ISSN 2225-5435

Вестник УрФО

БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ

№ 2(20) / 2016

Журнал «Вестник УрФО. Безопасность в информационной сфере» включен в Перечень рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени доктора и кандидата наук

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) 267-97-01.

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

В НОМЕРЕ

ТЕХНИЧЕСКИЕ СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

МАТЕМАТИЧЕСКИЕ МЕТОДЫ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ

TECHNICAL MEANS AND METHODS OF INFORMATION PROTECTION

COMPUTER SECURITY

MATHEMATICAL METHODS IN INFORMATION SECURITY

LEGAL REGULATION OF INFORMATION SECURITY

УДК 621.391.822 Вестник УрФО № 2(20) / 2016, стр. 4–10

Хорев А. А., Быков А. И., Соколов А. Н.

ПРОЕКТИРОВАНИЕ И ИССЛЕДОВАНИЕ ХАРАКТЕРИСТИК АНАЛОГОВОГО ГЕНЕРАТОРА АКУСТИЧЕСКИХ ПОМЕХ

В работе предложена схема аналогового генератора шума системы виброакустической маскировки, спроектированная при помощи программного средства моделирования электронных схем NI Multisim, и методика исследования его основных характеристик. Описаны требования, предъявляемые к генераторам шума систем виброакустической защиты. Сформулированы основные задачи при моделировании устройства виброакустической защиты. Представлена структурная схема аналогового генератора шума, принципиальные схемы ее элементов, осциллограммы и спектры сигналов в контрольных точках. Исследованы помеховые качества шумового сигнала и степень его приближения к идеальному "белому" шуму. Показано, что спроектированный генератор шума полностью отвечает предъявляемым требованиям, а полученные результаты могут быть использованы при проведении лабораторных работ по курсу «Техническая защита информации».

Ключевые слова: *технический канал утечки информации; перехват акустической информации; система виброакутической защиты; аналоговый генератор шумам.*

Horev A. A., Bykov A. I., Sokolov A. N.

DESIGN AND RESEARCH OF CHARACTERISTICS OF THE ANALOG ACOUSTIC NOISE GENERATOR

In operation is offered the diagram of the analog noise generator of system of vibroacoustic masking designed by means of a software of simulation of the electronic circuits NI Multisim and a technique of research of its main characteristics. Described requirements

for noise generators of vibro-acoustic security systems. Formulated main tasks in the simulation of vibro-acoustic security device. Presented block diagram of an analog noise generator, concepts of its elements, oscillograms and spectra of signals at control points. Researched interfering features of noise signal and the degree of its approximation to the ideal "white" noise. It is shown that the designed noise generator fully meets the requirements, and the obtained results can be used in laboratory works on the course "Technical protection of information".

Keywords: technical channel of information leakage; interception of acoustic information; system of vibroacoustic protection, analog generator to noise

I. ВВЕДЕНИЕ

Для защиты акустической (речевой) информации от утечки по техническим каналам широко используются системы виброакустической маскировки, построенные на основе аналоговых генераторов шума [1]. Целью работы являлось проектирование аналогового генератора шума с использованием программного средства разработки и моделирования электронных схем National Instruments Multisim и разработка методики исследования его основных характеристик.

II. ОСНОВНАЯ ЧАСТЬ

Для защиты речевой информации от утечки по прямому акустическому, акустовибрационному и акустооптическому каналам используются средства виброакустической защиты, которые создают вибрационные и акустические шумы в помещении [2]. Типовая система виброакустической защиты состоит из блока генерации шума и излучателей. Наиболее важным является моделирование генератора шума.

К генераторам шума систем виброакустической защиты предъявляются следующие требования [3]:

• шумовой сигнал должен генерироваться в семи октавных полосах речевого диапазона со среднегеометрическими частотами 125, 250, 500, 1000, 2000, 4000, 8000 Гц;

• коэффициент качества шума должен быть не меньше 0,6;

• должна быть предусмотрена возможность регулировки уровня сигнала в каждой октавной полосе.

Основными задачами при моделировании устройства виброакустической защиты являлись:

• выбор структурной схемы аналогового генератора шума;

• выбор элементной базы, которая будет использована в схеме устройства;

• моделирование принципиальной схемы устройства в среде Multisim 11;

• исследование осциллограмм и спектров шумового сигнала.

Структурная схема аналогового генератора шума с выходом на акустический излучатель с входным сопротивлением 4 Ом представлена на рис. 1.

Рассмотрим принципиальную схему генератора.

Источник шума Q2, представленный на рис. 2, выполнен на транзисторе BC548A и использует шумы эмиттерного перехода тран-

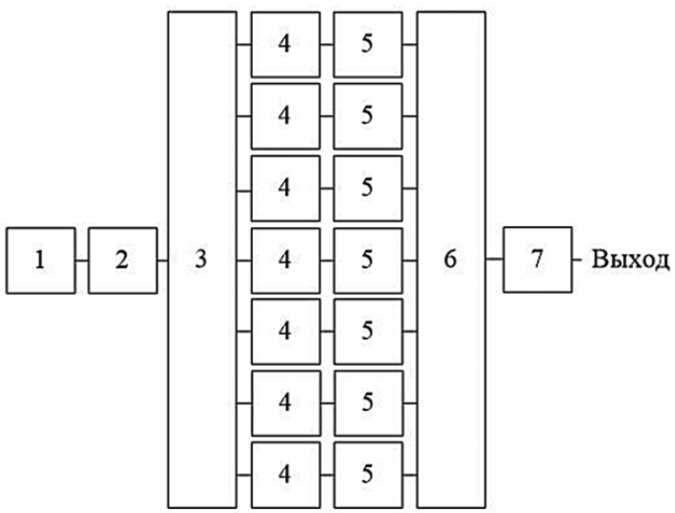

Рис.1. Структурная схема аналогового генератора шума:
1 – источник шума; 2 – усилитель; 3 – делитель; 4 – октавные фильтры;
5 – усилители октавных полос; 6 – сумматор; 7 – усилитель.

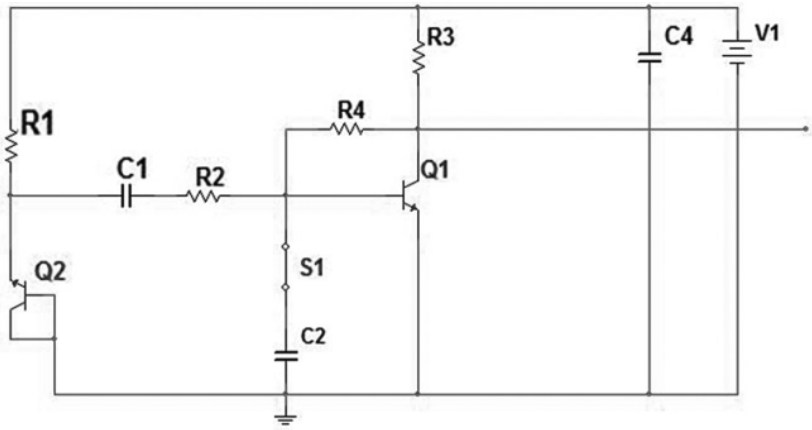

Рис. 2 Принципиальная схема источника аналогового шума

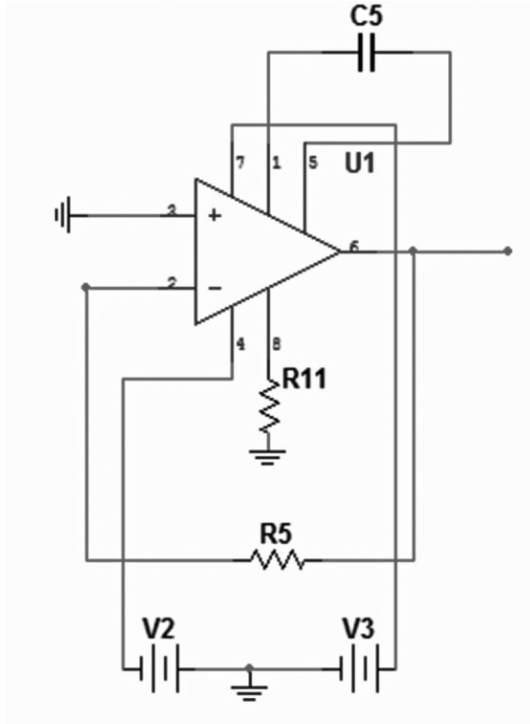

Рис. 3 Принципиальная схема операционного усилителя

зистора. Генерируемый сигнал является аналоговым хаотическим, как по частоте, так и по амплитуде.

