стали фактическим стандартом серверной виртуализации.

Наряду с преимуществами, виртуальная среда дает целый комплекс проблем, связанных с обеспечением безопасности информационных систем. Виртуальная среда динамична, а существующие средства обеспечения информационной безопасности рассчитаны на статические системы. Автоматизация управления виртуальной средой развита недостаточно и требует существенного человеческого участия. Ошибки в управлении виртуальной средой приводят к нехватке вычислительных ресурсов на физических узлах и могут спровоцировать лавинообразный процесс автоматического перемещения виртуальных машин, сопровождаемый каскадными отключениями физических серверов[4].

Размещенные в виртуальной среде информационные системы наиболее уязвимы к увеличениям нагрузок, вызванных DDoS-атаками злоумышленников, ошибками в программном обеспечении, а также нарушениями правил эксплуатации. В гетерогенной среде эта ситуация усугубляется тем, что необходимо одновременно управлять несколькими виртуальными платформами, а возможности автоматизации управления еще более ограничены совместимостью платформ.

Виртуализация физических серверов в ОАО «Оренбургоблгаз» была начата в 2011 году. Первая платформа виртуализации “Microsoft Hyper-V R2” была развернута в январе 2011 года. В феврале 2012 года на части физических серверов виртуальная платформа была изменена на XEN 4.1, что позволило значительно увеличить производительность существующих виртуальных серверов на базе ОС Ubuntu Server. Структура гетерогенной виртуальной среды представлена на рис. 1.

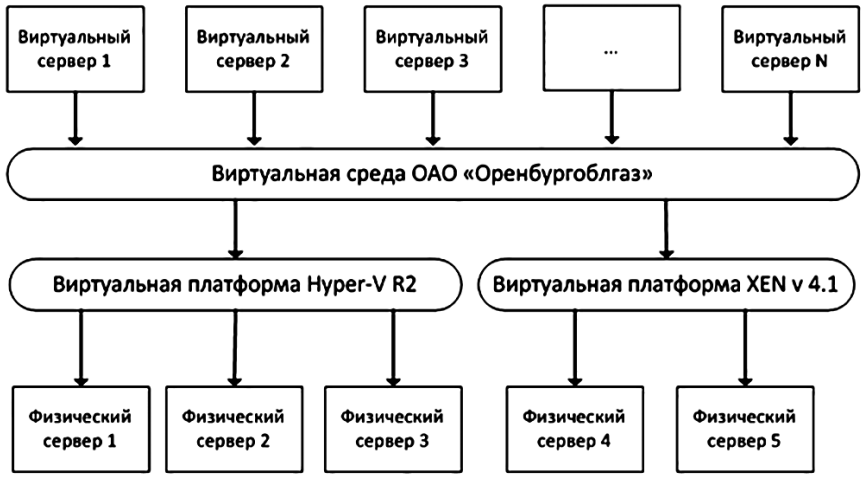

Рис. 1. Логическая структура гетерогенной виртуальной среды в ОАО «Оренбургоблгаз»

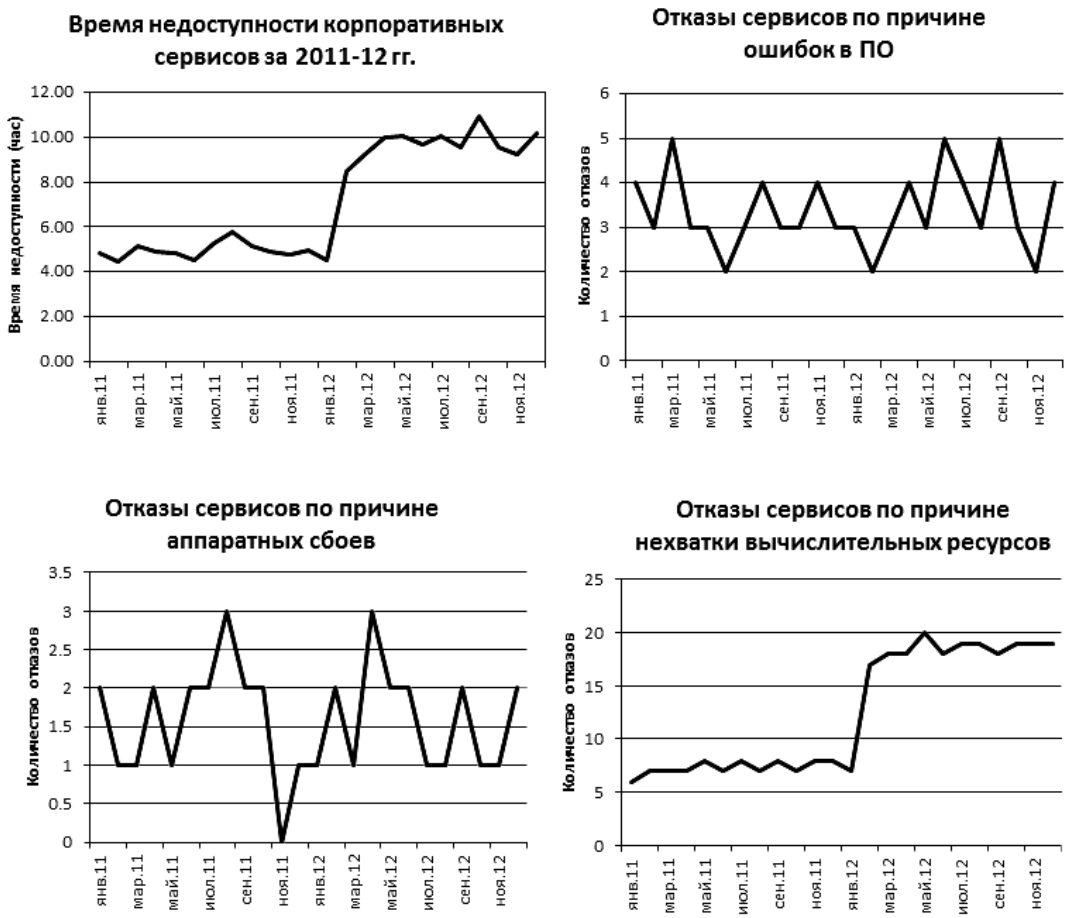

Рис. 2. Время недоступности и отказы информационных систем

Для управления и мониторинга в виртуальной среде используется программное обеспечение от производителей виртуальных платформ: Microsoft Virtual Machine Manager; Microsoft Performance Center; Virtmanager GNY GPL; XenMonitor tools GNU GPL.

После ввода в эксплуатацию второй платформы виртуализации в ОАО «Оренбургоблгаз» значительно выросло время недоступности информационных систем. Анализ причин отказов в обслуживании показал, что рост времени недоступности информационных систем вызван сбоями в работе программного обеспечения по причине нехватки вычислительных ресурсов для виртуализованных серверов. Диаграммы времени недоступности и отказов корпоративных информационных систем представлены на рис. 2.

Среднемесячное время недоступности корпоративных сервисов в ОАО «Оренбургоблгаз» в 2012 году возросло на 87%. Причиной нехватки вычислительных ресурсов во всех случаях отказов послужило некорректное распределение вычислительных ресурсов между виртуальными серверами. Несвоевременное реагирование администраторов виртуальной среды на появление растущего дефицита вычислительных ресурсов на физических серверах не позволяло вовремя выполнить перераспределение и предотвратить остановку корпоративных информационных систем.

В процессе анализа эксплуатации гетерогенной виртуальной среды выявлены следующие системные проблемы:

• в гетерогенной среде резко сократились возможности автоматического распределения вычислительных ресурсов, что увеличило вероятность появления дефицита вычислительных ресурсов на одном из участков виртуальной среды;

• для автоматизации мониторинга используются несколько различных программных продуктов, что снижает оперативность оценки состояния вычислительных ресурсов;

• в гетерогенной среде усилились последствия ошибок в распределении вычис-

лительных ресурсов, что ужесточает требования к точности оценки состояния ресурсов в виртуальной среде.

Таким образом, на основании выявленных проблем сделан вывод о недостаточной автоматизации информационных процессов мониторинга вычислительных ресурсов в гетерогенной виртуальной среде, заключающейся в низкой оперативности и точности оценки состояния вычислительных ресурсов.

Актуальность разработки программной системы

Обзор наиболее популярных программных систем, способных выполнять мониторинг вычислительных ресурсов в гетерогенных виртуальных средах выявил следующие программные продукты:

- Tivoli Monitoring от фирмы IBM[5];
- System Center от Microsoft[6];
- Veam One от фирмы Veam Software[7].

Tivoli Monitoring – позиционируется на рынке как система мониторинга вычислительных инфраструктур корпоративного уровня. Отличается широкой кроссплатформенностью, может быть развернут в различных операционных системах, поддерживает много платформ виртуализации, удобен в управлении, отличается высокой надежностью. Имеет хороший аналитический функционал. К минусам продукта можно отнести чрезвычайно высокую стоимость внедрения и поддержки, недостаточную гибкость настройки оповещений, использование разрозненных показателей производительности в модели состояния вычислительных ресурсов.

System Center от Microsoft – появился в результате слияния разных пакетов управления и мониторинга серверных продуктов. Функции мониторинга осуществляет входящий в System Center пакет Operation Manager. В последних версиях продукта в пакете появились функции мониторинга сторонних гипервизоров. Пакет отличается развитым и удобным в настройке механизмом оповещений, модель состояния вычислительных ресурсов представлена в виде разрозненных показателей, но зато имеются широкие возможности для самостоятельной настройки собственных показателей. Имеет развитый механизм формирования представлений со-

Таблица 1. Сравнительные характеристики систем мониторинга

Система мониторинга	IBM Tivoli Monitoring 7.1	MS System Center 2012	Veeam ONE v7
Операционные системы, доступные для установки программного продукта	MS Windows Server; Red Hat Enterprise Linux; Suse Linux Enterprise Server; AIX	MS Windows Server	MS Windows Server
Поддерживаемый сервер баз данных	IBM DB2	MS SQL Server	MS SQL Server
Поддерживаемые виртуальные платформы	Vmware ESX/ESXi; Citrix-XenServer; KVM	Microsoft Virtual Server; Microsoft Hyper-V; Vmware ESX/ESXi	Vmware ESX/ESXi; Microsoft Hyper-V
Стоимость лицензирования (на виртуальный сервер)	482$	x	x
Стоимость лицензирования (на физический процессор)	x	1940$	894$
Механизм статистического анализа состояния вычислительных ресурсов	есть	нет	с ограничениями
Настраиваемые представления для мониторинга вычислительных ресурсов в режиме реального времени	Есть	есть	нет
Настраиваемая система оповещений	с ограничениями	есть	есть

стояния вычислительных ресурсов. К минусам продукта можно отнести относительно высокую стоимость внедрения, отсутствие кроссплатформенности, отсутствие встроенных средств анализа, малый функционал управления сторонними виртуальными платформами, низкую надежность и высокую требовательность к вычислительным ресурсам.

Veam One от фирмы Veam Software – изначально разрабатывался как дополнительное средство управления виртуальными платформами, содержит функции, отсутствующие в стандартных средствах управления виртуальными платформами. Имеет достаточно низкую стоимость внедрения, не требователен к вычислительным ресурсам, имеет достаточно удобный, хоть и не гибкий, набор представлений состояния ресурсов, присутствует удобный механизм настраиваемых оповещений. Минусами продукта являются: отсутствие кроссплатформенности, невозможность настройки собственных представлений состояния ресурсов, всего две поддерживаемые виртуальные платформы.

Сравнительные характеристики рассматриваемых программных систем мониторинга представлены в табл. 1.

Ни один из рассмотренных продуктов не поддерживает виртуальную платформу Xen 4.1. Во всех продуктах используется модель состояния вычислительных ресурсов, основанная на отдельных несвязанных показателях, которая подвержена влиянию возмущающих воздействий со стороны управляющих операционных систем и самих гипервизоров, что снижает точность оценки состояния вычислительных ресурсов и затрудняет определение проблемных участков виртуальной среды. Рассмотренные программные продукты не способны обеспечить необходимую автоматизацию информационных процессов мониторинга в рассмотренной гетерогенной виртуальной среде, что доказывает актуальность разработки специализированной программной системы.

Концепция программной системы

Основной проблемой, возникающей при эксплуатации гетерогенной среды, является проблема единого управления, включающая проблему распределения и мониторинга вычислительных ресурсов. Мониторинг состояния ресурсов вычислительных систем, как и любая другая деятельность IT-подразделения должен проводиться в рамках определенного процесса управления. Основной целью внедрения процесса управления нагрузкой на предприятии является обеспечение оправданной нагрузки на IT-инфраструктуру, удовлетворяющей текущим и будущим потребностям бизнеса[8].

На практике мониторинг вычислительных ресурсов в виртуальных средах в первую очередь призван выявлять проблемы неэффективного использования и нехватки вычислительных ресурсов. Стремление максимально эффективно использовать физические сервера зачастую приводит к сильной конкуренции виртуальных машин и, как следствие, к снижению производительности виртуальных серверов вплоть до отказов корпоративных информационных систем. В гетерогенной виртуальной среде эта ситуация усугубляется, и увеличившееся количество отказов в обслуживании корпоративных информационных систем начинает представлять серьезную проблему для бизнеса.

Решением задачи снижения угрозы отказа в обслуживании является обеспечение достаточного количества вычислительных ресурсов на всех узлах виртуальной среды. Для эффективного размещения виртуальных серверов на физических узлах необходимо выделение групп узлов со схожими значениями ресурсообеспеченности из общего множества. Необходимость выделения групп узлов определяется задачей миграции виртуализованных серверов в группу с высокой ресурсообеспеченностью. Таким образом, процедура оценки состояния вычислительных ресурсов в гетерогенной виртуальной среде заключается в распределении физических узлов по группам ресурсообеспеченности с минимальным количеством ошибок и принимает вид целевой функции:

$$R\ (U(P_n), A) \xrightarrow{F} \min,$$

где R – ошибки классификации;

U – множество узлов гетерогенной виртуальной среды;

P_n – n-мерное пространство признаков классификации;

A – множество алгоритмов классификации.

Единая система мониторинга предполагает централизованное удаленное наблюдение за целевыми вычислительными системами.

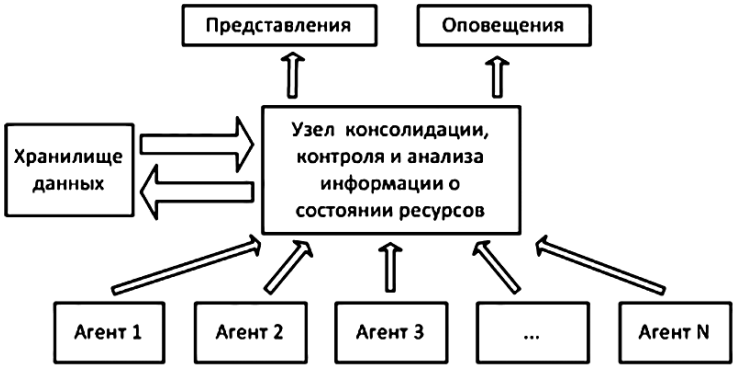

Рис. 3. Концептуальная модель системы мониторинга вычислительных ресурсов

Системы удаленного мониторинга построены по клиент–серверной модели, взаимодействие клиента и сервера осуществляется с помощью стандартных, либо же собственных протоколов, данные передаются через сети передачи данных[9]. Как правило, подобные системы используют доказавшую свою эффективность агент-ориентированную архитектуру. Концептуальная модель агент - ориентированной системы мониторинга приведена на рис. 3. В соответствии с этой моделью автономные программные агенты самостоятельно осуществляют сбор различных сведений о текущем состоянии ресурсов в целевых вычислительных системах и передают их в узел консолидации, контроля и анализа. Узел консолидации, контроля и анализа регистрирует поступающие сведения и использует их для пополнения реализуемой модели состояния вычислительных ресурсов в наблюдаемых вычислительных системах, используя выделенное хранилище для данных модели. Узел осуществляет постоянный контроль модели состояния ресурсов и при достижении заранее заданных критических условий оповещает пользователя. Также пользователь имеет доступ к различным представлениям модели состояния вычислительных ресурсов, на основании которых принимаются решения и выполняются операции по управлению вычислительными системами.