Для достижения необходимой мощности сигнал усиливается каскадами на другом транзисторе BC548A и на усилителях CA3130E и TDA2030. Для работы операционного усилителя CA3130E требуется двуполярное питание 15В. Усилитель TDA2030 поднимает уровень шумового сигнала до необходимой величины напряжения, равной 10В. Подбор этой величины осуществляется регулиров-

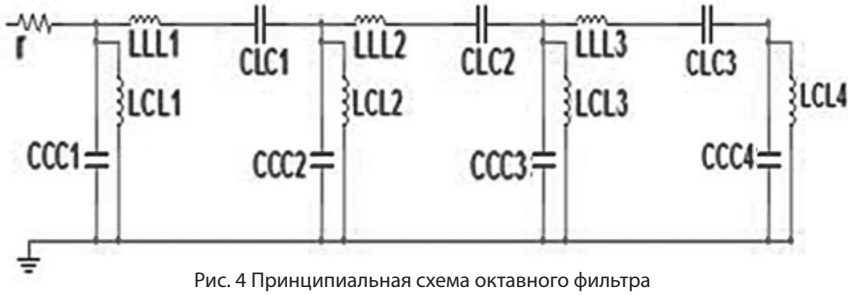

Рис. 4 Принципиальная схема октавного фильтра

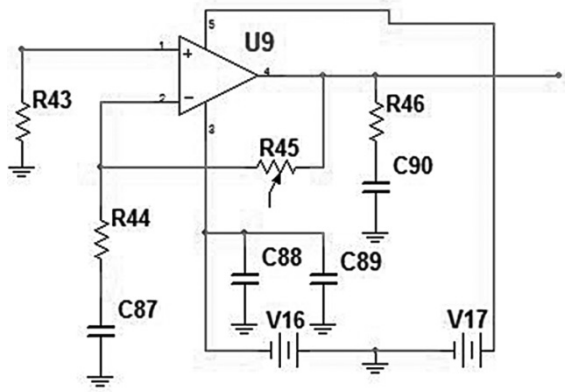

Рис. 5 Принципиальная схема усилителя октавных полос

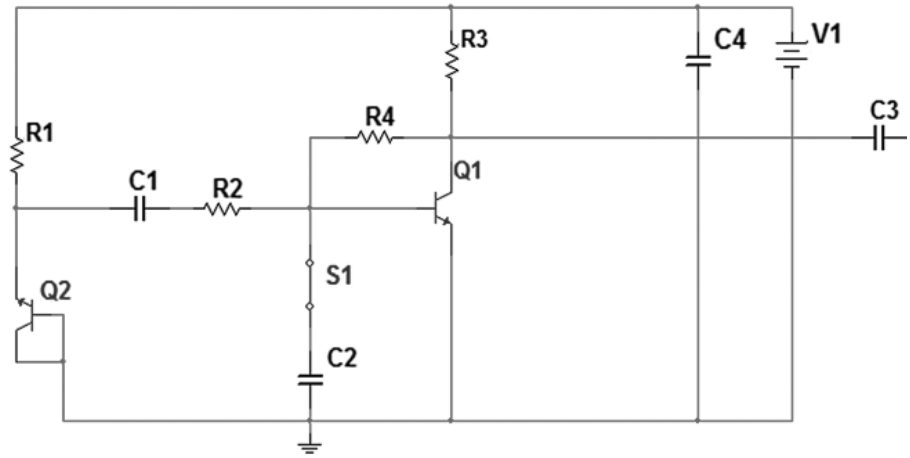

Рис. 6 Схема подключения осциллографа при измерении сигнала на выходе транзистора BC548A

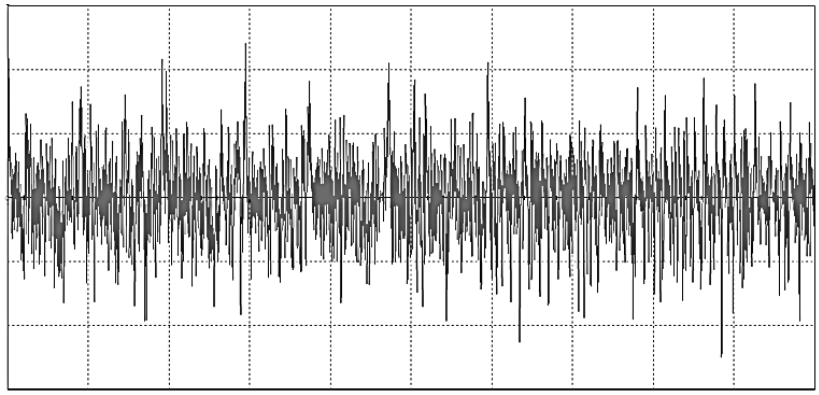

Рис. 7 Осциллограмма сигнала на выходе транзистора BC548A после усиления на каскаде с общим эмиттером

кой соотношения сопротивлений по формуле для инвертирующего операционного усилителя [4]. Принципиальная схема используемого операционного усилителя приведена на рис. 3.

Устройство производит фильтрацию по октавным полосам и усиление отфильтрованных сигналов по отдельности. Усиление производится операционным усилителем TDA2030, имеющий отечественный аналог К174УН19. Для работы операционного усилителя требуется двуполярное питание с напряжением в 15В. Также для его нормальной работы необходим радиатор, размеры которого зависят от получаемой с него выходной мощности. На рис. 4 представлен фрагмент типовой схемы октавного фильтра. На рис. 5 представлена схема используемого усилителя.

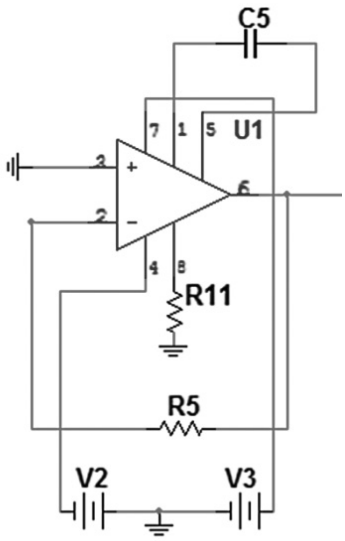

Рис. 8 Схема подключения осциллографа и анализатора спектра при измерении сигнала после операционного усилителя TDA2030

Стоит заметить, что благодаря наличию потенциометра в схеме усилителя возможна регулировка шумового сигнала для каждой октавной полосы.

Рассмотрим сигналы, получаемые в различных блоках устройств. Подключим осциллограф к источнику шума. Схема подключения представлена на рис. 6, показания прибора представлены на рис. 7.

Исследуем сигналы на выходе различных блоков устройства.

Подключим осциллограф к источнику шума по схеме, представленной на рис. 6. Осциллограмма сигнал на выходе усилителя представлена на рис. 7.

Далее сигнал усиливается на паре усилителей. На рис. 8 показана схема подключения измерительных приборов, а на рис. 9 и 10 представлены осциллограмма и спектр сигнала.

После блока усиления производится разделение сигнала на октавные полосы полосовыми фильтрами и усиление в пределах октавных полос. Схема подключения приборов пред-

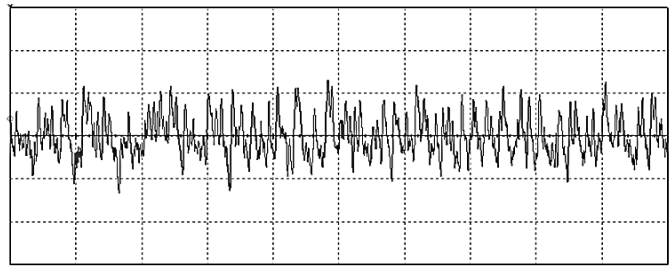

Рис. 9 Шумовой сигнал после операционного усилителя TDA2030

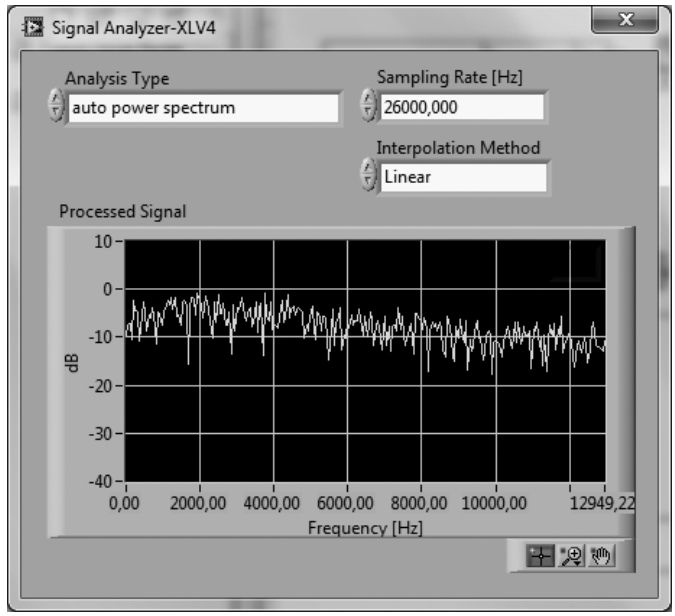

Рис. 10 Спектр сигнала на выходе операционного усилителя TDA2030

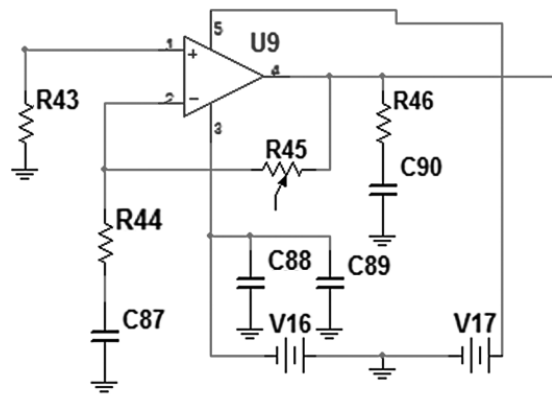

Рис. 11 Схема подключения осциллографа и анализатора спектра при измерении сигнала после полосовых фильтров

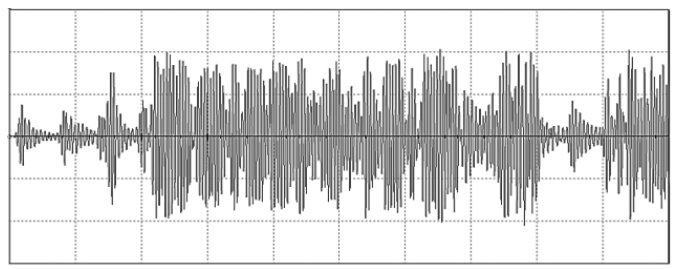

Рис. 12 Осциллограмма сигнала после полосового фильтра

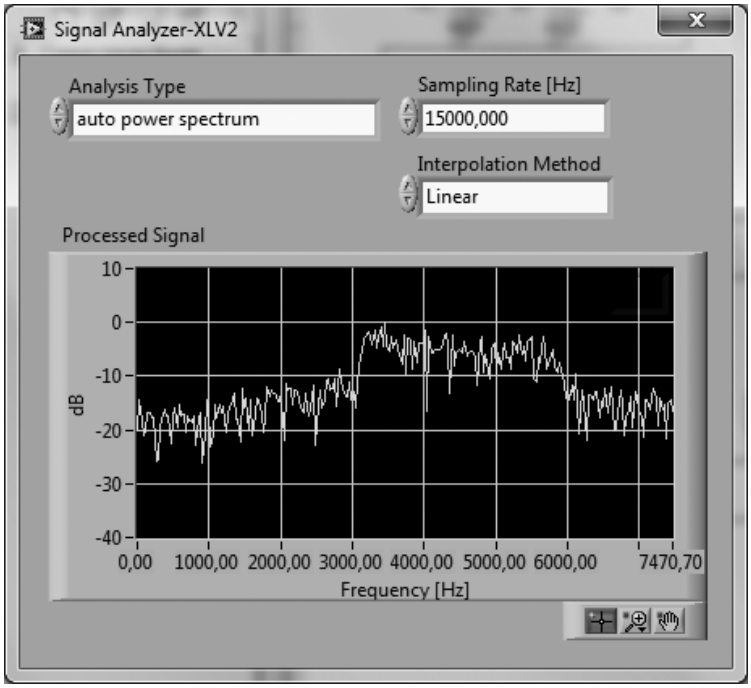

Рис.13 Спектр сигнала после полосового фильтра

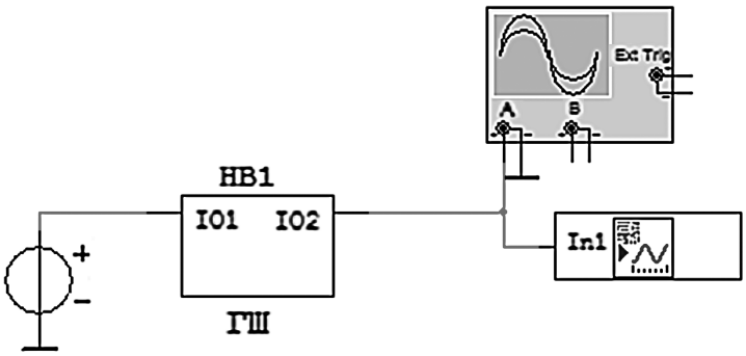

Рис. 14 Схема подключения осциллографа и анализатора спектра при измерении сигнала, генерируемого устройством

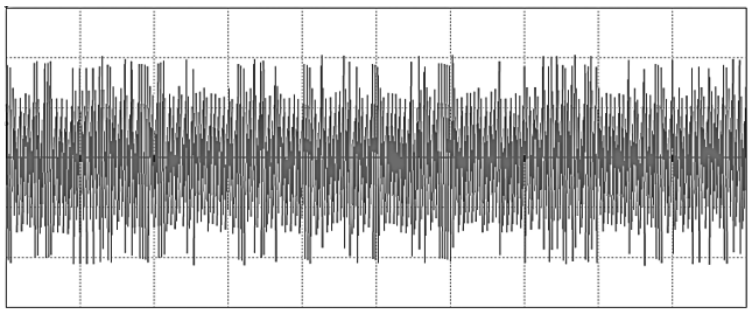

Рис. 15 Осциллограмма сигнала, генерируемого устройством

ставлена на рис. 11. Вид сигнала и его спектр после одного из полосовых октавных фильтров и операционных усилителей (для примера взята шестая октава) представлены на рис.12 и 13.