Основной проблемой разработки систем мониторинга ресурсов в виртуальных средах является невозможность использования стандартных системных библиотек для получения сведений об использовании вычислительных ресурсов[10].

На рис. 4 представлена стандартная архитектура гипервизора смешанного типа.

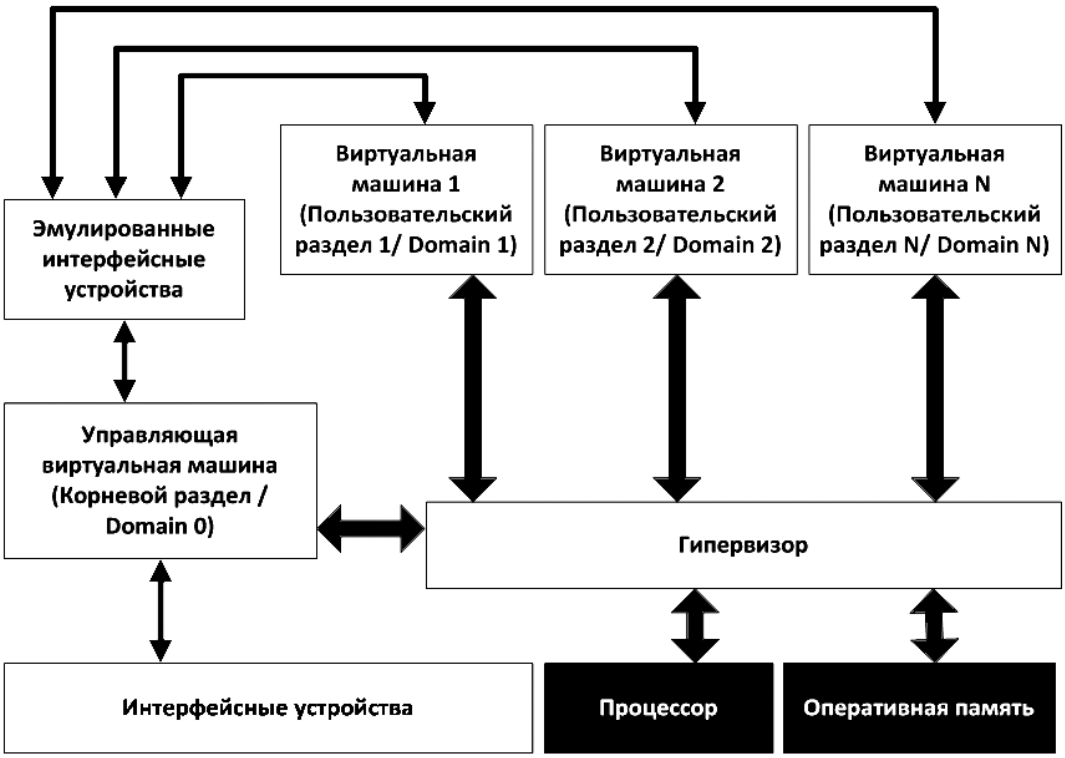

Рис. 4. Архитектура гипервизора смешанного типа

В соответствии с представленной архитектурой, непосредственное управление оперативной памятью и процессорным временем имеет только гипервизор, все виртуальные машины не имеют сведений о реальном использовании этих ресурсов. Доступ к ресурсам интерфейсных устройств (сетевые интерфейсы, дисковые подсистемы) предоставляется управляющей операционной системой, гостевые виртуальные машины также не имеют к ним доступа[11]. В связи с этим программные агенты систем мониторинга для получения сведений о состоянии вычислительных ресурсов должны использовать API управления конкретных гипервизоров. Эти API могут различаться даже в разных версиях одного гипервизора, что ограничивает число поддерживаемых виртуальных платформ в любой системе мониторинга.

Таким образом, программная система мониторинга вычислительных ресурсов в гетерогенной виртуальной среде должна удовлетворять следующим требованиям:

• агенты системы должны функционировать в различных операционных системах;

• для получения сведений о состоянии вычислительных ресурсов агенты должны использовать API различных гипервизоров и собирать сведения о состоянии различных вычислительных ресурсов на физических узлах виртуальной среды;

• система мониторинга должна использовать модель состояния вычислительных ресурсов, исключающую влияние случайных отклонений и дающую целостную картину состояния вычислительных ресурсов в виртуальной среде;

• система мониторинга должна предоставлять гибкую настройку и различные методы оповещения пользователей.

Выводы

Бурное развитие технологий виртуализации привело к возникновению феномена гетерогенных виртуальных сред. Производители виртуальных платформ и разработчики программных средств управления вычислительной инфраструктурой оказались не готовы к удовлетворению требований, накладываемых использованием разных платформ виртуализации для решения задач обеспечения доступности информационных систем. Существующие на рынке средства управления и мониторинга гетерогенных виртуальных сред не способны существенно снижать уровень угрозы отказа в обслуживании, что доказывает необходимость и актуальность разработки других программных систем, использующих новые модели и средства автоматизации.

Прммечания

[1] Черняк Л. Виртуализация серверов стандартной архитектуры // Открытые системы. СУБД. 2008. № 3. С. 40–47.

[2] Ширманов А. Е. Сосуществование гипервизоров – обычное явление? // COMNEWS Новости телекоммуникаций, вещания и ИТ: ежедневная интернет-газета. 2013. URL: http:// www.comnews.ru/ node/76551 (дата обращения: 03.12.2013).

[3] Bittman T. G00233251 Reconsidering Heterogeneous x86 Server virtualization. Stamford: Gartner Inc., 2012. 8 p.

[4] Черняк Л. Реальная безопасность виртуальных серверов // Открытые системы. СУБД. 2009. № 3. С. 60–62.

[5] Darmawan B., Chen G., Varkonyi L. End-to-End Planning for Availability and Performance Monitoring. Indianapolis: IBM press, 2008. 172 c.

[6] Ricks B. System Center 2012 R2 Operations Manager Documentation. Portland: Microsoft press, 2013. 1389 c.

[7] Veeam ONE for VMware vSphere and Hyper-V [Электронный ресурс] // Veeam: Modern Data Protection – Built for Virtualization: [сайт]. [2013]. URL: http://www.veeam.com/one-vmware-hyper-v-monitoring-reporting.html (дата обращения: 02.12.2013)

[8] Белкин П. Заметки о мониторинге виртуальной инфраструктуры // Intelligent Enterprise/RE («Корпоративные системы»). 2008. № 2. С. 7–8.

[9] Сильнов Д. С. Актуальность современных систем удаленного мониторинга вычислительных ресурсов // Известия Российского государственного педагогического университета им. А. И. Герцена. 2011. № 141. С. 56–57.

[10] Menon A. Diagnosing performance overheads in the Xen virtual machine environment // Proceedings of the 1st ACM/USENIX international conference on Virtual execution environments. 2005. P. 13–23.

[11] Гордеев А. В., Молчанов А. Ю. Системное программное обеспечение. СПб. : Питер, 2001. 736 с.

References

[1] Chernyak L. Virtualizatsiya serverov standartnoi arkhitektury [Virtualization of Servers of the Standard Architecture] // Otkrytye sistemy. SUBD. 2008. No. 3. p. 40–47.

[2] Shirmanov A.E. Sosushchestvovanie gipervizorov - obychnoe yavlenie? [Is Coexistance of Hypervizors a Common Phenomenon?]// COMNEWS- Novosti telekommunikatsii, veshchaniya i IT: ezhednevnaya internet gazeta. 2013. URL: http:// www.comnews.ru/node/76551 (Date of Access: 03.12.2013).

[3] Bittman T. G00233251 Reconsidering Heterogeneous x86 Server virtualization. Stamford: Gartner Inc., 2012. 8 p.

[4] Chernyak L. Real'naya bezopasnost' virtual'nykh serverov [Real Security of Virtual Servers]// Otkrytye sistemy. SUBD. 2009. No. 3. p. 60–62.

[5] Darmawan B., Chen G., Varkonyi L. End-to-End Planning for Availability and Performance Monitoring. Indianapolis: IBM press, 2008. 172 s.

[6] Ricks B. System Center 2012 R2 Operations Manager Documentation. Portland: Microsoft press, 2013. 1389 s.

[7] Veeam ONE for VMware vSphere and Hyper-V [Electronic Resource] // Veeam: Modern Data Protection – Built for Virtualization: [Web-site]. [2013]. URL: http://www.veeam.com/one-vmware-hyper-v-monitoring-reporting.html (data ob-rashcheniya: 02.12.2013)

[8] Belkin P. Zametki o monitoringe virtual'noi infrastruktury [Notes on Monitoring of Virtual Infrastructure]// Intelligent Enterprise/RE («Korporativnye sistemy»). 2008. No. 2. p. 7-8.

[9] Sil'nov D.S. Aktual'nost' sovremennykh sistem udalennogo monitoringa vychislitel'nykh resursov [Urgent Character of Modern Systems of Remote Monitoring of Computational Resources] // Izvestiya Rossiiskogo gosudarstvennogo pedagogicheskogo universiteta im. A. I. Gertsena. 2011. No. 141. P. 56-57.

[10] Menon A. Diagnosing performance overheads in the Xen virtual machine environment // Proceedings of the 1st ACM/USENIX international conference on Virtual execution environments. 2005. P. 13–23.

[11] Gordeev A.V., Molchanov A.Yu. Sistemnoe programmnoe obespechenie [System Programming Software]. St. Petersburg: Piter Publ., 2001. 736 p.

Тыщенко Сергей Валерьевич, бакалавр техники и технологий, ведущий программист. E-mail: tyshchenko@eplink.ru

Соловьев Николай Алексеевич, доктор технических наук, профессор, заведующий кафедрой программного обеспечения вычислительной техники и автоматизированных систем, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Оренбургский государственный университет». E-mail: povt@unpk.osu.ru

Sergey Valerievich Tyschenko, Bachelor of Technics and Technology. Leading programmer of JSC 'Orenburgoblgas'. E-mail: tyshchenko@eplink.ru

Nikolai Alekseevich Soloviev, PhD Engineering, Professor, Head of the Department of Programming Software of Computational Machinery and Automated Systems, Orenbugr State University. E-mail: povt@unpk.osu.ru

УДК 342.72+002:004:342.72

Поперина Е. Н.

ЧАСТНАЯ ЖИЗНЬ В УСЛОВИЯХ ИНФОРМАТИЗАЦИИ ОБЩЕСТВА

В статье рассмотрены вопросы, связанные с реализацией конституционного права на неприкосновенность частной жизни в условиях информатизации общества. В частности, выявлены и раскрыты новые современные угрозы праву на неприкосновенность частной жизни, представляющие собой особую опасность в силу отсутствия или недостаточно четкого их закрепления в действующем законодательстве; проанализированы основные прецеденты нарушения частной жизни в условиях информатизации общества. Исходя из анализа, сформулированы прогнозы реализации права на неприкосновенность частной жизни в информационном обществе, а также предложены меры по защите рассматриваемого права.

Ключевые слова: *конституционное право на неприкосновенность частной жизни, защита права на неприкосновенность частной жизни, угрозы неприкосновенности частной жизни, частная жизнь, информатизация, информация.*

Poperina E. N.

PRIVACY IN THE CONDITIONS OF INFORMATIZATION OF SOCIETY

In the article the questions connected with realization of the constitutional right to privacy in the conditions of Informatization of society. In particular, identified and disclosed new modern threats to the right to privacy, which represent a special risk due to the lack of or unclear of their fastening in the current legislation; review the major cases of violation of privacy in the conditions of Informatization of society. Based on the analysis, formulated predictions of the realization of the right to privacy in the information society, as well as proposed measures for the protection of the considered law.

Keywords: *the constitutional right to privacy, the protection of the right to privacy, threats to privacy, privacy, information.*

Уважение к частной жизни лица представляет собой один из аспектов индивидуальной свободы. Это предоставленная человеку и гарантированная государством возможность контролировать информацию о самом себе, а также препятствовать разглашению сведений личного, интимного характера. Но несмотря на то, что право на неприкосновенность частной жизни признается и гарантируется государством, существует множество угроз данному праву.

В рамках данной статьи рассматриваются новые современные угрозы неприкосновенности частной жизни, которые, на наш взгляд, представляют собой особую опасность рассматриваемому праву ввиду отсутствия или

недостаточно четкого их закрепления в законодательстве. Однако главной причиной, способствующей появлению новых угроз приватности, является развитие информационных технологий и переход к информатизации общества.

Одной из таких угроз является применение технологий определения местонахождения. Суть угрозы сводится к тому, что с помощью устройств спутниковой системы глобального позиционирования (GPS) можно определить местонахождение объектов.

Кроме того, по всему миру находит новые сферы применения технология RFID-меток, дающая возможность отслеживать перемещение их носителей. RFID-метки используются для маркировки товаров в магазинах с целью отследить потребительское поведение покупателей. Особую опасность представляет разработанный в Дании новый вид винтовки, производящей выстрелы микроскопическими RFID-чипами, позволяющими метить людей незаметно для них самих[1].

Разработчики приводят ряд аргументов, свидетельствующих о пользе в использовании RFID-меток: экономическая выгода, экономия времени, предотвращение преступлений и т. д. Однако необходимо обратить внимание на ряд угроз неприкосновенности частной жизни, возникающих вследствие применения данных технологий:

1) возможность дистанционного считывания информации с RFID-метки без ведома ее владельца;

2) возможность отслеживания перемещений злоумышленниками;

3) возможность заражения RFID-метки компьютерным вирусом, что может привести к искажению информации, содержащейся в RFID-метке;

4) возможность перехвата передаваемых данных;

5) возможность присутствия скрытого считывающего устройства и т. д.

Отметим, что прецеденты нарушения права на неприкосновенность частной жизни посредством использования RFID-меток уже существуют. Например, американская компания Caspian, ведущая борьбу за невмешательство супермаркетов в частную жизнь граждан, призвала к всемирному бойкоту Компании Gillette, использующей RFID-маркировку своей продукции. В рамках эксперимента по оптимизации продаж в супермаркетах Tesco в Великобритании возмущение покупателей вызвал тот факт, что человек, взявший с полки упаковку с продукцией фирмы Gillette, сразу попадает под прицел видеокамеры, которая отслеживает его путь до самого выхода из магазина. Gillette отверг обвинения, мотивируя это тем, что введение RFID-маркировки было произведено исключительно для оптимизации торговли. Правозащитные организации США и Великобритании подписали воззвание к представителям индустрии информационных технологий с предложением добровольно прекратить разработку и внедрение RFID-меток. Среди прочих воззвание подписали Американский союз гражданских свобод, Информационный центр электронной конфиденциальности и британская организация Исследований информационной политики[2].