После объединения усиленных для каждой октавной полосы сигналов получим модель для проведения исследований. Схема подключения измерительных приборов представлена на рис. 14, а полученные осциллограмма и спектр – на рис. 15 и 16.

Для оценки помехового качества шумового сигнала рассчитывался показатель энтропийного коэффициента качества шума. Энтропийный коэффициент качества шума характеризует приближение к идеальному «белому» шуму. Для получения значения коэффициента качества шума была использована программа, разработанная в среде математического моделирования Matlab. Полученные результаты показали, что коэффициент качества шума, получаемого устройством, равно 0,8497, что удовлетворяет требованиям, предъявляемым к генератору шума.

Таким образом, проведенные исследования показали, что спроектированный генератор шума полностью отвечает требованиям, предъявляемым к генераторам шума систем виброакустической маскировки.

Разработанные в среде National Instruments Multisim схема генератора

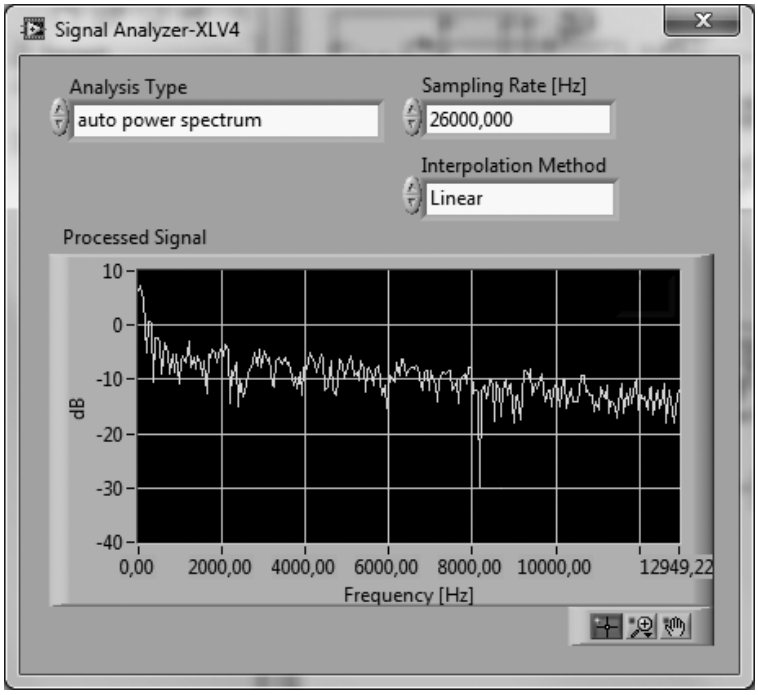

Рис. 16 Спектр сигнала, генерируемого устройством

шума и методика исследования его характеристик может быть использована при проведении лабораторных работ по курсу «Техническая защита информации» для студентов, обучающихся по направлению «Информационная безопасность».

Примечания

1. Антясов И.С., Сафонов А.В., Соколов А.Н. Защита информации в помещении от утечки по техническим каналам //Вестник УрФО. Безопасность в информационной сфере. – Челябинск: Изд. центр ЮУрГУ, 2015. – № 3(17) – С. 12 – 16.

2. Железняк В.К., Макаров Ю.К., Хорев А.А. Некоторые методические подходы к оценке эффективности защиты речевой информации // Специальная техника. — М.: 2000. — №4. — с. 39–45.

3. Хорев А.А. Техническая защита информации: учебное пособие: В 3-х т. т. 1: Технические каналы утечки информации / А. А. Хорев. — М.: НПЦ «Аналитика», 2008. — 436 с.

4. Акустический генератор «белого шума». [Электронный ресурс]. – Режим доступа:http://www.qrz.ru/schemes/contribute/security/jammers/generator2.shtml.

ХОРЕВ Анатолий Анатольевич, доктор технических наук., профессор, зав. кафедрой информационной безопасности Национального исследовательского университета «Московский институт электронной техники», г. Зеленоград, г. Москва. E-mail: horev@miee.ru

БЫКОВ Андрей Игоревич, магистрант кафедры информационной безопасности Национального исследовательского университета «Московский институт электронной техники», г. Зеленоград, г. Москва. E-mail: mr.aibykov@gmail.com

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

Anatoly Horev, Doctor of Technical Sciences, Professor, Head. the Department of Information Security National Research University of Electronic Technology, Zelenograd, Moscow. E-mail: horev@miee.ru

Andrei Bykov, Graduate Student of the Department of Information Security National Research University of Electronic Technology, Zelenograd, Moscow. E-mail: mr.aibykov@gmail.com

Alexander Sokolov, a. M. N., Associate Professor, Head. the Department of Information Systems Security "South Ural State University", Chelyabinsk. E-mail: ANSokolov@inbox.ru

УДК 004.7 Вестник УрФО № 2(20) / 2016, стр. 11–14

Куц Д. В., Третьяк Н. В.

ОСОБЕННОСТИ ВОССТАНОВЛЕНИЯ ДАННЫХ В ФАЙЛОВОЙ СИСТЕМЕ FAT 32

В данной статье рассматриваются вопросы восстановления удалённых файлов в файловой системе FAT 32. В силу особенностей файловой системы, большинство утилит для восстановления данных, не в полной мере справляются со своей задачей. Анализируются основные недостатки утилит и предлагается алгоритм восстановления, который при необходимости позволяет восстанавливать файлы вручную, а также в последующем может лечь в основу программы. Файловая система FAT 32 в течении еще некоторое время будет сохранять актуальность, и как следствие необходимо проводить исследования в области поиска оптимальных путей восстановления данных и создавать на их основе программные продукты. Разработанная методика может помочь в первую очередь для восстановления одиночных удалённых файлов.

Ключевые слова: *файловая система FAT32, восстановление данных, сигнатурный анализ, байт, сектор, кластер, алгоритм.*

Kuts D. V.., Tretiak N.V.

CHARACTERISTICS OF DATA RECOVERY IN FAT32 FILE SYSTEM

This article describes questions related to recovery of deleted files in FAT 32 file system. Most of utilities for data recovery cannot fully manage this kind of tasks because of characteristics of the file system. The second part of the article is dedicated to the analysis of the most common errors of the utilities and advises an effective algorithm of recovery, which allows to restore files manually if needed, and can lay the basis for a future program as well.

FAT 32 file system will remain actual for some time period, and therefore it's necessary to conduct researches aimed on exploration of the optimal ways of data recovery and create software products based on them. This technique, in the first place, can be of a great help in recovery of single deleted files.

Keywords: *FAT 32 file system, data recovery, signature analysis, bite, cluster, sector, algorithm.*

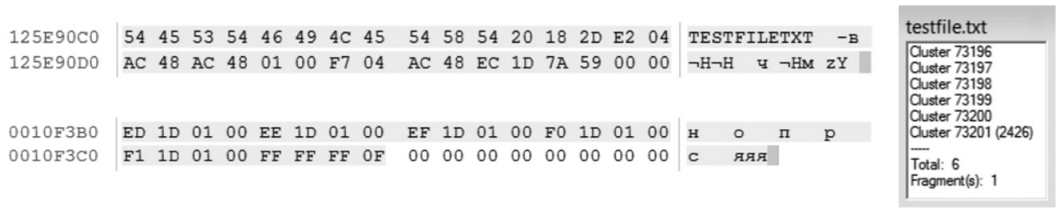

Рис. 1. Файловая запись в каталоге,цепочка кластеров (в таблице FAT и списком)

Файловая система FAT32 через несколько месяцев отметит свое 20-летие, а семейству FAT в целом уже 40 лет. Однако, несмотря на столь солидный возраст, FAT32 прежнему актуальна и используется на многих носителях. Причин этому несколько. Самые основные – высокое быстродействие, простота реализации поддержки на аппаратных устройствах, низкое ресурсопотребление[1]. Однако быстродействие не бывает бесплатным. В этой файловой системе отсутствует журналируемость, поддержка прав доступа. Также, жизненно важные структуры дублируются лишь отчасти.