Полагаем, что произвол в сфере использования технологии RFID-меток помогут предотвратить следующие меры:

1) законодательное закрепление ограничений по использованию RFID-меток;

2) уведомление покупателей о товарах, содержащих RFID-метки (например, путем нанесения на них предупреждающих знаков);

3) введение законодательных ограничений на использование информации, полученной при помощи RFID-меток;

4) законодательное закрепление запрета на определение местонахождения человека без его предварительного согласия, допуская ограничения в экстренных случаях.

В качестве еще одной новой угрозы неприкосновенности частной жизни следует выделить уязвимость биометрических систем. Биометрия представляет собой систему идентификации человека по его физиологическим и поведенческим чертам. В настоящее время существует множество способов распознания людей: идентификация по дактилоскопическим данным, радужной оболочке глаза, по голосу, почерку и т. д. Биологические системы идентификации применяются как на особо охраняемых объектах, так и в общественных местах в целях обеспечения безопасности. Наиболее распространенным является применение систем идентификации в аэропортах. Так, например, в США предусмотрена процедура фотосъемки и дактилоскопии для иностранных граждан, въезжающих в США[3].

Странами «Большой восьмерки» были приняты стандарты о внедрении высокотехнологических паспортов, снабженных ми-

крочипами. Основываясь на этих стандартах, в России была создана нормативно-правовая база для внедрения государственной системы изготовления, оформления и контроля паспортно-визовых документов нового поколения с использованием биометрической информации[4]. В настоящее время в России биометрические данные вносятся в заграничные паспорта. Вполне вероятно, что в скором будущем такие данные будут вноситься и в гражданские паспорта россиян, как это уже осуществляется в некоторых странах.

Нельзя не отметить, что внесение биометрических персональных данных в паспорта таит в себе серьезную угрозу не только для частной жизни граждан, но и для безопасности государства. Основная опасность для частной жизни заключается в том, что после внесения биометрических персональных данных в паспорт гражданина того или иного государства появляется возможность дистанционного снятия таких данных, что неизбежно приведет к созданию тотальной системы средств слежения за людьми. Так, иностранные спецслужбы смогут с легкостью отследить военнослужащих и сотрудников спецслужб того или иного государства, носящих при себе паспорта, что непременно приведет к снижению возможностей национальных вооруженных сил и спецслужб по защите своего государства.

Таким образом, выражая отрицательное отношение к применению биометрических технологий, отметим, что их использование непременно приведет не только к ограничению прав и свобод российских граждан, но и к тотальному контролю над людьми, что угрожает безопасности не только Российской Федерации, но и любого другого государства.

Примечания

[1] Байковски Д. Шпионы внутри нас // Computerworld Россия. – 2004. – № 20.

[2] Во зло или во благо? // Все о вашей безопасности. – 2003. – № 4.

[3] Пятаков С. Страны, где проводят дактилоскопию въезжающих граждан. Справка // РИА Новости [Электронный ресурс] – Режим доступа: [ria.ru/spravka/20110617/389554429.html].

[4] Кочева О. Граждане под контролем технологий // Личное дело. – 2004. - № 9 (79).

References

[1] Bajkovski D. Shpiony vnutri nas // Computerworld Rossija. – 2004. – №20.

[2] Vo zlo ili vo blago? // Vse o vashej bezopasnosti. – 2003. - №4.

[3] Pjatakov S. Strany, gde provodjat daktiloskopiju v#ezzhajushhih grazhdan. Spravka // RIA Novosti [Jelektronnyj resurs] – Rezhim dostupa: [ria.ru/spravka/20110617/389554429.html].

[4] Kocheva O. Grazhdane pod kontrolem tehnologij // Lichnoe delo. – 2004. - №9 (79).

Поперина Екатерина Николаевна, преподаватель кафедры правовых дисциплин, филиал Южно-Уральского государственного университета в г. Озерске. E-mail: poperina@mail.ru

Poperina Ekaterina, Legal Disciplines Department , Ozersk branch of the South Ural State University (National research University). E-mail: poperina@mail.ru.

УДК 002:004.738.5+004.738.5:316.472.4

Лазуков А. С.

ОРГАНИЗАТОР РАСПРОСТРАНЕНИЯ ИНФОРМАЦИИ В СЕТИ ИНТЕРНЕТ

В статье раскрывается понятие «распространитель информации в сети Интернет», ставятся основные вопросы, необходимые для точности определения понятия. В статье автор дает перечень основных целей и задач, которые стоят перед распространителями информации в сети Интернет, раскрываются основные группы видов деятельности, при которых обеспечивается функционирование информационных систем и программного обеспечения для передачи электронных сообщений по сети Интернет. Отдельно в статье раскрыто понятие «информационная система» и приведены виды объектов распространения информации. Приведены примеры технических средств и программного обеспечения. Дано понятие «организатор массового распространения информации в сети Интернет», наиболее характеризующее данный субъект по мнению автора.

Ключевые слова: *распространение информации, массовая информация, размещение информации, организатор распространения информации.*

Lazukov A. S.

ORGANIZER DISSEMINATION OF INFORMATION IN THE INTERNET

The article explains the concept of information in the distributor network «Internet», put the main issues needed for precision definition. The author gives a list of the main goals and objectives facing the disseminators of information in the network «Internet», reveals the main groups of activities which provide functioning of information systems and software for the transmission of electronic communications network «Internet». Separately, in the article the concept of information system and object types are given information dissemination. Are examples of hardware and software. Given the concept of «organizer of mass dissemination of information in the network» Internet «» most characterizes the entity according to the author.

Keywords: *Dissemination of information, media, placement of information, dissemination of information organizer.*

На современном этапе развития административного права аппарат государственного контроля расширяет список своих объектов во всех сферах общественных отношений. Причиной данных действий государства, на мой взгляд, является не столько отсутствие доверия к сознательности граждан, сколько прогрессирующее развитие научно-технического прогресса, вывод в массы новых сфер деятельности, которые нуждаются в нормативном урегулировании.

Федеральный закон «Об информации, информационных технологиях и о защите информации» в последнее время претерпевает значительные изменения и дополнения. 1 августа 2014 года вступил в силу Федеральный закон от 05.05.2014 № 97-ФЗ «О внесении изменений в Федеральный закон “Об информации, информационных технологиях и о защите информации” и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с

использованием информационно-телекоммуникационных сетей», регулирующий данный вид общественных отношений и вносящий новые понятия в нормативно-правовую базу Российской Федерации. В данном нормативно-правовом акте усилия законодателей направлены на регулирование информации в сети Интернет, размещаемой пользователями сети Интернет, не являющимися сотрудниками интернет-изданий, СМИ, членами общественных организаций и объединений, но при этом имеющими достаточное количество «потребителей» этой информации, которое может превышать аудиторию официальных СМИ.

Новинкой для отечественного законодательства становятся понятия «организатор распространения информации в сети Интернет» и «блоггер», давно вошедшие в современный обиход интернет-пользователей. Законодатель дал данные определения, и можно смело предположить о возможных проблемах, которые повлечет толкование данных понятий. *Организатором распространения информации в сети Интернет является лицо, осуществляющее деятельность по обеспечению функционирования информационных систем и (или) программ для электронных вычислительных машин, которые предназначены и (или) используются для приема, передачи, доставки и (или) обработки электронных сообщений пользователей сети Интернет*[1]. Данное понятие, на мой взгляд, является запредельно широким и не конкретизирует данную категорию пользователей. Чтобы раскрыть суть понятия, необходимо охарактеризовать его «состав».

«Можно спорить, что это не так и таким лицом является владелец сайта или публичного почтового сервера, но у себя дома именно я обеспечиваю функционирование почтовой программы и никто иной. Так что размытость формулировки может сыграть злую шутку с авторами закона, которые требуют регистрации 70 миллионов пользователей Интернета в Роскомнадзоре»[2]. Из данного закона следует, что организатором распространения информации в сети Интернет является лицо, осуществляющее деятельность по обеспечению функционирования информационных систем и (или) программ для электронных вычислительных машин, которые предназначены и (или) используются для приема, передачи, доставки и (или) обработки электронных сообщений пользователей сети Интернет. Из данного определения выстраивается ряд вопросов, которые также нуждаются в урегулировании.

1. С какой целью информация размещается в сети Интернет? Данный вопрос имеет непосредственное значение, пользователь, выкладывая информацию в сеть Интернет, не всегда сознательно желает массового распространения информации, либо имеет безразличное к этому отношение. Пользователи «всемирной паутины» сети при размещении информации в сети Интернет, как правило, преследуют данные цели:

• в целях извлечения прибыли, осуществляя коммерческую деятельность. К данной категории мы можем отнести все без исключения организации, торгующие товарами или предлагающие услуги с помощью сети Интернет;

• в целях удовлетворения информационных потребностей населения. Человек нуждается в информации, преимущественному большинству интересно и важно знать о текущей ситуации в тех или иных сферах общественных отношений. У каждого индивида свой круг интересов и увлечений, свой вид профессиональной деятельности, свои ценности. В данную категорию входят специализированные СМИ, выпускающие в свет информационные продукты определенных тематических категорий;

• в целях создания идеологического фона. Современной мировой политической системе присущ плюрализм, множество политических партий, общественных и религиозных объединений, общественных движений. Необходимым атрибутом перечисленных объектов является наличие собственных СМИ, что играют немаловажную роль в жизни различных социальных институтов и выполняют возложенные на них задачи информирования населения, поиска новых членов объединений или просто неравнодушных граждан, формирования общественного мнения. В современной политике данная информация играет ведущую роль в сознании общества;

• в собственных личных целях. Появление множества так называемых социальных сетей дает возможность всем пользователям размещать любую информацию в любом виде воспроизведения (текст, фото, видео и др.) для реализации своих личных потребностей. Необходимо также заметить, что данная информация доступна для неограниченного

круга лиц, и распространитель информации сам регулирует доступ к ней;

• в целях распространения информации. К этой категории относится распространение информации через любые ресурсы сети Интернет с целью дать возможность получить эту информацию любому пользователю в любом объеме, примером будут являться файлообменные сети.

2. Каким образом происходит обеспечение функционирования информационных систем и программ для ЭВМ? С 2000 по 2008 год темпы роста применения информационных технологий в России составили 20–30% в год, по итогам 2007 года в РФ насчитывалось порядка 31,5 млн компьютеров, но, однако, события финансового кризиса 2008 года не оправдали ожидания аналитиков, рост количества электронных вычислительных устройств временно уменьшился. В связи с последними политическими событиями на Украине стала заметна нестабильность курса рубля, что очень негативно повлияло на развитие рынка компьютеров и других телекоммуникационных устройств. Оценивая современную ситуацию, учитывая нестабильность роста рынка информационных технологий, верным остается факт того, что информатизация в России идет успешно, и количество электронных вычислительных устройств, подавляющее большинство из которых имеет доступ в сеть Интернет, увеличивается. Обеспечение функционирования информационных систем и программ для ЭВМ является очень распространенным видом деятельности. Можем ли мы прировнять деятельность профессионального программиста, дизайнера, журналиста, системного администратора к деятельности рядового пользователя, ведь пусконаладочные работы в Дата-Центре нельзя ставить в одну линию с настройкой почтового клиента у себя на домашнем компьютере. Варианты «обеспечения функционирования» можно разделить по нисходящей на три уровня:

• создание программного обеспечения, разработка оборудования для передачи, хранения и обработки информации. Наивысший уровень, основной характеристикой которого является отличительный субъектный состав, как правило, это высококвалифицированные в области информационных технологий специалисты, сюда входят инженеры, создающие оборудование для хранения, обработки и передачи информации, программисты, ведущие разработки программ для ЭВМ;

• профессиональная деятельность, связанная с обслуживанием информационных систем, обновлением контента, требующая специальной подготовки и специальных навыков. Информатизация диктует для рынка труда свои условия, в последние 20 лет появилось множество востребованных профессий, таких как системные администраторы, контент-редакторы web-сайтов, операторы ЭВМ, дизайнеры (имеются в виду дизайнеры, использующие для творчества специальные технические и программные средства). Как и в первом уровне, данные специальности объединяет общий признак, особенностью которого является квалификация субъекта. Но наличие знаний и подготовки необходимо для правильного применения и использования как оборудования, так и программ для ЭВМ;

• деятельность по обеспечению работы персональных устройств. Низший, но самый широкий по кругу субъектов уровень. Объем продаж персональных компьютеров, планшетов, ультрамобильных компьютеров и мобильных телефонов в 2014 году вырастет на 7,6% по сравнению с 2013 годом и достигнет 2,5 млрд устройств[4]. Учитывая, что население земли в 2014 году составляет 7,2 млрд человек[5], мы можем делать выводы о значительной доле интернет-пользователей среди мирового населения, и каждый участник информационного процесса, используя собственное устройство, *осуществляет деятельность по обеспечению функционирования информационных систем и (или) программ для электронных вычислительных машин, которые предназначены и (или) используются для приема, передачи, доставки и (или) обработки электронных сообщений пользователей сети Интернет*[6].

3. Какие имеются виды объектов обеспечения функционирования? Из данного законодателем понятия мы можем выделить два основных объекта обеспечения функционирования: информационные системы и программы для ЭВМ. Согласно ст. 2 п. 4 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» информационная система – это совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств[7], отсюда ясно, что техни-

ческие средства являются неотъемлемой частью информационных систем. Изучив рынок информационных услуг, а именно сферы деятельности специалистов данного рынка, мы видим огромное количество лиц, занимающихся обеспечением деятельности технических средств, от проектировщика линий связи до программиста социальной сети. Даже если считать под техническими средствами только те, которые обеспечивают обработку информации в базах данных, все равно круг как оборудования, так и задействованных специалистов очень широк. Деятельность по проектированию линий связи, прокладке линий связи, пусконаладочным работам, обслуживание линий связи, разработка программного обеспечения для линий и оборудования связи, разработка и производство оборудования связи, продвижение услуг связи и др. – это все то, что мы можем объединить под понятие *обеспечение функционирования технических средств*. Соответственно, широким будет перечень видов технических средств: волоконно-оптические линии связи, серверное оборудование, коммуникационное оборудование, проводные линии связи, устройства беспроводной связи, конечное оборудование пользователя и технические системы и устройства с измерительными функциями[8]. Что касается баз данных, то перечень субъектов обеспечения функционирования и перечень объектов не могут быть шире, чем у технических средств. Согласно ч. 2 ст. 1260 Гражданского кодекса Российской Федерации (часть четвертая) базой данных является представленная в объективной форме совокупность самостоятельных материалов (статей, расчетов, нормативных актов, судебных решений и иных подобных материалов), систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью электронной вычислительной машины (ЭВМ)[9]. Соответственно, выделяются две характеристики базы данных: совокупность информации и систематизированность таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью ЭВМ. Деятельность по обеспечению функционирования баз данных можно свести к следующим действиям: создание базы данных, изменение базы данных, пополнение базы данных, систематизация и индексация информации в базе данных, регулирование доступа к базе данных. Данными действиями занимаются правообладатели (изготовители) базы данных, т. е. лица, организовавшие создание базы данных и работу по сбору, обработке и расположению составляющих ее материалов[10]. Последним видом объекта обеспечения функционирования является программа для ЭВМ. Законодатель дает уточнение – программа для ЭВМ должна предназначаться или использоваться для приема, передачи, доставки и (или) обработки электронных сообщений пользователей сети Интернет[11]. Если проанализировать рынок программного обеспечения, в частности обратить внимание на свободно распространяемое программное обеспечение (freeware), а к этой категории относится абсолютное большинство программ web-браузеров (Opera, Mozilla Firefox, Google Chrome, Internet Explorer, Yandex Browser, Safari), то можно сделать выводы о распространенности программ данной категории. В частности программа web-браузер присутствует в стандартном комплекте программ для любого нового компьютера или портативного устройства; в первую очередь, именно браузер дает возможность приема, передачи, обработки электронных сообщений пользователей сети Интернет. Обратим внимание на программы – сетевые клиенты: социальные сети выпускают собственные программы-клиенты, которые основной целью имеют подключение к социальной сети, обмен электронными сообщениями, загрузку и просмотр контента в пределах указанной социальной сети. Так же имеют собственные программы-клиенты сайты блог-платформы, такие как Я.ру и LiveJournal, а несколькими годами ранее огромную популярность имели программы обмена мгновенными сообщениями. В обеспечении функционирования программы для ЭВМ задействованы как разработчики этой программы (программисты и дизайнеры) и специалисты по обслуживанию и настройке, так и рядовые пользователи, которые самостоятельно для личного и (или) служебного использования устанавливают, настраивают и используют программное обеспечение на персональных компьютерах и портативных устройствах.

Рассмотрев ряд основных вопросов, считаю целесообразным выделить понятие «организатор массового распространения информации в сети Интернет».

*Организатором **массового** распространения информации в сети Интернет является лицо, осуществляющее торговую, реклам-*

ную, журналистскую, агитационную или другого вида деятельность по обеспечению функционирования информационных систем и (или) программ для электронных вычислительных машин, которые предназначены и (или) используются для приема, передачи, доставки и (или) обработки информации, выраженной в любой способной к восприятию объективной форме[12] (текстовой, аудиовизуальной, и др.), доступной неограниченному кругу лиц, с целью достижения наибольшего распространения информации.

Основными критериями для отнесения субъектов информационного обмена к организаторам массового распространения информации в сети Интернет являются:

• вид деятельности, как правило, профессиональный вид деятельности, направленный на обеспечение функционирования информационных систем;

• нахождение информации, которую распространяют в открытом доступе, то есть пользователь Интернета не имеет никаких ограничений на просмотр данной информации, может в любое время получить к ней доступ и распространить ее далее;

• распространяемая информация может быть в любой форме, понятие «электронное сообщение» я считаю слишком узким. Распространитель должен руководствоваться законодательством, распространяя информацию в любом виде;

• распространитель имеет цель максимального распространения информации в обществе посредством сети Интернет, то есть распространитель будет прибегать к мерам технического и программного характера с целью увеличения круга потребителей информации.

При этом необходимым считаю также изменить понятие «организатор распространения информации в сети Интернет», расширив вид информации, аналогично понятию «Организатор массового распространения информации в сети Интернет».

Примечания

[1] Федеральный закон от 05.05.2014 № 97-ФЗ «О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей». Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 05.05.2014

[2] «Под определение "организатор распространения информации в сети Интернет" подпадают все пользователи» Алексей Лукацкий. Информационный ресурс об инновациях и идеях для развития бизнеса iBusiness.ruhttp://ibusiness.ru/blog/ekspyertiza/32018 (дата обращения 28.05.2014).

[3] RB.ru – Бизнес-информация и Деловое сообщество. А. Паршуков «Количество компьютеров на душу населения.» http://www.rb.ru/article/kolichestvo-kompyuterov-na-dushu-naseleniya/5128777.html (дата обращения 28.05.2014).

[4] Издательство «Открытые системы» Gartner: в 2014 году рынок персональных компьютеров и мобильных устройств вырастет на 7,6%. http://www.osp.ru/news/2014/0110/13022663/ (дата обращения 02.06.2014).

[5] ВГТРК. Вести. Экономика. ООН: население Земли достигло 7,2 млрд человек http://www.vestifinance.ru/articles/41515 (дата обращения 02.06.2014).

[6] Федеральный закон от 05.05.2014 № 97-ФЗ «О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей». Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 05.05.2014.

[7] Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 28.12.2013) «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 01.02.2014) // Российская газета – 2006. – 27 июл. – № 165.

[8] Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» (ред. от 23.06.2014) // Российская газета – 2003. – 10 июл. – № 135.

[9] Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ (ред. от 23.07.2013) // Российская газета – 2006. – 22 дек. – № 289.

[10] Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ. Ст. 1333 (ред. от 23.07.2013) // Российская газета – 2006. – 22 дек. – № 289.

[11] Федеральный закон от 05.05.2014 № 97-ФЗ «О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей». Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 05.05.2014.

[12] Минбалеев А. В. «Система информации: теоретико-правовой анализ» : дис. … канд. юрид. наук, Челябинск, 2006. С. 35.

References

[1] Federal Law of 05.05.2014 N 97-FZ «On Amending the Federal Law» On Information, Information Technologies and Protection of Information «and some legislative acts of the Russian Federation on streamlining the exchange of information with the use of information and telecommunication networks» The official internet-portal of legal information http://www.pravo.gov.ru, 05.05.2014,

[2] «The definition of the» organizer information dissemination in the «Internet» get all users «Alexei Lukatskii. Information resource about innovation and ideas for business development iBusiness.ruhttp :/ / ibusiness.ru/blog/ekspyertiza/32018 (date accessed 05/28/2014)

[3] RB.ru - Business information and business community. A. Parshukov «The number of computers per capita.» http://www.rb.ru/article/kolichestvo-kompyuterov-na-dushu-naseleniya/5128777.html (date accessed 28/05/2014)

[4] Publisher «Open Systems» Gartner: in 2014 the market of personal computers and mobile devices will grow by 7.6% http://www.osp.ru/news/2014/0110/13022663/ (date accessed 02.06.2014)

[5] RTR. News. Economy. UN world population reached 7.2 billion people http://www.vestifinance.ru/articles/41515 (date accessed 02.06.2014)

[6] Federal Law of 05.05.2014 N 97-FZ «On Amending the Federal Law» On Information, Information Technologies and Protection of Information «and some legislative acts of the Russian Federation on streamlining the exchange of information with the use of information and telecommunication networks» The official internet-portal of legal information http://www.pravo.gov.ru, 05.05.2014,

[7] Federal Law of 27.07.2006 N 149-FZ (as amended on 28.12.2013) «On Information, Information Technologies and Protection of Information» (with rev. And ext., Entered. Into force on 01.02.2014) «Rossiyskaya Gazeta», N 165, 29.07.2006,

[8] Federal Law of 07.07.2003 N 126-FZ «On communication» (as amended on 23.06.2014) «Rossiyskaya Gazeta», N 135, 10.07.2003,

[9] The Civil Code of the Russian Federation (Part Four) from 18.12.2006 N 230-FZ (as amended on 23.07.2013) «Rossiyskaya Gazeta», N 289, 22.12.2006,

[10] The Civil Code of the Russian Federation (Part Four) from 18.12.2006 N 230-FZ Art. 1333 (as amended on 23.07.2013) «Rossiyskaya Gazeta», N 289, 22.12.2006, p. 1333

[11] Federal Law of 05.05.2014 N 97-FZ «On Amending the Federal Law» On Information, Information Technologies and Protection of Information «and some legislative acts of the Russian Federation on streamlining the exchange of information with the use of information and telecommunication networks» The official internet-portal of legal information http://www.pravo.gov.ru, 05.05.2014,

[12] Minbaleev A. V. «Information system: theoretical and legal analysis» : dis. ... cand. jurid. Sciences, Chelyabinsk, 2006. P. 35

Лазуков Александр Сергеевич, аспирант Уральского финансово-юридического института. E-mail: 4447191@mail.ru

Lazukov Alexander Sergeevich, Ural Institute of Finance and Law. E-mail: 4447191@mail.ru

УДК 343.131

Даровских С. М.

К ВОПРОСУ О НЕДОПУСТИМОСТИ РАЗГЛАШЕНИЯ ДАННЫХ ПРЕДВАРИТЕЛЬНОГО РАССЛЕДОВАНИЯ КАК СПОСОБЕ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ГРАЖДАН

В статье рассматриваются актуальные вопросы, связанные с обеспечением безопасности участников уголовного судопроизводства в результате распространения информации, полученной в ходе предварительного расследования уголовных дел. Автор рассматривает основания, требующие от следователей, дознавателей принятия решения о запрете разглашения информации, круг лиц, на которых может распространяться указанный запрет, тот объем информации по уголовному делу, который может находиться под запретом разглашения, ограничения, либо любые сведения, ставшие участнику процесса известными в связи с определенным уголовным делом.

Ключевые слова: *информация, безопасность, участники, уголовное судопроизводство, разглашение.*

Darovskikh S. M.

TO THE QUESTION OF INADMISSABILITY OF INFORMATION DISCLOSURE ON INTRODUCTORY INVESTIGATION AS A MEANS OF PROVIDING CIVIL SAFETY

The article dwells on topical issues connected with provision of civil safety in criminal proceedings as a result of information distribution obtained in introductory investigation. The author considers foundation and grounds which demand from investigators the decisions on in-

terdiction on information disclosure, as well as the scope of persons on which the abovementioned interdiction is disseminated, the scope of information on a criminal offence which can be under the interdiction on information disclosure or the information which came to notice in connection with certain criminal case.

Keywords: *information, security, participants, criminal procedings, interdiction.*

Понятие «безопасность» в последнее время получило широкое распространение во всем мире. В российской науке понятие «безопасность и ее обеспечение» толкуется как в широком смысле, так и в более узком, применимо к определенной отрасли права. Ученые-процессуалисты неоднократно обращались к вопросу обеспечения безопасности граждан, вовлеченных в уголовный процесс, например О. А. Зайцев, Г. П. Химичева, А. П. Гуляев, В. Т. Томин, С. П. Щерба и другие. Одну из наиболее удачных формулировок понятия «безопасность в уголовном судопроизводстве» сформулировала М. В. Новикова, которая дала следующее определение данной правовой категории: «безопасность в уголовном судопроизводстве – это состояние защищенности жизни, здоровья, прав и законных интересов участников уголовного судопроизводства, а также их имущества от каких-либо посягательств и наличия возможности у указанных лиц беспрепятственно выполнять возложенные на них обязанности и реализовать свои права в уголовном процессе»[1].

Защита прав и обеспечение безопасности граждан, вовлеченных в орбиту уголовного судопроизводства, а также эффективность и объективность расследования предполагают принятие различных мер, к которым следует отнести и необходимость сохранения в тайне информации, полученной в ходе предварительного расследования. Еще в 2008 году уполномоченный по правам человека в Российской Федерации В. Лукин писал, что «ежегодно жертвами преступлений становятся до 4 миллионов человек. Четвертая часть потерпевших по тем или иным причинам отказались от своих показаний в процессе судебного разбирательства. Примерно столько же не явились в суд вообще. Около 60 процентов лиц, пострадавших от разного рода преступлений, предпочитают не обращаться в правоохранительные органы, будучи уверенными, что защиты они не получат. До 90 процентов опрошенных ответили, что в случае угрозы их жизни или здоровью откажутся от показаний или дадут ложные показания»[2]. Безусловно, существует множество причин данного поведения граждан, и одна из этих причин – это разглашение информации, полученной при расследовании уголовного дела. Заинтересованные лица, получив соответствующую интересующую их информацию, могут оказывать и оказывают давление на потерпевших, свидетелей и иных участников процесса (специалистов, переводчиков, экспертов), в результате чего участники меняют показания, выполняют требуемые от них действия, а уголовные дела утрачивают перспективу в суде.

Определенной гарантией правильного поведения участников предварительного расследования выступают ст. 161 УПК РФ, озаглавленная законодателем «Недопустимость разглашения данных предварительного расследования», помещенная в главу 21 «Общие условия предварительного расследования», и статья 310 УК РФ, которая предусматривает уголовную ответственность за нарушение указанного поведения и разглашения данных предварительного расследование. Однако можно ли считать их надлежащим образом работающими, если за несколько лет в России были зафиксированы чуть более 20 случаев разглашений данных предварительного расследования? Результаты же расследования этих дел оставляют желать лучшего: только по 54 процентам уголовных дел были установлены виновные, а 46 процентов преступлений остались нераскрытыми. Из раскрытых только 60 процентов были направлены в суды, но 40 процентов из них были прекращены в судах по реабилитирующим основаниям[3].

Очевидно, данная статистика объяснима и ожидаема, поскольку изучение диспозиции статьи 161 УПК РФ не позволяет однозначно ответить на ряд важных вопросов. Например, какие основания позволят следователю, дознавателю принять решение о неразглашении данных предварительного расследования? Должно ли данное решение в обязательном порядке распространяться на всех участников уголовного судопроизводства, либо предупреждены могут быть только отдельные участники процесса? Требует ли реше-

ние о предупреждении о неразглашении данных предварительного расследования вынесения отдельного постановления следователем? Какой объем информации по уголовному делу может находиться под запретом разглашения, либо любые сведения, ставшие участнику процесса известными в связи с определенным уголовным делом? И, наконец, обладателями ценной для кого-то информации могут стать не только участники процесса, наделенные определенным статусом, такие как потерпевший, обвиняемый, подозреваемый, переводчик, эксперт, защитник, но и не имеющие процессуального статуса, но участвующие в процессе лица, поскольку п. 58 ст. 5 УПК РФ определяет, что участники уголовного судопроизводства – лица, принимающие участие в уголовном процессе. К ним могут быть отнесены, например, статисты – участники следственного действия, опознания; заявитель – лицо, обнаружившее преступление, лица, которые по требованию следователя, в рамках доследственной проверки например, проводили ревизию или инвентаризацию, либо лица, у которых при проведении доследственной проверки были получены объяснения, а также другие участвующие в процессе лица. То есть круг лиц, которые могут обладать и распространять определенную информацию, достаточно широк.

Анализируя диспозицию статьи 161 УПК РФ, нельзя сделать однозначный вывод, что требование о неразглашении данных предварительного расследования, в частности подписка о неразглашении, применяется во всех случаях и по всем уголовным делам. Данное решение принимает должностное лицо и по своему усмотрению. Как правило, должностные лица, следователи, дознаватели, начальники органа дознания, руководители следственного органа начинают применять данное средство обеспечения безопасности участников уголовного судопроизводства, если появляется информация о наличии заинтересованных лиц в определенном решении по конкретному уголовному делу, которые уже совершают либо готовятся совершить определенные действия в ущерб интересам следствия. Но эта информация может появиться не с первого дня расследования. Однако к этому времени участники процесса, как представители заинтересованных сторон, так и просто причастные к расследуемым событиям (знакомые, родственники потерпевшего, заявитель, родственники и близкие люди обвиняемого, подозреваемого, свидетели, понятые), по недомыслию, незнанию ситуации, доверчивости и прочим причинам могут распространить те сведения о той части расследования и его результатах, которые стали им известны. Своевременно не предупрежденные в соответствии с законом, участники процесса невольно могут и создают ситуацию, исправить которую бывает невозможно, и тем самым ставят под угрозу безопасность иных участников процесса, а в некоторых случаях и перспективу уголовного дела. Данное обстоятельство диктует, на наш взгляд, целесообразность информирования участников процесса, которым стали известны обстоятельства уголовного дела, о недопустимости их разглашения непосредственно в момент, когда указанные данные предварительного расследования стали им известны. Например, если в соответствии со ст. 170 УПК РФ при проведении осмотра места происшествия по решению следователя участвуют понятые, которым становится известно о доказательствах, полученных при совершении данного следственного действия, то вполне разумно предупредить их о недопустимости разглашения данного факта сразу после окончания осмотра. Исследования, проводимые в этом плане показали, что чаще всего, до 90%, разглашалась информация, полученная в ходе проведения следственных действий[4].