Существует ряд серьёзных проблем, связанных с восстановлением данных в этой файловой системе. Большинство проблем связаны с самой концепцией таблицы размещения файлов FAT. Она отслеживает свободное дисковое пространство и отображает размещение содержимого файлов на диске посредством цепочек кластеров [2]. Пример файловой записи и цепочки кластеров приведены на рис. 1.

При удалении файла цепочка кластеров обнуляется, т.е. содержимое всех ячеек таблицы, относящихся к данному файлу, заполняется нулями. После этого, в случае, если файл был фрагментирован, можно только угадывать, в каких кластерах находится содержимое файла. С уверенностью можно сказать лишь о первом кластере файла, поскольку его номер хранится не в таблице FAT, а в файловой записи в каталоге и не стирается. Однако во многих случаях и эта уверенность оказывается обманчивой. Дело в том, что адрес первого кластера, в котором хранится содержимое файла состоит из двух половинок по 2 байта. При удалении файла два старших байта адреса также заполняются нулями[2]. Пример файловой записи до удаления с выделенными старшими и младшими байтами, и файловой записи удаленного файла приведен ниже (см. рис. 2, 3).

В случае, если эти два байта адреса хранили нули, т.е. в файл начинался в кластере с номером не более 65535, то адрес первого кластера при удалении не меняется. В этом случае информацию файловой записи можно использовать для восстановления файла, что существенно облегчает задачу. Однако, при стандартном размере кластера в 4Кб это бывает возможным только дляфайлов, хранившихся в первых 256 МБ памяти носителя. В остальных же случаях информация в файловой записи скорее сбивает с толку программу восстановления данных, нежели помогает ей.

Программы восстановления удалённых файлов с файловых систем FAT в основном используютдва алгоритма. Это восстановление на основании данных файловой записи и поиск по сигнатурам некоторых типов файлов в области данных, а также комбинированные алгоритмы на основе первых двух методов. Однако во многих случаях, полностью восстановить данные не удаётся. Наибольшей эффективностью пользуются комбинированные алгоритмы, однако данные, полученные из файловой записи в каталоге не всегда бывают надёжны. В большинстве случаев, при удалении файла адрес первого кластера содержит неправильное значение. Т.е. начало файла потеряно. В этих случаях применим только

Рис. 2. Рамками выделены 2 старших байта по смещению 0x14 и 2 младших по смещению 0x1A

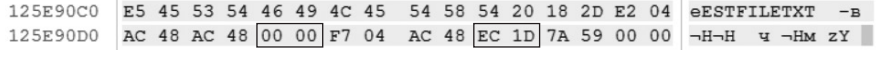

Рис. 3. Рамками выделены 2 старших байта по смещению 0x14
и 2 младших по смещению 0x1A – 2 старших байта обнулились.

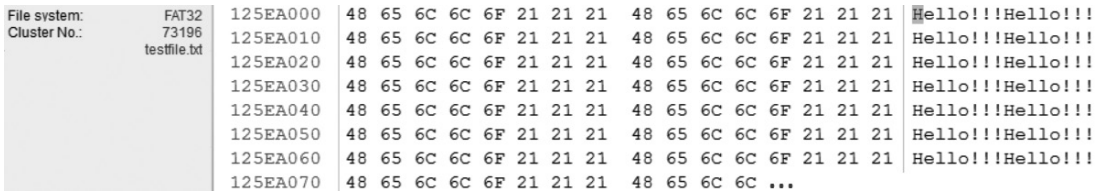

Рис. 4. Так выглядел файл до удаления и последующего восстановления

Рис. 5. Результат попытки восстановления программой

сигнатурный анализ. В некоторых случаях можно обойтись без информации в файловой записи [3]. Например для файлов *.tiff , *.zip, *.avi, *.psd, *.pst, *.jpeg, *.rar, и некоторых других мы можем определить размер файла из заголовка. Но мы не можем восстановить название файла, временные отметки, не можем определить точный размер для других типов файлов.

Мы провели тестирование нескольких наиболее популярных утилит для восстановления удалённых файлов с искажённым адресом первого кластера.

Исходя из результатов тестов, мы убедились, что в случае, если при удалении файла обнуляются первые два байта адреса первого кластера, ни одна программа не восстанавливает файл (см. рис. 4, 5). Вместо этого, она обращается в кластер области данных, на который указывает изменённый адрес в файловой записи и восстанавливает в файл содержимое этого кластера и последующие кластеры, исходя из размера файла. Т.е. в случае восстановления удалённых файлов по файловой записи, программы не проверяют содержимое кластеров и восстанавливают содержимое, не имеющее никакого отношения к исходному. Однако все программы восстановили практически все файлы (не фрагментированные), где в файловых записях мы вручную восстановили адрес первого кластера, после удаления.

Для восстановления файлов, без использования данных файловой записи, программы предлагают сигнатурный анализ, но он имеет ряд недостатков. Во-первых, используя покластерное сканирование логического диска, мы не используем файловую запись и теряем такие важные метаданные, как имя файла, размер файла. У многих типов файлов размер не прописан в заголовке и определить, где заканчивается данный файл довольно затруднительно. Кроме того, даже, если файл восстановлен корректно, бывает довольно трудно пользователю найти его в огромном количестве восстановленных файлов.

Мы в своей работе предлагаем алгоритм (см. рис. 6.) восстановления удалённых файлов, который легко реализовать программно, тем самым значительно повысив успех восстановления файлов, которые начинаются на определённую сигнатуру. Их список довольно обширен. Этот алгоритм будет удобен, если вы пытаетесь восстановить удалённый файл по данным файловой записи, которую вы обнаружили в каталоге. Программу, реализующую этот алгоритм, можно использовать, как отдельный инструмент для поиска данных и правки адреса первого кластера в файловой записи, или же встроить реализацию алгоритма в уже существующие средства восстановления данных, что нам кажется наиболее эффективным. Также возможно использовать этот алгоритм в «ручном» режиме, используя HEX редактор.

1. Проверяем адрес первого кластера в файловой записи. Если в старших байтах нули, например, получается адрес 0x00001DEC, то обращаемся в кластер 0x00001DEC и проверяем наличие сигнатуры, соответствующей типу восстанавливаемого файла. Если она есть, пытаемся восстановить файл. Просим пользователя проверить, корректно ли восстановлен файл. Если нет, переходим в пункт 2.