Рассуждая о том, следует ли решение о недопустимости разглашения данных предварительного расследования распространять в обязательном порядке на всех участников уголовного судопроизводства, либо предупреждаться могут только отдельные участники процесса, мы приходим к выводу, что всех участников процесса невозможно предупредить о недопустимости разглашения сведений, полученных в ходе предварительного расследования. Определенная категория лиц, в частности представляющая сторону защиты, априори не может входить в число лиц, с которых может быть получена подписка о предупреждении об уголовной ответственности в соответствии со статьей 310 УК РФ. Это подозреваемый и обвиняемый по уголовному делу. Данные лица вправе защищать себя любыми средствами и способами, и какие-либо ограничения в этом плане не могут быть оправданы и рассматриваться ни эффективными для хода расследования, ни целесообразными. Поэтому распростра-

нение сведений, сообщение о любых данных, известных им о ходе процесса, кому-либо может рассматриваться только как способ защиты от обвинения и никак более. Мы также полагаем, что требование о неразглашении информации, полученной в ходе предварительного расследования, должно обязательно соблюдаться и защитниками-адвокатами. Сложность, на наш взгляд, здесь состоит в том, что адвокат-защитник не может и не должен скрывать от своего доверителя информацию, которая стала ему известна, так как обязан использовать для осуществления защиты все средства и способы, но разглашать информацию по делу другим лицам он не вправе, и данное требование закреплено в части 3 статьи 53 УПК РФ, и если это произойдет и сведения, относящиеся к уголовному делу по которому он выступает защитником, будут им преданы огласке без разрешения следователя, дознавателя, должны наступить соответствующие последствия. Можно привести следующий пример: следственными органами Следственного комитета по Калининградской области было возбуждено уголовное дело в отношении адвоката-защитника одного из филиалов Калининградской областной коллегии адвокатов по признакам преступления предусмотренного ст. 310 УК РФ. Решение о возбуждении уголовного дела принято следствием по материалам проверки, проведенной службой собственной безопасности управления Федеральной службы по контролю за оборотом наркотиков по Калининградской области. По версии следствия, в феврале 2014 года при осуществлении защиты прав и интересов подозреваемого по уголовному делу о незаконном обороте наркотических средств адвокат дала подписку о неразглашении данных предварительного расследования. При этом в установленном законом порядке она была предупреждена об уголовной ответственности за разглашение таких сведений без разрешения дознавателя УФСКН. Как полагает следствие, невзирая на дачу подписки и требования закона, адвокат умышленно разгласила значимую по уголовному делу информацию, полученную ею в ходе участия в следственных действиях. В результате данные предварительного расследования стали известны посторонним лицам, имеющим личную заинтересованность в исходе дела[5].

И последнее: рассматривая некоторые проблемы, относящиеся к недопустимости разглашения данных предварительного расследования как способе обеспечения безопасности граждан, следует остановиться на вопросе, какой объем информации по уголовному делу может находиться под запретом разглашения. Могут ли это быть только конкретные данные любого уголовного дела, либо любые сведения, ставшие известными участнику процесса? Как нам представляется, что абсолютно вся информация, относящаяся к расследованию уголовного дела и полученная в рамках предварительного расследования, не может представлять тайну следствия. Например, факт проведения обыска в квартире (доме) подозреваемого, как правило, сразу становится известен жителям подъезда жилого дома либо соседних домов. К информации, разглашение которой может повлиять на ход и результаты расследования, либо поставить под угрозу безопасность участников процесса, на наш взгляд, следует отнести: любые сведения о лицах, втянутых в орбиту расследования уголовного дела, их местожительстве, родственниках; виды доказательств полученных в ходе предварительного расследования должностными лицами правоохранительных органов, как непосредственно, так и в результате отдельных поручений, а также их содержание; место и время проведения следственных действий, и данные о том, какие именно следственные действия собирается проводить следователь, дознаватель. Применимо к тактике следственного действия не должны разглашаться сведения о тактических решениях, тактических приемах и тактических комбинациях.

Однако любые меры, предпринимаемые для ограничения разглашения данных предварительного расследования, не могут никаким образом ограничивать возможность реализации прав участников уголовного судопроизводства. И поэтому любой участник процесса в случае дачи им подписки о неразглашении данных предварительного расследования вправе потребовать от следователя конкретизации той информации, которую он не вправе разглашать.

Примечания

[1] Новикова М. В. Обеспечение безопасности участников уголовного судопроизводства как гарантия осуществления правосудия в современных условиях : автореферат дис. ... канд. юрид. наук. – Екатеринбург, 2006. – С. 9.

[2] Специальный доклад Уполномоченного по правам человека в Российской Федерации В. Лукина. Проблемы защиты прав потерпевших от преступлений // Российская газета. – 2008. – 04 июня. – № 4676.

[3] Тепляшин П. Недопустимость разглашения данных предварительного расследования. // Режим доступа: http://www.lawmix.ru

[4] Новикова М. А. Расследование разглашения данных предварительного расследования и сведений о мерах безопасности, применяемых в отношении участников уголовного судопроизводства : автореферат дис. ... канд. юрид. наук. – М., 2009. – С. 18.

[5] В Калининграде адвокат обвиняется в разглашении данных предварительного расследования // Режим доступа: http://www.kld.sledcom.ru

References

[1] Novikova M. V. Obespechenie bezopasnosti uchastnikov ugolovnogo sudoproizvodstva kak garantija osushhestvlenija pravosudija v sovremennyh uslovijah [Security Provision for Participants of Criminal Proceeding as a Guaranty of Justice in Modern Conditions]. Avtoreferat diss. kand. jurid. nauk [Synopsis of Thesis of Cand. Sc. Law]. – Yekaterinburg, 2006. – p.9.

[2] Special report of the human-rights ombudsman of the Russian Federation, L.V. Lukin. Problems of protection of rights of victims of crimes // Rossijskaja gazeta. – 04.06.2008. – No. 4676.

[3] Tepljashin P. Nedopustimost' razglashenija dannyh predvaritel'nogo rassledovanija [Inadmissability of Information Disclosure on Introductory Investigation] // http://www.lawmix.ru

[4] Novikova M. A. Rassledovanie razglashenija dannyh predvaritel'nogo rassledovanija i svedenij o merah bezopasnosti, primenjaemyh v otnoshenii uchastnikov ugolovnogo sudoproizvodstva [Investigation of Information Disclosure on Introductory Investigation and Information on Measures of Security]. Avtoreferat kand. jurid. nauk [Synopsis of Thesis of Cand. Sc. Law]. – Moscow, 2009. – p. 18.

[5] A lawyer is convinced of information disclosure on introductory investigation in Kaliningrad // http://www.kld.sledcom.ru

Даровских Светлана Михайловна, доктор юридических наук, профессор, заведующий кафедрой уголовного процесса и криминалистики ЮУрГУ. E-mail darsvet@mail.ru

Svetlana Mikhailovna Darovskikh, Phd Law, professor, chairholder of the Department of the Criminal Proceedings and Criminal Science of the South Ural State University. E-mail darsvet@mail.ru.

УДК 659.1+351.766.2:002:004+347.157:004.056

Дорогова Е. В.

РЕКЛАМА И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ДЕТЕЙ

В статье рассматриваются проблемные вопросы регулирования сферы рекламы в контексте защиты детей от информации, причиняющей вред их здоровью и развитию. Проводится анализ отдельных положений ФЗ РФ «О защите детей от информации, причиняющей вред их здоровью и (или) развитию» и ФЗ РФ «О рекламе». Анализируются различные модели защиты детей от вредной информации в разных странах.

Ключевые слова: *информация, вредная информация, реклама, защита детей.*

Dorogova E. V.

ADVERTISING AND INFORMATION SECURITY OF CHILDREN

The article deals with the problematic issues regulation of advertising in the context of the protection of children from information harmful to their health and development. The analysis of certain provisions of the Federal Law "On protection of children from information harmful to their health and (or) development" and the Federal Law "On Advertising". The various models of protecting children from harmful information on the different countries.

Keywords: *information, harmful information, advertising, protection of children.*

В настоящее время актуальной остаётся дискуссия о практической реализации норм Федерального закона Российской Федерации «О защите детей от информации, причиняющей вред их здоровью и (или) развитию». В частности, высказываются негативные мнения по поводу исключения рекламы из сферы действия указанного закона. Среди высказываемых мыслей встречаются достаточно категоричные, например, И. В. Жилавская пишет, что исключение «рекламы из сфер, подлежащих экспертизе, контролю, ограничению в соответствии с новым законом, скорее всего кроется в миллиардных бюджетах рекламных компаний, которые, очевидно, не пожалели средств на сохранение существующего положения вещей»[1]. Но действительно ли законодатель создал пробел по вопросам регулирования рекламы с вредной для детей информацией? Для того чтобы разобраться в данном вопросе, предлагается провести сравнительный анализ некоторых положений двух федеральных законов – «О защите детей от информации, причиняющей вред их здоровью и (или) развитию» и «О рекламе». Целесообразно начать сравнение именно с запрещённых к распространению среди детей видов информации, то есть той информации, которая должна распространяться со знаком информационной продукции «18+». Так, п. 1 ч. 2 ст. 5 ФЗ «О защите детей от информации, причиняющей вред их здоровью и (или) развитию» запрещает распространение среди детей информации, «побуждающей детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству»[2]. Аналогичное положение содержится в ФЗ «О рекламе», так, п. 6 ст. 6 запрещает «показ несовершеннолетних в опасных ситуациях, включая ситуации, побуждающие к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоро-

вью»[3]. Информация «способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством» не допускается и в рекламе, так как п. 3 ч. 5 ст. 5 ФЗ «О рекламе» запрещает использовать в рекламе демонстрацию процессов курения и потребления алкогольной продукции, ст. 21 посвящена запретам и ограничениям в отношении рекламы алкогольной продукции, ст. 7 этого же закона запрещает рекламу «наркотических средств, психотропных веществ и их прекурсоров, растений, содержащих наркотические средства или психотропные вещества либо их прекурсоры, и их частей, содержащих наркотические средства или психотропные вещества либо их прекурсоры», ст. 27 содержит нормы, запрещающие направленность рекламы игр и пари на несовершеннолетних, а ч. 4 ст. 5 гласит, что реклама не должна «побуждать к совершению противоправных действий». Запрет на побуждение к насилию и жестокости также присутствует в обоих рассматриваемых законах, в п. 3 ч. 2 ст. 5 ФЗ «О защите детей от информации, причиняющей вред их здоровью и (или) развитию» и в п. 1 ч. 4 ст. 5 ФЗ «О рекламе». Нормы, направленные на защиту семейных ценностей, содержатся в п. 4 ч. 2 ст. 5 «О защите детей от информации, причиняющей вред их здоровью и (или) развитию» и в ст. 6 ФЗ «О рекламе». Также ФЗ «О рекламе» запрещает использование бранных слов, показ противоправных действий и информацию порнографического характера в рекламе, что отвечает требованиям законодательства о защите детей от вредной информации. А что касается информации, пропагандирующей нетрадиционные сексуальные отношения, то следует отметить, что ФЗ «О рекламе» не содержит запретов на использование в рекламе подобного рода информации, однако пропаганда нетрадиционных сексуальных отношений среди несовершеннолетних запрещена ст. 6.21 КоАП РФ[4], а значит и реклама не может содержать такую информацию.

Теперь стоит выяснить, разрешена ли в рекламе информация, ограниченная к распространению среди детей определённых возрастных категорий. Информация, представляемая в виде изображения или описания половых отношений между мужчиной и женщиной, может расцениваться как использование в рекламе непристойных образов, недопустимость чего устанавливается ч. 6 ст. 5 ФЗ РФ «О рекламе». Запрет на использование бранных слов, не относящихся к нецензурным выражениям, содержится в той же статье рассматриваемого закона. Однако норм, которые бы запрещали или ограничивали использование информации, представляемой в виде изображения или описания жестокости, физического и (или) психического насилия, преступления или иного антиобщественного действия; вызывающей у детей страх, ужас или панику, в том числе представляемой в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий, в рекламе не предусмотрено. Также не отражается в законе «О рекламе» запрет на распространение среди детей информации о несовершеннолетнем, пострадавшем от правонарушения.

Таким образом, некоторые виды информации, запрещённой или ограниченной к распространению среди детей, в принципе не могут быть использованы в рекламе! Однако для остальных видов вредной для детей информации и на случай изобретательности креативных работников рекламной сферы законодательно закреплён запрет на распространение рекламы, содержащей информацию, запрещенную для распространения среди детей в предназначенных для детей образовательных организациях, детских медицинских, санаторно-курортных, физкультурно-спортивных организациях, организациях культуры, организациях отдыха и оздоровления детей или на расстоянии менее чем сто метров от границ территорий указанных организаций[5].

На основании вышеизложенного можно сделать вывод, что законодательное выведение рекламы из сферы регулирования ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» – это не пробел, не оплошность и тем более не сознательное разрешение манипулировать детьми с помощью рекламы запрещённой информацией. Такой обход сферы рекламы в законодательстве о защите детей от вредной информации необходим, чтобы сохранить традиционный взгляд на приоритет специальных норм права перед общими. Но, тем не менее,

нельзя не отметить, что существующее законодательное решение проблемы защиты детей от вредной информации в рекламе не идеально и требует доработок.

Во-первых, вполне закономерно возникает необходимость приведения законодательных формулировок в рассматриваемых нами нормативно-правовых актах к единому виду, чтобы избежать продолжения существующих споров и возникновения возможных коллизий.

Во-вторых, дискуссии об эффективности детской рекламы и необходимости обеспечить информационную безопасность детей существуют на общемировом уровне, и каждое государство справляется с этой проблемой по-разному. Так, например, в § 3 ст. 5 Закона «О сети эфирного и кабельного телевидения и коммерческой рекламы на радио и телевидении» Бельгии содержится положение о запрете показа элементов «телевизионных программ, ориентированных в первую очередь на детей младше двенадцати лет, непосредственно после или перед за коммерческой рекламой»[6]. Безусловно, этот метод не оградит детей от рекламы вообще, но он может существенно уменьшить просмотр телевизионной рекламы детьми, разумеется, при наличии родительского контроля времени нахождения ребёнка у телевизора. Китайская Народная Республика по-другому решает вопрос о защите детей от информации в рекламе. В ст. 8 Закона КНР «О рекламе» содержится положение о том, что реклама не должна причинять ущерб духовному и физическому здоровью несовершеннолетних»[7]. И хотя в Китае принимаются достаточно жёсткие меры по ограничению опасного для детей контента в Интернете, но именно законодательство о рекламе содержит лишь декларативную норму о защите детей от информации. В Республике Казахстан данный вопрос решается в ст. 8 Закона «О рекламе» путём запрета на прерывание детских передач рекламой, за исключением рекламы, предназначенной для детей и подростков[8]. А также путём закрепления в ч. 2 ст. 17 данного закона положения о предотвращении и пресечении рекламы, посягающей на общественные ценности и общепринятые нормы морали и нравственности, как основном направлении деятельности государства[9]. Таким образом, разрешена только детская реклама, а вот большинство видов «вредной информации» в РК не могут быть использованы в рекламе вообще.

На основе даже этих примеров видно, что модели защиты детей от информации в рекламе встречаются разнообразные, более чётко выделяются две группы: выделяющие детскую рекламу и налагающие общие ограничения на рекламу, независимо от целевой аудитории.

Выделение детской рекламы и регулирование информации, используемой в ней, осуществляется также несколькими путями в разных странах:

1) разрешение показывать до и после детских передач только детскую коммерческую рекламу;

2) запрет на использование вредной для детей информации в рекламе для детей и подростков;

3) обязательное одобрение властей детской рекламы;

4) запрет на детскую рекламу во всех СМИ.

Во второй группе выделяются следующие ограничения:

1) запрет на показ во время, до и после детских передач любой коммерческой рекламы;

2) запрет на использование в рекламе информации, не отвечающей целям духовного оздоровления нации;

3) запрет на прямое обращение в рекламе к детям.

Рассуждая о том, какая же из рассмотренных моделей подходит нашей стране, необходимо учитывать и российскую ментальность, и моральное здоровье современного общества, и рвение населения к использованию своего права на свободу слова. С одной стороны, если учесть столь неспокойное и небезопасное время, в котором мы живём, то, возможно, есть смысл внести поправки в ФЗ «О рекламе» в виде всего одной строчки: «Запрещается использование в рекламе информации, запрещённой или ограниченной к распространению среди детей». И тогда хотя бы реклама будет чуть добрее, нравственнее и спокойнее, по сравнению с большим количеством негативной информации, окружающей нас в повседневной жизни. С другой стороны, использование несколько агрессивной рекламы – это теперь неотъемлемая составляющая современного мышления, и возможно, что та же реклама – это один из способов подготовиться подростку к тому массиву разнообразной по эмоциональной окраске ин-

формации, который получают взрослые люди. И вновь этот вопрос остаётся неоднозначным, и у специалистов разных сфер остаются разные взгляды на данную проблему, а значит, предстоит проделать ещё немалую работу по разрешению существующих дискуссий на тему защиты детей от вредной информации в рекламе.

Примечания:

[1] Жилавская И. В. Проблемы информационной безопасности детей через призму нового закона – 2011 // Сайт Научно-издательского центра «Социосфера». URL: http://sociosphera.com/publication/conference/ 2011/118/problemy_informacionnoj_bezopasnosti_detej_cherez_prizmu_novogo_zakona/

[2] П. 1 ч. 2 ст. 5. ФЗ РФ «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29 декабря 2010 г. № 436-ФЗ // Российская газета. – 2010. – № 5376.

[3] П. 6 ст. 6 ФЗ РФ «О рекламе» от 13 марта 2006 г. № 38-ФЗ // Российская газета. – 2006. – № 51.

[4] Ст. 6.21 ФЗ РФ «Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001 № 195-ФЗ // Российская газета. – 2001. – № 256.

[5] Ч. 10.2 ст. 5 ФЗ РФ «О рекламе» от 13 марта 2006 г. № 38-ФЗ // Российская газета. – 2006. – № 51.

[6] § 3 ст. 5 Закона Королевства Бельгии «О сети эфирного и кабельного телевидения и коммерческой рекламы на радио и телевидении» от 06.02.1987 // Сайт Всемирной организации интеллектуальной собственности WIPO. URL: http://www.wipo.int/wipolex/ru/text.jsp?file_id=263986

[7] Ст. 8 Закона КНР «О рекламе» // Законодательство и практика масс-медиа. URL: http://www.medialaw.ru/publications/zip/161/7.htm

[8] Ст. 8 Закона Республики Казахстан «О рекламе» от 19.12.2003 № 508-II // Информационные системы Параграф. URL: http://online.zakon.kz/ Document/?doc_id=1045608

[9] Ч. 2 ст. 17 Закона Республики Казахстан «О рекламе» от 19.12.2003 № 508-II // Информационные системы Параграф. URL: http://online.zakon.kz/ Document/?doc_id=1045608

References

[1] Zhilavskaya, I.V. Problemy informatsionnoi bezopasnosti detei cherez prizmu novogo zakona [Problems of Information Security of Children through the Prism of the New Law] – 2011 // Web-site of Scientific Publishing Center «Sotsiosfera». URL: http://sociosphera.com/publication/conference/ 2011/118/problemy_informacionnoj_bezopasnosti_detej_cherez_prizmu_novogo_zakona/

[2] Item 1 of part 2 of the article 5 of the Federal Law of the Russian Federation «On Defense of Children from Information Harmful for their Health and Development» as of December 29, 2010 No. 436-FZ // Rossiiskaya gazeta. – 2010. – No. 5376. (In Russ.)

[3] Item 6 of the article 6 of the Federal Law of the Russian Federation «On Advertising» as of March 13, 2006 No. 38-FZ // Rossiiskaya gazeta. - 2006. – No. 51. (In Russ.)

[4] Article 6.21 6 of the Federal Law of the Russian Federation «Administrative Code of the Russian Federation» as of 30.12.2001 No. 195-FZ // Rossiiskaya gazeta. – 2001. – No. 256. (In Russ.)

[5] Part 10.2 of the article 5 6 of the Federal Law of the Russian Federation «On Advertising» as of March 13, 2006 No.38-FZ // Rossiiskaya gazeta. - 2006. – No.51. (In Russ.)

[6] Paragraph 3 of the article 5 of the Law of the Belgian Kingdom «On Terrestrial and Cable Television and Commercial Advertising on Radio and Television» as of 06.02.1987 // Web-site of the WIPO. URL: http://www.wipo.int/wipolex/ru/text.jsp?file_id=263986

[7] Article 8 of the Law of PRC «On Advertising» // Legislation and Practice of Mass Media. URL: http://www.medialaw.ru/publications/zip/161/7.htm

[8] Article 8 of the Law of the Republic of Kazakhstan «On Advertising» as of 19.12.2003 No. 508-II // Paragraf Information System. URL: http://online.zakon.kz/ Document/?doc_id=1045608 (In Russ.)

[9] Part 2 of the article 17 of the Law of the Republic of Kazakhstan «On Advertising» as of 19.12.2003 No. 508-II // Paragraf Information System. URL: http://online.zakon.kz/ Document/?doc_id=1045608 (In Russ.)

Дорогова Евгения Вадимовна, ассистент кафедры Государственных и гражданско-правовых дисциплин факультета подготовки сотрудников правоохранительных органов, «Южно-Уральский государственный университет» (НИУ). E-mail: EVgeniyA2406@yandex.ru

Dorogova Eugenia Vadimovna, assistenst of State and civil disciplines department, faculty of Law enforcement officials training «South Ural State University» (national research university). E-mail: EVgeniyA2406@yandex.ru

УДК 005.922.1 + 347.96138 + 343.45

Соболев А. А.

СООТНОШЕНИЕ КАТЕГОРИЙ РЕЗУЛЬТАТА ИНТЕЛЛЕКТУАЛЬНОЙ ДЕЯТЕЛЬНОСТИ И СЕКРЕТА ПРОИЗВОДСТВА (НОУ-ХАУ)

В статье проводится анализ имеющихся в научной литературе точек зрения на природу результатов интеллектуальной деятельности и секретов производства. Проводится сравнение данных объектов как род и вид.

Ключевые слова: *интеллектуальное право, результат интеллектуальной деятельности, секрет производства, ноу-хау.*

Sobolev A. A.

CORRESPONDENCE OF THE CATEGORIES OF THE RESULT OF THE INTELLECTUAL ACTIVITY AND THE SECRET OF PRODUCTION (KNOW-HOW)

The article dwells on the analysis of the scientific viewpoints on the results of intellectual activity and secrets of production. The comparison of both categories is given according to the type and class.

Keywords: *intellectual right, result of the intellectual activity, secret of production, know how.*

Статья 1225 Гражданского кодекса Российской Федерации (далее – ГК РФ) содержит исключительный перечень результатов интеллектуальной деятельности (далее – РИД) и средств индивидуализации, приравненных к ним, охраняемых законом. Под номером 12 в этом списке числится и секрет производства (ноу-хау), что говорит о том, что законодатель формально относит секрет производства к РИД. Однако справедливость отнесения секрета производства (ноу-хау) к РИД вызывает сомнения в научном сообществе. Так, Е. А. Кондратьева пишет, что ноу-хау нельзя отнести ни к РИД, ни к средствам индивидуализации [1. С. 18]. Э. Гаврилов в своей статье прямо указывает на то, что секрет производства не относится к категории РИД [2. С. 25].

Для обеспечения полноты исследования представляется необходимым провести обзор точек зрения на понятие и признаки РИД, имеющихся в литературе.

Отечественное законодательство не даёт легальной дефиниции РИД. Как справедливо отметила М. А. Астахова, «определения, сло-

жившиеся по её поводу (по поводу легальной дефиниции РИД. – Примеч. автора) в правовой литературе, отличаются значительным разнообразием» [3]. Проведём краткий обзор мнений авторов о том, что же такое РИД и какими признаками они обладают.

О. В. Новосельцев приводит следующее определение: «понятие "результаты интеллектуальной деятельности" предлагается определить как индивидуально-определенную и зафиксированную на материальных носителях или посредством материальных носителей документированную информацию, созданную в результате интеллектуального труда, в отношении которой в определенных законом случаях признается исключительное право интеллектуальной собственности» [4. С. 106].

М. В. Волынкина в своей работе даёт следующее определение: «результат творческой (интеллектуальной) деятельности – это выраженный в объективной форме ее продукт, именуемый в зависимости от его характера научным или научно-техническим результатом, достижением либо изобретением, промышленным образцом, товарным знаком, произведением науки, литературы, искусства» [5. С. 2].

Э. Гаврилов: «Результаты интеллектуальной деятельности (РИД) – это такие нематериальные объекты, которые созданы творческим трудом гражданина. Указанный гражданин признается автором РИД» [2. С. 26].

М. А. Астахова [3] выделяет следующие признаки: 1. источник возникновения РИД – умственная деятельность; 2. легитимность – объектами гражданских прав могут выступать только те виды РИД, которые прямо обозначены в законе; 3. новизна РИД. При этом отмечается, что для разных РИД это требование принимает разные формы; 4. объективная форма. Результаты умственного труда для того, чтобы стать доступными для других участников правовых отношений, нуждаются во внешнем выражении.

В. А. Дозорцев [6. С. 38] выделяет следующие свойства объекта исключительных прав, под которыми следует понимать РИД: этот объект имеет нематериальный характер; объект также должен иметь коммерческую ценность, выступать в экономическом обороте; объект должен иметь эстетическое или информационное содержание; объект должен поддаваться обособлению от других, смежных с ним объектов. Также автор указывает, что для предоставления охраны такому объекту необходимо указание закона.

Согласно мнению Л. Б. Гальперина и Л. А. Михайлова, РИД присущи такие признаки, как возможность стоимостной оценки, наличие авторов, непотребляемость, возможность использования неопределённым кругом лиц [7. С 11].

С. А. Бабкин указывает на следующие признаки: нематериальная природа, объективная форма, передаваемость посредством воспроизведения, правовая определённость, коммерческая ценность [8. С. 10].

Из приведённых положений видно, что авторские позиции относительно признаков РИД имеют как сходства, так и различия. Проанализируем эти позиции и на основе анализа попытаемся вывести общее понятие РИД.

Первый признак, который встречается в половине представленных точек зрения, а в другой половине выводится из иных признаков, это связь РИД и интеллектуального труда. На важность данного признака указывает уже само название данной группы объектов гражданского права. Характеризуя интеллектуальный труд, посредством которого создаются РИД, часто говорят о творческом характере данного труда. Именно отсутствием творческого начала при создании ноу-хау обосновывают невозможность отнесения его к РИД. Далее этот момент будет обсуждён подробнее.

Вторым признаком, который можно выделить, является нематериальность РИД. Идеи, концепции, информация как таковые существуют в нашем сознании, которым и порождаются. С этим признаком тесно связан другой, а именно признак наличия у РИД объективной формы. Не покинув сознания создателя, результат его мыслительной деятельности не сможет найти путь к другим людям, а более того, такой РИД не получит законодательную защиту, так как его существование попросту не будет очевидно для любых участников гражданских правоотношений, кроме автора. Стоит отметить, что форма объективизации РИД должна соответствовать установленным законом правилам.

Следующий признак – это признак коммерческой ценности, или стоимостной оценки. Вопрос стоимостной оценки РИД сам по себе заслуживает отдельного рассмотрения как со стороны юристов, так и со стороны экономистов. Оценка РИД характеризуется такими особенностями, как первостепенное

значение в науке личного творческого начала, уникальность труда и его продукта; воплощение в результатах научного труда вклада, не только настоящего, но и прошлого труда; разовый характер затрат живого и овеществленного труда в процессе создания того или иного научного продукта; высокая степень неопределенности сроков и вероятность достижения намеченных научных результатов [9. С. 59]. Также указывают на отсутствие прямой связи между затратами и результатами, затраченным временем, интеллектуальными усилиями и значимостью научного продукта; сложность оценки творческого труда и его продукта; неадекватная интеллектуальным затратам исследователя оплата труда; разнообразие форм материально-предметного воплощения научных продуктов; неограниченные возможности тиражирования научного продукта [10. С. 81]. Полагаем, что данный признак справедлив, так как любой РИД, например изобретение, отвечающее критериям патентоспособности, должно иметь определённую ценность.

Последний признак, на который следует указать, это признак правовой определённости РИД. Так как ст. 1225 ГК РФ содержит исчерпывающий перечень охраняемых правом РИД и средств индивидуализации для наделения статусом РИД, результат интеллектуального труда человека должен быть указан в ст. 1225 ГК РФ.

Относительно признака непотребляемости, на который ссылаются Л. Б. Гальперина и Л. А. Михайлов [7. С 11], стоит заметить, что данный признак непосредственно вытекает из признака нематериальности РИД, в силу чего отдельное его выделение представляется необоснованным.

Таким образом, по нашему мнению, РИД – это нематериальный результат интеллектуальной деятельности человека, выраженный в объективной форме, доступной другим участникам гражданских правоотношений, имеющий коммерческую ценность и защищаемый законодательством.

Теперь перейдём к вопросу о том, является ли ноу-хау (секрет производства) РИД, отмеченному выше как центральному вопросу данного небольшого исследования.

Для начала взглянем на определение секрета производства (ноу-хау), данное в ст. 1465 ГУ РФ. Секретом производства (ноу-хау) признаются сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.

Внимательно прочитав данное определение, можно выделить следующие признаки секрета производства:

1) секретом производства являются сведения, при этом любого характера, в том числе о РИД в научно-технической сфере, и сведения о способах осуществления профессиональной деятельности;

2) секрет производства обладает коммерческой ценностью, действительной или потенциальной;

3) в отношении сведений, составляющих секрет производства, введён режим коммерческой тайны, который обеспечивает недоступность этих сведений для третьих лиц и создаёт коммерческую ценность данных сведений.

Е. А. Кондратьева отмечает, что «результатом интеллектуальной деятельности могут быть признаны только творческие объекты интеллектуальной собственности – объекты, созданные творческим трудом автора. Исходя из этого, не могут быть отнесены к таковым секреты производства (ноу-хау)» [1. С. 18]. Подобная точка зрения содержится и в уже указанной статье Э. Гаврилова [2. С. 25].

Особо следует обратить внимание на следующие слова Е. А. Кондратьевой, сказанные в том же абзаце, в котором сделано заключение о невозможности отнести ноу-хау к РИД: «Другое дело, что у сведений, составляющих секрет производства, может быть автор либо они могут быть и не созданным автором “продуктом”». [1. С. 18]. Из данного предложения можно сделать вывод, что автор отделяет непосредственно само ноу-хау и сведения, составляющие его.