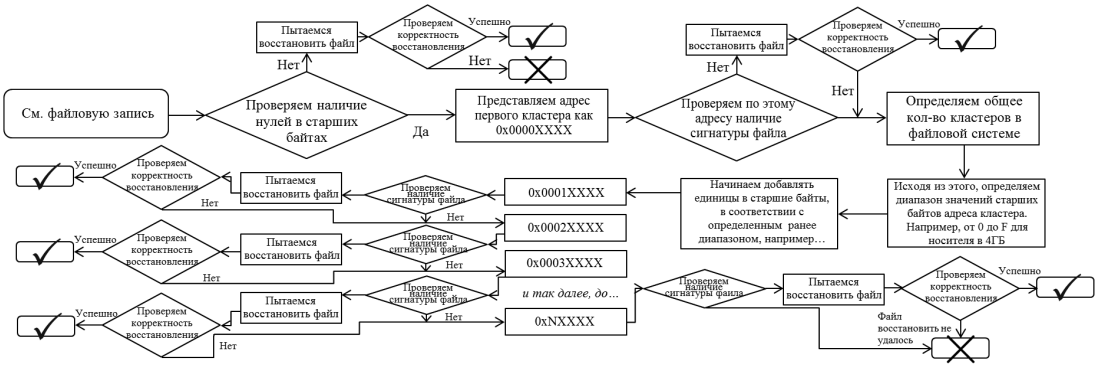

Рис. 8 Алгоритм восстановления удаленных данных

2. Определяем общее количество кластеров в файловой системе. Исходя из этого определяем максимально возможное значение старших байтов адреса кластера. Например, для флэш накопителя емкостью 4 ГБ с кластером 4 Кб получается количество кластеров примерно около 1 млн. В шестнадцатиричной системе это число 0xF4240. Т.е. в старших байтах д.б. число от 0 до F. Т.е. всего 16 возможных комбинаций. Для диска в 8 Гб это 32 комбинации и пр.

3. Осуществляем поиск нужных данных, обращаясь последовательно в кластеры с адресами 0x00001DEC, 0x00002DEC, 0x00003DEC и пр. В случае обнаружения нужной сигнатуры делаем предположение, что обнаруженные данные и есть содержимое файла и восстанавливаем его на другой диск, затем продолжаем поиск. В результате у нас получается несколько вариантов восстановленного файла, один из которых, весьма вероятно, окажется тем самым.

Для дисков большого объема алгоритм не очень удобен, однако количество возможных вариантов восстановленного файла совсем не обязательно будет большим, т.к. наличие искомой сигнатуры в начале свободного кластера с нужным номером, но с чужими данными – вопрос случайности. Кроме того, мы отсеиваем кластеры, помеченные как занятые в файловой системе.

Примечания

1. Мюллер Скотт. Модернизация и ремонт ПК. 19-е изд. М.: издательство Вильямс, 2011. 1072 с.
2. КэрриэБрайан. Криминалистический анализ файловых систем. СПб.: Питер, 2007.480 с.
3. Леонов В. Восстановление данных. М.:Эксмо, 2009.304 с.

Куц Дмитрий Владимирович, старший преподаватель кафедры теоретических основ радиотехники, Института радиоэлектроники и информационных технологий – РтФ, Уральский федеральный университет имени первого Президента России Б.Н.Ельцина. 620002, г. Екатеринбург, ул. Мира, 19. E-mail: d.v.kutc@urfu.ru

Третьяк Наталия Вадимовна, магистрант кафедры управления общественными отношениями Института государственного управления и предпринимательства, Уральский федеральный университет имени первого Президента России Б.Н.Ельцина. 620002, г. Екатеринбург, ул. Мира, 19. E-mail: n.v.tretiak@urfu.ru

Kuts Dmitry Vladimirovich, seniorteacherof the "Basic Theory of Radio Engineering" department, Institute of Radioelectronics and Information Technologies, Ural Federal University named after the first President of Russia B.N.Yeltsin. 620002, Sverdlovsk region, Ekaterinburg, Mira street, 19. E-mail: d.v.kutc@urfu.ru

Tretyak Nataliya Vadimovna, master of the "Public Administration" department, Institute of Public Administration and Entrepreneurship, Ural Federal University named after the first President of Russia B.N.Yeltsin. 620002, Sverdlovsk region, Ekaterinburg, Mira street, 19. E-mail: n.v.tretiak@urfu.ru

УДК 004.43 Вестник УрФО № 2(20) / 2016, стр. 15–18

Скурлаев С. В., Соколов А. Н.

УСТАНОВКА ОПЕРАЦИОННЫХ СИСТЕМ СЕМЕЙСТВ WINDOWS И LINUX СО СРЕДСТВАМИ ЗАЩИТЫ ИНФОРМАЦИИ НА ОТЧУЖДАЕМЫЙ НАКОПИТЕЛЬ

Рассмотрены особенности установки операционной системы специального назначения «ASTRALinuxSpecialEdition» (релиз «Смоленск»)на отчуждаемый USB-накопитель. Проведено сравнение с установкой на отчуждаемый USB-НЖМД накопитель рабочей среды WindowsToGo и средства защиты информации SecretNet 7. Проанализированыпреимущества и недостатки каждой из рассмотренныхинсталляций и особенности сценариев их применимости для реализации методов доверенной загрузки.

Ключевые слова: *автоматизированная система (АС), несанкционированный доступ (НСД), операционная система (ОС), операционная система специального назначения (ОССН), средство защиты информации (СЗИ).*

Skurlaev S. V., Sokolov A. N.

INSTALLING OPERATING SYSTEMS FROM WINDOWS AND LINUX FAMILIES WITH MEANS OF PROTECTING INFORMATION ON A REMOVABLE DEVICE

The article discusscertain checkpoints of setting up an operating system of special meaning (ASTRA Linux «Smolensk» Release) on a removable USB-device. Compares installing Windows To Go environment with mean of protecting information Secret Net 7 on a USB-HDD. Analyzedadvantages and disadvantages of each of the considered installations and especially their application scenarios for implementing trusted boot methods.

Keywords: *automated system (AS), unauthorized access (UA), operating system (OS), operating system of special meaning (OSSM), means of protecting information from unauthorized access.*

В [1] описано применение технологии WindowsToGo и сертифицированного средства защиты информации SecretNet 7 с целью реализации установки операционной системы на отчуждаемыйнакопитель.Проанализируем возможности и особенности установки на внешний USB-Flash накопитель сертифицированной операционной системы «ASTRA Linux Special Edition» (релиз «Смоленск») (далее операционная система специального назначения, ОССН), а также особенности функционирования, преимущества и недостатки каждой из представленных инсталляций.

Установка ОССН на USB-Flashнакопитель проведена в штатном режиме:

Компьютер загружен с оптического диска с инсталляционным дистрибутивом ОССН.

Все ответы на запросы мастера установкиданы стандартно, на вопросе выбора системного диска указан подключенный USB-Flashнакопитель. На рис. 1 приведён вывод утилиты fdisk, показывающий существующие разделы на используемом в эксперименте USB-Flashнакопителе Kinston Data Traveler Hyper X 3.0 128 Gb. На рис. 2 приведён вывод мастера установки после выбора используемого накопителя в качестве основного системного диска для установки ОССН.На приведённых рисунках видно, что отчуждаемый накопитель определяется как стандартное блочное устройство (/dev/sda) и ничем не отличается для мастера установки от фиксированного накопителя, например, накопителя на жёстких магнитных дисках (НЖМД), напрямую подключенного к материнской плате компьютера.

Получено сообщение «Установка завершена».

```
~ # fdisk -l /dev/sda

Disk /dev/sda: 126.6 GB, 126567317504 bytes
255 heads, 63 sectors/track, 15387 cylinders, total 247201792 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00028fa6

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *        2048     1953791      975872   83  Linux
/dev/sda2         1955838   247199743   122621953    5  Extended
/dev/sda5         1955840    15626239     6835200   83  Linux
/dev/sda6        15628288    19531775     1951744   83  Linux
/dev/sda7        19533824    27918335     4192256   82  Linux swap / Solaris
/dev/sda8        27920384    28698623      389120   83  Linux
/dev/sda9        28700672   152928255    62113792    7  HPFS/NTFS/exFAT
~ # _
```

Рис. 1. Вывод утилиты fdisk, отражающий существующие разделы на используемом накопителе.