Позволим себе не согласиться с данным мнением. Полагаю, что разделение сведений, признаваемых ноу-хау, и сведений, составляющих секрет производства, не совсем корректно. Дело в том, что секрет производства отличается от других РИД дополнительным

набором признаков: секретность, недоступность третьим лицам и связанная с этим действительная или потенциальная коммерческая ценность. Становясь ноу-хау, любой РИД получает дополнительные признаки, которые отличают его от того, чем он был раньше.

Также следует обратить внимание на творческий момент в секрете производства. Согласно понятию, данному Е. А. Кондратьевой, к РИД относятся только результаты творческого труда автора. Не вдаваясь в вопрос о том, что представляет собой творчество, хочется привести пример, когда такой подход к РИД не сработает. Представим себе совокупность патентоспособных сведений об изобретении. Обладатель данных сведений, не патентуя изобретение, устанавливает режим коммерческой тайны в отношении данных сведений, превращая данные сведения в секрет производства. Согласно приведённой выше точке зрения, такое ноу-хау не может быть отнесено к РИД по причине отсутствия творческого характера. Наше же мнение заключается в том, что в данной ситуации творческий характер деятельности автора, являясь объективной характеристикой, никуда не пропал, что позволяет отнести как минимум данный секрет производства к РИД.

Скорее всего, внося ноу-хау в перечень РИД, указанный в ст. 1225 ГК РФ, законодатель подразумевал под данным ноу-хау те сведения, которые имели творческий характер. Иные же секретные сведения, обладающие коммерческой ценностью, но не обладающие творческой характеристикой, попадают в группу информации, составляющей коммерческую тайну, но не составляющую секрет производства.

Примечания

[1] Кондратьева Е. А. Объекты интеллектуальных прав: особенности правовой охраны. М.: Статут, 2014. 160 с.

[2] Гаврилов Э. Исключительные права на результаты интеллектуальной деятельности как права, связанные с личностью автора // Хозяйство и право. 2008. № 9. С. 24–29.

[3] Астахова М. А. Результаты интеллектуальной деятельности как объекта гражданских прав: понятие и квалифицирующие признаки // Юрист. 2006. № 6. // СПС Консультант-Плюс.

[4] Новосельцев О. В. Интеллектуальная собственность в системе гражданского права: проблемы правопонимания // Интеллектуальная собственность. Актуальные проблемы теории и практики: Сборник научных трудов. Т. 1 / Под ред. В. Н. Лопатина. М.: Юрайт, 2008. С. 93–108.

[5] Волынкина М. В. Концепция исключительных прав и понятие интеллектуальной собственности в гражданском праве // Журнал российского права. 2007. № 6. С. 29–35.

[6] Дозорцев В. А. Интеллектуальные права: Понятие. Система. Задачи кодификации. Сборник статей / Исслед. центр частного права. - М.: Статут, 2005. 416 с.

[7] Гальперин Л. Б., Михайлова Л. А. Интеллектуальная собственность: сущность и правовая природа / Право промышленной и интеллектуальной собственности. Новосибирск: «Наука», 1992. 167 с.

[8] Бабкин С. А. Интеллектуальная собственность в сети Интернет. М.: АО «Центр ЮрИнфоР», 2005. 215 с.

[9] Волкова Т. Условия инновационного обмена // Экономист. 2005. № 3. С. 54–60.

[10] Бирагова Р. Т. Проблемы оценки объектов интеллектуальной собственности // Общество и право. 2010. № 3. С. 79–82.

References

[1] Kondrat'eva E.A. Ob»ekty intellektual'nykh prav: osobennosti pravovoi okhrany [Objects of Intellectual Rights: Peculiarities of Legal Defense]. Moscow: Statut Publ., 2014. 160 p.

[2] Gavrilov E. Isklyuchitel'nye prava na rezul'taty intellektual'noi deyatel'nosti kak prava, svyazannye s lichnost'yu avtora [Prerogative rights on Results of Intellectual Activity as the Right Connected with the Personality of the Author]// Khozyaistvo i pravo. 2008. No. 9. p. 24-29.

[3] Astakhova M.A. Rezul'taty intellektual'noi deyatel'nosti kak ob»ekta grazhdanskikh prav: ponyatie i kvalifitsiruyushchie priznaki [Results of Intellectual Activity as an Object of Civil Rights: Notion and Classification Properties]// Yurist. 2006. No. 6. // Konsul'tant-Plyus Information System.

[4] Novosel'tsev O.V. Intellektual'naya sobstvennost' v sisteme grazhdanskogo prava: problemy pravoponimaniya [Intellectual Property in the System of Civil Rights: Issues of Legal Consciousness]// Intellektual'naya sobstvennost'. Aktual'nye problemy teorii i praktiki: Sbornik nauchnykh trudov. T. 1 [Intellectual Property. Topical Issues of Theory and Practice: Collection of Scientific Works. Volume 1] Under the Editorship of V.N. Lopatin. Yurait Publ., 2008. p. 93 - 108.

[5] Volynkina M.V. Kontseptsiya isklyuchitel'nykh prav i ponyatie intellektual'noi sobstvennosti v grazhdanskom prave [Concept of Prerogative Rights and the Notion of Intellectual Property in the System of Civil Rights] // Zhurnal rossiiskogo prava. 2007. No. 6. p. 29-35.

[6] Dozortsev V.A. Intellektual'nye prava: Ponyatie. Sistema. Zadachi kodifikatsii. Sbornik statei [Intellectual Rights: Notion. System. Tasks of Codification. Collection of Articles] / Issled. tsentr chastnogo prava [Investigation Center of Private Law]. - Moscow: Statut Publ., 2005. 416 p.

[7] Gal'perin L.B., Mikhailova L.A. Intellektual'naya sobstvennost': sushchnost' i pravovaya priroda [Intellectual Property: Essence and Legal Nature]/ Pravo promyshlennoi i intellektual'noi sobstvennosti [Right of Industrial and Intellectual Property]. Novosibirsk: «Nauka» Publ., 1992. 167 p.

[8] Babkin S.A. Intellektual'naya sobstvennost' v seti Internet [Intellectual Property in the Internet]. Moscow: AO «Tsentr YurInfoR» Publ., 2005. 215 p.

[9] Volkova T. Usloviya innovatsionnogo obmena [Conditions of Innovation Exchange]// Ekonomist. 2005. No. 3. p. 54 - 60.

[10] Biragova R.T. Problemy otsenki ob»ektov intellektual'noi sobstvennosti [Problems of Assessment of Objects of Intellectual Property]// Obshchestvo i pravo. 2010. No. 3. p. 79 - 82.

Соболев Александр Александрович, аспирант юридического факультета, Южно-Уральский государственный университет. E-mail: alas-74@yandex.ru@is74.ru

Aleksandr Aleksandrovich Sobolev, PhD Student of the faculty of Law, South Ural State University: 76, Lenin Av., Chelyabinsk, 454080, Russia. E-mail: alas-74@yandex.ru@is74.ru

ТРЕБОВАНИЯ К СТАТЬЯМ, ПРЕДСТАВЛЯЕМЫМ К ПУБЛИКАЦИИ В ЖУРНАЛЕ «ВЕСТНИК УрФО. БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ».

Редакция просит авторов при направлении статей в печать руководствоваться приведенными ниже правилами и прилагаемым образцом оформления рукописи, а также приложить к статье сведения о себе (см. Сведения об авторе).

Сведения об авторе

ФИО (полностью)	
Ученая степень	
Ученое звание	
Должность и место работы (полностью)	
Домашний адрес	
Контактные телефоны	
e-mail	
Тема статьи	
Являетесь ли аспирантом (если да, то указать дату приема в аспирантуру и научного руководителя)	

УДК
ББК

ОБРАЗЕЦ

А. А. Первый, Б. Б. Второй, В. В. Третий

НАЗВАНИЕ СТАТЬИ, ОТРАЖАЮЩЕЕ ЕЕ НАУЧНОЕ СОДЕРЖАНИЕ, ДЛИНОЙ НЕ БОЛЕЕ 12—15 СЛОВ

Аннотация набирается одним абзацем, отражает научное содержание статьи, содержит сведения о решаемой задаче, методах решения, результатах и выводах. Аннотация не содержит ссылок на рисунки, формулы, литературу и источники финансирования. Рекомендуемый объем аннотации — около 50 слов, максимальный — не более 500 знаков (включая пробелы).

Ключевые слова: список из нескольких ключевых слов или словосочетаний, которые характеризуют Вашу работу.

Рисунки

Вставляются в документ целиком (не ссылки). Рекомендуются черно-белые рисунки с разрешением от 300 до 600 dpi. Подрисуночная подпись формируется как надпись («Вставка», затем «Надпись», без линий и заливки). Надпись и рисунок затем группируются, и устанавливается режим обтекания объекта «вокруг рамки». Размер надписей на рисунках и размер подрисуночных подписей должен соответствовать шрифту Times New Roman, 8 pt, полужирный. Точка в конце подрисуночной подписи не ставится. На все рисунки в тексте должны быть ссылки.

Все разделительные линии, указатели, оси и линии на графиках и рисунках должны иметь толщину не менее 0,5 pt и черный цвет. Эти рекомендации касаются всех графических объектов и объясняются ограниченной разрешающей способностью печатного оборудования.

Формулы

Набираются со следующими установками: стиль математический (цифры, функции и текст — прямой шрифт, переменные — курсив), основной шрифт — Times New Roman 11 pt, показатели степени 71 % и 58 %. Выключенные формулы должны быть выровнены по центру. Формулы, на которые есть ссылка в тексте, необходимо пронумеровать (сплошная нумерация). Расшифровка обозначений, принятых в формуле, производится в порядке их использования в формуле. Использование букв кириллицы в формулах не рекомендуется.

Таблицы

Создавайте таблицы, используя возможности редактора MS Word или Excel. Над таблицей пишется слово «Таблица», Times New Roman, 10 pt, полужирный, затем пробел и ее номер, выравнивание по правому краю таблицы. Далее без абзацного отступа следует таблица. На все таблицы в тексте должны быть ссылки (например, табл. 1).

Примечания

Источники располагаются в порядке цитирования и оформляются по ГОСТ 7.05-2008.

Статья публикуется впервые
Подпись, дата

Структура статьи (суммарный объем статьи – не более 40 000 знаков):

1. УДК, ББК, название (не более 12–15 слов), список авторов.
2. Аннотация (не более 500 знаков, включая пробелы), список ключевых слов.
3. Основной текст работы.
4. Примечания.

Объем статьи не должен превышать 40 тыс. знаков, включая пробелы, и не может быть меньше 5 страниц. Статья набирается в текстовом редакторе Microsoft Word в формате *.rtf шрифтом Times New Roman, размером 14 пунктов, в полуторном интервале. Отступ красной строки: в тексте — 10 мм, в затекстовых примечаниях (концевых сносках) отступы и выступы строк не ставятся. Точное количество знаков можно определить через меню текстового редактора Microsoft Word (Сервис — Статистика — Учитывать все сноски).

Параметры документа: верхнее и нижнее поле — 20 мм, правое — 15 мм, левое — 30 мм.

В начале статьи помещаются: инициалы и фамилия автора (авторов), название статьи, аннотация на русском языке объемом до 50 слов, ниже отдельной строкой — ключевые слова. Инициалы и фамилия автора (авторов), название статьи, аннотация и ключевые слова должны быть переведены на английский язык.

В случае непрямого цитирования источников и литературы в начале соответствующего примечания указывается «См.:».

Цитируемая литература дается не в виде подстрочных примечаний, а общим списком в конце статьи с указанием в тексте статьи ссылки порядковой надстрочной цифрой (Формат — Шрифт — Надстрочный) (например, [1]). Запятая, точка с запятой, двоеточие и точка ставятся после знака сноски, чтобы показать, что сноска относится к слову или группе слов, например: по иску собственника[1]. Вопросительный, восклицательный знак, многоточие и кавычки ставятся перед знаком сноски, чтобы показать, что сноска относится ко всему предложению, например: …все эти положения закреплены в Федеральном законе «О ветеранах»[1].

Литература дается в порядке упоминания в статье.

При подготовке рукописи автору рекомендуется использовать ГОСТ Р 7.0.5-2008 «Система стандартов по информации, библиотечному и издательскому делу. Библиографическая ссылка. Общие требования и правила составления» (Полный текст ГОСТ Р размещен на официальном сайте Федерального агентства по техническому регулированию и метрологии).

В конце статьи должна быть надпись *«Статья публикуется впервые»,* ставится дата и авторучкой подпись автора (авторов). При пересылке статьи электронной почтой подпись автора сканируется в черно-белом режиме, сохраняется в формате *.tif или *.jpg и вставляется в документ ниже затекстовых сносок.

Обязательно для заполнения: В конце статьи (в одном файле) на русском языке помещаются сведения об авторе (авторах) — ученая степень, ученое звание, должность, кафедра, вуз; рабочий адрес, электронный адрес и контактные телефоны.

В редакцию журнала статья передается качественно по электронной почте одним файлом (название файла — фамилия автора). Тема электронного письма: Информационная безопасность.

Порядок прохождения рукописи

1. Все поступившие работы регистрируются, авторам сообщается ориентировочный срок выхода журнала, в макет которого помещена работа.

2. Поступившая работа проверяется на соответствие всем формальным требованиям и при отсутствии замечаний, в случае необходимости, направляется на дополнительную экспертизу.

3. Для публикации работы необходима положительная рецензия специалиста из данной или смежной области. На основании рецензии принимается решение об опубликовании статьи (рецензия без замечаний) или о возврате автору на доработку, в этом случае рукопись может проходить экспертизу повторно. При получении второй отрицательной рецензии на работу редакция принимает решение об отказе в публикации.

Материалы к публикации отправлять по адресу
E-mail: urvest@mail.ru в редакцию журнала «Вестник УрФО».

Или по почте по адресу:
Россия, 454080, г. Челябинск, пр. им. В. И. Ленина, 76, ЮУрГУ, Издательский центр.

ЦЕНТР ПО ЭКСПОРТНОМУ КОНТРОЛЮ ЮУрГУ

В соответствии с решением Комиссии по экспортному контролю Российской Федерации Южно-Уральский госуниверситет получил Свидетельство о специальном разрешении № 027 на осуществление деятельности по проведению независимой идентификационной экспертизы товаров и технологий в целях экспортного контроля.

В настоящее время ФГБОУ ВПО «Южно-Уральский государственный университет» (НИУ) располагает научно-педагогическим персоналом с высоким профессиональным и интеллектуальным уровнем, а также развитой лабораторной базой, это позволяет профессионально и качественно осуществлять деятельность по проведению независимой идентификационной экспертизы товаров и технологий, проводимой в целях экспортного контроля.

В соответствии с номенклатурой продукции, в отношении которой планируется осуществлять экспертизу, подобрано 107 экспертов, из них докторов наук 35, кандидатов наук 57 и 15 специалистов, не имеющих ученой степени. Все эксперты являются сотрудниками университета и способны квалифицированно и качественно провести экспертизу.

Если Вы являетесь поставщиками оборудования, машин, материалов, запасных частей и комплектующих для них, выпускаете сложную технику, научно-техническую продукцию и Вам приходится сталкиваться с терминами **«экспортный контроль»** и **«товары двойного назначения»**, то мы можем быть Вам полезны.

В соответствии с российским законодательством экспертизу товаров и технологий для целей экспортного контроля могут проводить только экспертные организации, получившие специальное разрешение Комиссии экспортного контроля Российской Федерации.

Центр по экспортному контролю ЮУрГУ осуществляет деятельность по проведению независимой идентификационной экспертизы товаров и технологий в целях экспортного контроля в отношении **продукции по всей номенклатуре действующих контрольных списков, утвержденных указами Президента Российской Федерации.**

Директор Центра:
Анатолий Григорьевич Мещеряков.
Тел. (351) 267-95-49.

Заключения нашей экспертизы действуют на всей территории России и являются официальным документом, подтверждающим принадлежность или непринадлежность объекта экспертизы к продукции, включенной в списки контролируемых товаров и технологий.

Наши услуги:

1. Оформление заключений идентификационной экспертизы для целей экспортного контроля и таможенного оформления.
2. Консультация по экспортному контролю товаров (технологии).

Перечень документов, необходимых для проведения экспертизы:

1. Заявка.
2. Контракт (договор, соглашение).
3. Спецификация (перечень поставляемой продукции) и иные приложения.
4. Техническая документация (паспорта, сертификаты качества, руководства по эксплуатации, технические описания, этикетки и пр.).
5. Доверенность.

Наши координаты

Адрес: 454080, г. Челябинск, пр. им. В. И. Ленина, 85, корпус 3А, ауд. 502.
Телефон (351) 267-95-49
E-mail: exp-174@mail.ru
Транспорт (автобус, троллейбус, маршрутное такси): остановка «ЮУрГУ»

ФИРМЕННЫЙ БЛАНК ОРГАНИЗАЦИИ

Исх. № _____
от «___» _____ 201__ г.

Директору Центра по экспортному
контролю ГОУ ВПО «ЮУрГУ»
А. Г. Мещерякову
454080, пр. им. В. И. Ленина, 85,
корпус 3А, ауд. 502

ЗАЯВКА
на проведение работ

Прошу Вас провести независимую идентификационную экспертизу товаров (технологий) в целях экспортного контроля и таможенного оформления.

Грузоотправитель: _____
_____

Грузополучатель: _____
_____

Перечень поставляемой продукции:

№ п/п	Наименование продукции	Единица измерения	Количество	Код ТН ВЭД

Оплату работ по выставлении счета гарантирую.

Уполномоченный по техническим вопросам: _____
_____

_____ _____ _____
(должность) (подпись) (Ф. И. О.)

Полезная информация

1. Экспертиза проводится в течение 3-х рабочих дней. По просьбе заказчика экспертиза может быть проведена в более короткие сроки.

2. Стоимость проведения экспертизы зависит от:

- объема рассматриваемого материала, продукции, информации, представленных согласно заявке;
- количества наименований товаров;
- количества кодов ТН ВЭД;
- сроков исполнения заявки;
- степени секретности материала, представленного на экспертизу.

3. Готовое заключение выдается на бумажном носителе (по просьбе заказчика — в электронном варианте).

4. Договор на оказание услуг заключается каждый раз в соответствии с заявкой.

Федеральные органы исполнительной власти

ФСТЭК России: http://www.fstec.ru/

РЕГИОНАЛЬНЫЙ АТТЕСТАЦИОННЫЙ ЦЕНТР ЮУрГУ

«Региональный аттестационный центр» создан на основании решения Ученого совета Южно-Уральского государственного университета от 25.06.2007 г. № 10 по согласованию с Управлением ФСБ России по Челябинской области. Основными функциями «Регионального аттестационного центра» являются:

1) всестороннее обследование предприятий-заявителей на предмет их готовности к выполнению работ, связанных с использованием сведений, составляющих государственную тайну;

2) осуществление мероприятий по оказанию услуг в данной области;

3) повышение квалификации сотрудников режимно-секретных подразделений.

Решением Межведомственной комиссии по защите государственной тайны № 95 от 06 апреля 2005 года Южно-Уральский государственный университет включен в перечень учебных заведений, осуществляющих подготовку специалистов по вопросам защиты информации, составляющей государственную тайну, свидетельство об окончании которых дает руководителям предприятий, учреждений и организаций право на освобождение от государственной аттестации.

Курсы повышения квалификации по программе «Защита информации, составляющей государственную тайну» (в зачет государственной аттестации).

Категория слушателей: руководители организаций, заместители руководителей организации, ответственные за защиту сведений, составляющих государственную тайну.

По окончании обучения слушателям выдается удостоверение государственного образца о краткосрочном повышении квалификации, которое дает право руководителям предприятий, учреждений, организаций на освобождение от государственной аттестации.

Форма обучения – очно-заочная (48 часов заочная, 24 часа – очная форма обучения).

Слушатели обеспечиваются раздаточным материалом, нормативными документами на компакт-диске, учебным пособием курса лекций.

Курсы повышения квалификации по программе «Защита информации, составляющей государственную тайну».

Категория слушателей: руководители и сотрудники структурных подразделений по защите государственной тайны.

По окончании обучения слушателям выдается удостоверение государственного образца о краткосрочном повышении квалификации.

Форма обучения – очная (72 часа). Обучение слушателей осуществляется с отрывом от производства – 2 недели.

Слушатели обеспечиваются раздаточным материалом, нормативными документами на компакт-диске.

Программа предусматривает изучение следующих дисциплин:

1) Правовое и нормативное обеспечение защиты государственной тайны;

2) Организация комплексной защиты информации в организациях;

3) Организация режима секретности в организации;

4) Организация защиты информации, обрабатываемой средствами вычислительной техники;

5) Организация защиты информации при осуществлении международного сотрудничества;

6) Допуск граждан к сведениям, составляющим государственную тайну;

7) Организация и ведение секретного делопроизводства;

8) Ответственность за нарушение законодательства РФ по защите государственной тайны. Порядок проведения служебного расследования по нарушениям.

«Региональный аттестационный центр» на договорной основе предоставляет предприятиям, учреждениям и организациям услуги в сфере защиты государственной тайны:

• оказание методической и консультационной помощи работникам режимно-секретных подразделений предприятий и организаций;

• специальное обслуживание предприятий, не имеющих в своей структуре режимно-секретных подразделений:

1) ведение допускной работы в соответствии с требованиями «Инструкции о порядке допуска должностных лиц и граждан РФ к государственной тайне», утвержденной постановлением Правительства РФ от 06 февраля 2010 г. № 63;

2) выделение для проведения секретных работ помещений, соответствующих требованиям Инструкции по обеспечению режима секретности в Российской Федерации, утвержденной постановлением Правительства РФ от 05.01.2004 № 3-1 (далее – Инструкция № 3-1-04 г.);

3) выделение для хранения секретных документов помещений, соответствующих требованиям Инструкции № 3-1-04 г.;

4) организация и ведение секретного делопроизводства в соответствии с общими нормативными требованиями Инструкции № 3-1-04 г.;

5) обеспечение защиты государственной тайны при обработке и хранении секретной информации на средствах вычислительной техники и (или) в автоматизированных системах;

6) подготовка Заключения о фактической осведомленности работников в сведениях, составляющих государственную тайну;

7) разработка нормативно-методической документации по вопросам защиты государственной тайны;

8) профессиональная подготовка и обучение работников Заказчика, допущенных к работам с носителями секретной информации;

9) осуществление мероприятий по подготовке к проведению специальной экспертизы Заказчика на предмет получения и продления лицензии на право работ с использованием сведений, составляющих государственную тайну, а также к проведению государственной аттестации его руководителя, ответственного за защиту сведений, составляющих государственную тайну.

Контактные адреса и телефоны:

Юридический адрес: 454080, г. Челябинск, пр. им. В. И. Ленина, д. 76
Фактический адрес: г. Челябинск, пр. им. В. И. Ленина, д. 85, ауд. 512/3
Телефоны: (351) 267-91-55, 267-93-14, 267-92-85
E-mail: rac512@mail.ru

РЕГИОНАЛЬНЫЙ УЧЕБНО-НАУЧНЫЙ ЦЕНТР «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» ЮУрГУ (РУНЦ ИБ ЮУрГУ)

Региональный учебно-научный центр «Информационная безопасность» ЮУрГУ создан при кафедре «Безопасность информационных систем» приборостроительного (компьютерных технологий, управления и радиоэлектроники) факультета во исполнение Приказа Министерства образования и науки Российской Федерации от 9 марта 2005 года № 126 «Об утверждении Перечня региональных учебно-научных центров по проблемам информационной безопасности в системе высшей школы на базе государственных образовательных учреждений высшего профессионального образования, находящихся в ведении Федерального агентства по образованию».

Центр осуществляет повышение квалификации и переподготовку кадров по проблемам информационной безопасности по следующим программам:

1. Программа профессиональной переподготовки «Комплексные системы обеспечения информационной безопасности в организациях» (504 часа).

По окончании программы выдается Диплом о профессиональной переподготовке. Потребность в обучении по данной программе обусловлена требованиями Постановления Правительства Российской Федерации от 16 апреля 2012 г. № 313 г. «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)». Центр предлагает пройти обучение по данной программе руководителей и инженерно-технических специалистов подразделений обеспечения информационной безопасности (защиты информации) предприятий, организаций и учреждений.

Обучение в РУНЦ ИБ ЮУРГУ ведется по модульному принципу с использованием дистанционных технологий. Слушателям программы профессиональной переподготовки на выбор предлагается 7 из 10 модулей объемом по 72 часа:

КПП-01. Организация и управление системой информационной безопасности организации.

КПП-02. Криптографическая и программно-аппаратная защита информации.

КПП-03. Инженерно-техническая защита информации.

КПП-04. Обеспечение безопасности персональных данных при их обработке в ин-

формационных системах персональных данных.

КПП-05. Расследование инцидентов информационной безопасности.

КПП-06. Документирование защиты информации и организация конфиденциального документооборота.

КПП-07. Защита коммерческой тайны.

КПП-08. Кадровая безопасность.

КПП-09. Культура информационной безопасности.

КПП-10. Криптографическая защита информации.

2. Программы повышения квалификации (72 часа). По окончании программ выдается Удостоверение о повышении квалификации.

2.1. «Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных». Главная цель курса заключается в том, чтобы помочь специалистам различных категорий – от руководителей предприятий и их структурных подразделений до лиц, ответственных за организацию обработки персональных данных, – обеспечить работу с персональными данными в соответствии с требованиями российских законов и с учетом последних изменений в законодательстве. В рамках курса изучается весь комплекс мероприятий по обеспечению правомерности обработки персональных данных с использованием правовых, организационных и технических мер, способы снижения рисков утечки персональных данных и наложения штрафных санкций со стороны государственных надзорных органов.

2.2. «Защита коммерческой тайны». В курсе изучаются особенности российского законодательного регулирования вопросов защиты исключительных прав на секреты производства, закрепленные в Федеральном законе от 29.07.2004 г. № 98-ФЗ «О коммерческой тайне» и в других нормативных актах, а также технологии установления и поддержания режима коммерческой тайны в организации. Особое внимание уделяется формированию перечня сведений, составляющих коммерческую тайну, разработке и вводу в действие внутренних нормативных документов предприятия, регулированию трудовых отношений, связанных с доступом к коммерческой тайне, процедуре заключения лицензионных договоров, договоров об отчуждении исключительных прав на секреты производства и коммерческой концессии, особенностям представления информации о коммерческой тайне в органы власти, порядку проведения совещаний с контрагентами, на которых раскрывается коммерческая тайна, способам минимизации рисков, вызванных угрозами конфиденциальным сведениям.

2.3. «Расследование компьютерных инцидентов». В курсе изучаются все аспекты деятельности службы безопасности (отдела информационной безопасности) организации при реагировании на инциденты в информационной системе, в том числе методика предупреждения таких инцидентов, ликвидации нанесенного ими ущерба, пресечения хакерской активности, перекрытия каналов незаконного съема информации и выявления виновных лиц. Слушатели изучают методики анализа рисков и уязвимостей безопасности информационных систем организации, основные способы обеспечения непрерывности функционирования информационной системы в случае возникновения компьютерных инцидентов и скорейшего устранения их последствий. В завершение курса слушатели самостоятельно проводят полный цикл расследования компьютерных инцидентов с составлением необходимых документов.

2.4. «Документирование защиты информации и организация конфиденциального делопроизводства». Цель курса – подготовка слушателей к проведению комплекса мероприятий по защите информации в организации с учетом требований нормативно-правовых документов, регламентирующих защиту информации в организации, в том числе – информации ограниченного доступа и ведения конфиденциального делопроизводства. Особое внимание уделяется практическим аспектам реализации всего процесса конфиденциального делопроизводства – от составления перечня информации ограниченного доступа до особенностей электронного конфиденциального документооборота, использования электронной цифровой подписи. Детально рассматриваются обязанности сотрудников, организующих, осуществляющих и контролирующих конфиденциальное делопроизводство. Специалисты, обучающиеся на курсе, получают практические знания и навыки, позволяющие создать или усовершенствовать существующую систему конфиденциального делопроизвод-

ства на предприятиях и в организациях любой формы собственности и отраслевой принадлежности.

2.5. «Культура информационной безопасности». Актуальность программы обусловлена, во-первых, технологизацией образовательного процесса, а следовательно, возрастающими требованиями к развитию компьютерной грамотности руководителя, учителя, специалиста муниципальных образовательных учреждений, во-вторых, существующими тенденциями современного информационного общества, которые повышают зависимость безопасности общества, каждого конкретного человека от качества информационной инфраструктуры, достоверности, целостности используемой информации, ее защищенности от несанкционированной модификации. Обучение направлено на формирование навыков работы с офисными программами и Интернетом, изучение основ защиты информации, а также развитие компетенций в области обеспечения личной информационно-психологической безопасности и защиты детей, подрастающего поколения от негативных информационных воздействий (агрессии, экстремизма, деструктивных организаций, зависимости от информационного шума, сообществ в социальных сетях, провоцирующих суицидальное поведение, и пр.). Программа рассчитана на специалистов образовательных учреждений.

Слушателям предлагаются также курсы повышения квалификации по программам «Программно-аппаратная защита информации», «Криптографическая защита информации», «Инженерно-техническая защита информации» и др.

Кроме образовательной деятельности, Центр активно ведет научные и хоздоговорные исследования по актуальным проблемам защиты информации.

Контактная информация:
Адрес: 454080, Челябинск, пр. Ленина, 84, ауд. 513/3а.
Тел.: 8 (351) 267-99-24, 267-93-77
E-mail: runc-ib@mail.ru
Сайт: http://runc-ib.susu.ac.ru/

Contact information:
Address: Office 513/3a, 84 Lenina Str., Chelyabinsk, 454080,
tel.: 8(351) 267-99-24, 267-93-77
E-mail: runc-ib@mail.ru
http://runc-ib.susu.ac.ru/

ВЕСТНИК УрФО
Безопасность в информационной сфере № 2(12) / 2014

Дата выхода в свет 30.06.2014. Формат 70×108 1/16. Печать трафаретная.
Усл.-печ. л. 5,60. Тираж 300 экз. Заказ 368/522.
Цена свободная.

Отпечатано в типографии Издательского центра ЮУрГУ.
454080, г. Челябинск, пр. им. В. И. Ленина, 76.

Bulletin of the Ural Federal District
Security in the Sphere of Information No. 1(11)/2014

Date of publication of the 30.06.2014. Format 70X108 1/16. Screen printing.
Conventional printed sheet 5,60. Circulation - 300 issues. Order 368/522. Open price.

Printed in the printing house of the Publishing Center of SUSU.
76, Lenina Str., Chelyabinsk, 454080