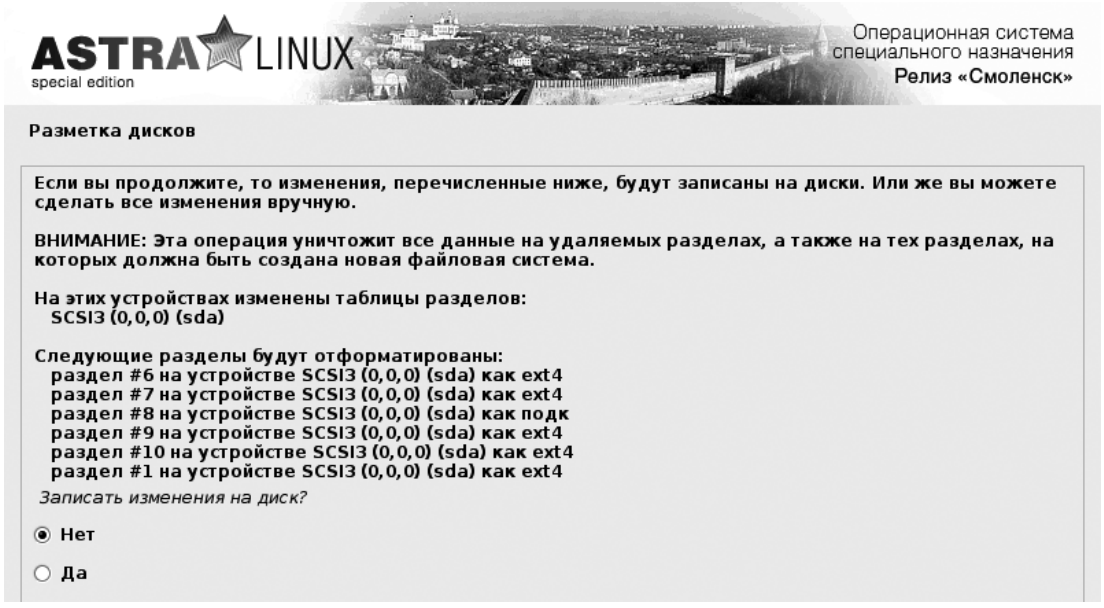

Рис. 2. Вывод мастера установки после выбора используемого накопителя в качестве основного диска для установки ОССН.

Таблица 1. Сравнение применимости инсталляций решений на базеоперационных систем семейств Windows и Linux со средствами защиты на отчуждаемый накопитель

Сравниваемые аспекты	**Рабочая среда Windows To Go с установленным SecretNet 7**	**ОССН ASTRALinux версия «Смоленск»**
Применимые USB-накопители	USB-HDD (НЖМД); при использовании USB-Flash накопителя возникают проблемы с откликом файловой системы, что не является строгим ограничением, но сильно затрудняет использование системы	USB-Flash или USB-HDD: возможно оптимально использовать оба типа накопителей
Масштабируемость ПО	Возможность установки любого прикладного ПО, работающего под управлением ОС Windows	Возможностьиспользования ПО из официальных репозиториев, а также скомпилированногосредствами ОССН; есть сертификационные ограничения, - например, нельзя пересобирать ядро и системные библиотеки
Ограничения в применении	Полностью подходит только для АС классов 3А и ниже; для класса АС 2А требуется применение дополнительных организационных мер [1]	Установка на отчуждаемый накопитель не накладывает ограничений на использование
Переносимость инсталляции с фиксированного диска	Возможностьпереноса всего окружения Windows с внутреннего НЖМД компьютера с предварительным созданием на базе этого окружения шаблона установки (возможность развёртывания этого шаблона на отчуждаемый накопитель)	Возможностьпереносадомашних каталогов и файлов конфигураций сервисов с внутреннего НЖМД компьютера на отчуждаемый накопитель после установки ОССН

После перезагрузки компьютер загружен с USB-Flashнакопителя, указаны реквизиты созданного во время установки пользователя, вход в систему осуществлён успешно.

Проведён тест работоспособности установленного по умолчанию программного обеспечения (ПО) (из инсталляционного дистрибутива на оптическом диске) путём его запуска. Тест прошёл успешно.

Настроены основные механизмы согласно руководству [2]. Проведены тесты работоспособности механизмов защиты согласно руководству [3], а также путём реализации экспертным методом модели, рассмотренной в [4]. Сделан вывод о полной работоспособности встроенных механизмов защиты.

В табл. 1 приведены результаты сравнения решения на базе рабочей среды WindowsToGo с установленным СЗИ SecretNet 7 и решения на базе ОССН ASTRA Linux версия «Смоленск», установленной на отчуждаемый USB-Flash накопитель.

По результатам сравнения можно сделать следующие выводы:

1. Несмотря на то, что нет технических ограничений на использование рабочей среды Windows To Go с USB-Flash накопителем, сопутствующая задержка операций ввода-вывода файловой системы существенно сказывается на удобстве работыс данной ОС. Отчуждаемые накопители типа USB-HDD или USB-SSD не имеют подобного недостатка. В случае использования ОССН ASTRA Linuxтип отчуждаемого накопителя не играет особой роли.

2. Под масштабируемостью здесь понимается возможность установки прикладного ПО без нарушений требований руководящих документов. На WindowsToGoвозможна установка любого прикладного ПО, разработанного для использования в ОС семейства Windows. В случае использования ОС вместе с СЗИ количество операций ввода-вывода значительно увеличивается, что приводит к задержкам при работе с компьютером, но данное утверждение справедливо не только для отчуждаемых накопителей. В случае использования ОССН ASTRALinux возможно пользоваться стандартными возможностями

для дистрибутивов GNU/Linux на основе Debian: использование официальных репозиториев (разработчиков ОССН), компиляция собственных программ из исходных текстов. Ограничения, которые касаются невозможности компиляции новых системных модулей, например, последних версий ядра с сайта kernel.org или последних версий системных библиотек и другого ПО из текстов, не размещённых в официальных репозиториях ОССН, диктуется целесообразностью ненарушения функциональных возможностей продукта по защите информации и сохранению сертификационных требований.

3. Ввиду особенностей реализации средства защиты информации SecretNet 7, функционирование некоторых защитных механизмов на данный момент невозможно без нарушения работоспособности всей рабочей среды WindowsToGo, что требует применение дополнительных организационных мер для восполнения этого недостатка. Защитные механизмы ОССН могут работать в штатном режиме и в случае установки на отчуждаемый накопитель, этоникак не сказывается на работоспособности предлагаемого решения.

4. Перенести всё рабочее окружение с внутреннего НЖМД на отчуждаемый накопитель возможно в рамках любого из предложенных решений. В случае Windows To Go потребуется создать шаблон-образ с установленной системы, который после будет использован для реализации рабочего окружения WindowsToGo. В случае использования ОССН ASTRALinux потребуется скопировать на отчуждаемый накопитель домашние каталоги пользователей и конфигурационные файлы сервисов с предварительной установкой и воссозданием списков пользователей, а также установленного ПО.

Перечисленные преимущества и ограничения являются техническими. Стоит также отметить, что на применимость того или иного решения в конкретном сценарии влияют и другие характеристики. Например, ОССН ASTRA Linux возможно использовать в тех АС, где технологический процесс предполагает использование СУБД и клиента базы данных, которые присутствуют в официальных репозиториях, или где пользователи обучены правилам работы в подобных ОС. Вариант с использованием WindowsToGoне повлечёт необходимость дополнительного обучения пользователей, не ограничит в выборе прикладного ПО, но потребует применения дополнительных организационных мер.

Примечания

1. Скурлаев С. В., Соколов А. Н. Применение технологии WindowsToGo в автоматизированных системах классов 2А и 3А с сертифицированными средствами защиты информации //Вестник УрФО. Безопасность в информационной сфере.– Челябинск:Изд.центрЮУрГУ,2015.– №4(18).– С. 12 – 15.

2. «Операционная система специального назначения «AstraLinuxSpecialEdition». Руководство по КСЗ. Часть 1»РУСБ.10015-01 97 01-1 – 2012.

3. «Операционная система специального назначения «AstraLinuxSpecialEdition». Руководство по КСЗ. Часть 2»РУСБ.10015-01 97 01-2 – 2012.

4. Скурлаев С.В., Соколов А.Н. Исследование системы разграничения доступа на основе поведенческой модели пользователя //Информационное противодействие угрозам терроризма: научно-практический журнал. Материалы XIV научно-практической конференции «Информационная безопасность – 2015». Таганрог, 4 – 7 июня 2015 г. – Таганрог: Изд. Южного федерального университета, 2015. – №24. – С. 98 – 102.

Скурлаев Сергей Вадимович, аспирант кафедры безопасности информационных систем ФГБОУ ВПО «Южно-Уральский государственный университет» (национальный исследовательский университет); специалист по защите информации ООО «Стратегия безопасности», г. Челябинск. E-mail: sch1081024@mail.ru

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

Sergey Skurlaev, postgraduate Department of Information Systems Security "South Ural State University", security engineer of the LLC "Strategy of security", Chelyabinsk. E-mail: sch1081024@mail.ru

Alexander Sokolov, a. M. N., Associate Professor, Head. the Department of Information Systems Security "South Ural State University", Chelyabinsk. E-mail: ANSokolov@inbox.ru

УДК 004.032.26 Вестник УрФО № 2(20) / 2016, стр. 19–22

Бондарев В. Ю., Сорокин А. С., Кротова Е. Л.

ИСКУССТВЕННАЯ НЕЙРОННАЯ СЕТЬ КАК СРЕДСТВО И МЕТОД СТАТИСТИЧЕСКОЙ ОБРАБОТКИ ДАННЫХ

В статье изучается использование искусственной нейронной сети для решения задач статистической классификации и оценивания. Как правильно использовать искусственную нейронную сеть для решения задач статистической классификации и определять пригодность сети для решения этих задач. Обучение нейронной сети рассматривается, как одна из причин почему мы используем искусственную нейронную сеть для решения поставленных задач. Также,если наши данные искажены или неполны, нейронная сеть все равно выдаст верный результат при правильном обучении, конечно же. Это является еще одной причиной использовать искусственную нейронную сеть. В работе описывается анализ данных, которые мы пропускали через нашу обученную сеть и находили коэффициент искажения.

Ключевые слова: *искусственная нейронная сеть, нейроны, статистическая классификация, статистическая обработка данных.*

Bondarev V. Yu., Sorokin A. S., Krotova E. L.

ARTIFICIAL NEURAL NETWORK AS A MEANS AND METHOD OF STATISTICAL DATA PROCESSING

This article examines the use of artificial neural network to solve the problems of statistical classification and evaluation. How to use an artificial neural network to solve the problems of statistical classification and determine the suitability of the network to meet these challenges. Neural network training is regarded as one of the reasons why we use an artificial neural network for the task.

Also, if our data are distorted or incomplete, the neural network still will give the correct result with the right training course. This is another reason to use an artificial neural network. The

paper describes the analysis of the data, which we passed through our network of trained and found distortion coefficient.

Keywords: *artificial neural network, neurons, statistical classification, statistical data processing.*

Введение

Статистическая обработка и анализ данных является актуальной задачейв медицине, в технике, в бизнесе или в тех же информационных технологиях. Эта задача имеет разные пути решения. Мы рассмотрим решения данной задачи с помощью искусственной нейронной сети. Искусственная нейронная сеть (ИНС) - это набор искусственных нейронов, которые соединены между собой, подобно биологической нейронной сети. Задача обучения нейронной сети состоит в преобразовании входных данных в выходные, причем это преобразование задается нейронами. Нейроны ищут сложную зависимость между входными данными и выходными, далее, применяя эту зависимость, ИНС может выдать на выходе верный результат даже, если исходные данные были неполными или искаженными. Для нахождения этой зависимости сеть обучается и находит связь между нейронами. В этом и есть большой плюс ИНС перед другими алгоритмами.

Описание этапов создания искусственной нейронной сети

Для создания ИНС был использован пакет прикладных программ MATLAB. Формат данных бинарный, то есть 0 или 1. Тип сети выбираем feed-forwardbackprop (Сеть с прямым распространением сигнала и обратным распространением ошибки). Количество нейронов берем равное 10.

Входной бинарный вектор состоит из 28000 значений, но мы возьмем ¼ часть. Но прежде чем, запустить эти данные в сеть мы высчитываем коэффициент корреляции Пирсона, для того, чтобы найти статистическую взаимосвязь между входным вектором и выходным. Выбрав, входной вектор с большим коэффициентом, запускаем входные и выходные данные в сеть. Сеть обучается за 5 итераций. Ниже показан график обучения, в котором на оси абсцисс располагается номер итерации, а на оси ординат степень среднеквадратичной ошибки.

Из графика видно, что все три прямые совпадают, и степень квадратичной ошибки маленькая, а наилучшая проверка 0.1 на 5 - ой итерации. Следовательно, сеть обучена правильно.

Теперь по этой обученной сети проверяем остальную часть данных и проводим их анализ.

Анализ полученных данных на выходе и сравнение их с целевыми, определение пригодности нашей сети.

При анализе данных будем высчитывать коэффициент искажения

$$k = \frac{m}{n} * 100$$

где m – кол-во искаженных, n – количество всех данных

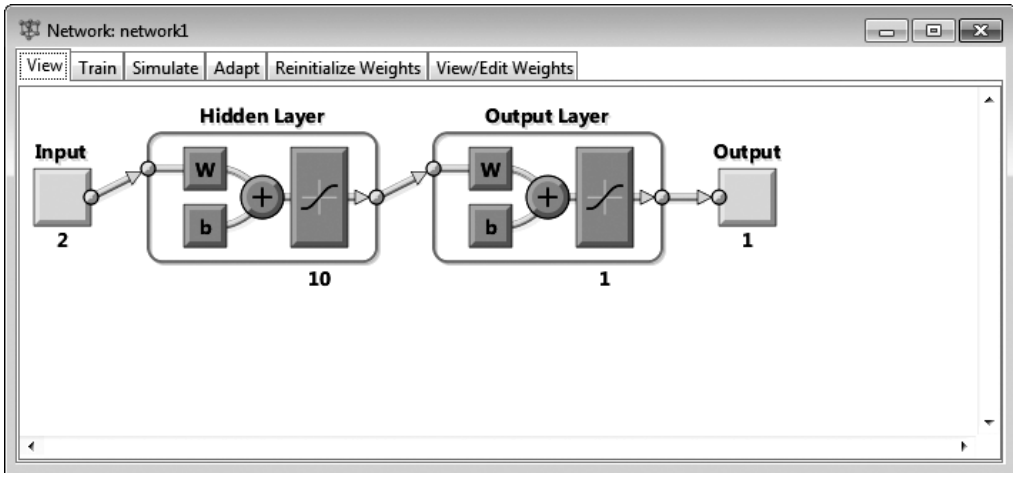

Рисунок 1. Структура нейронной сети

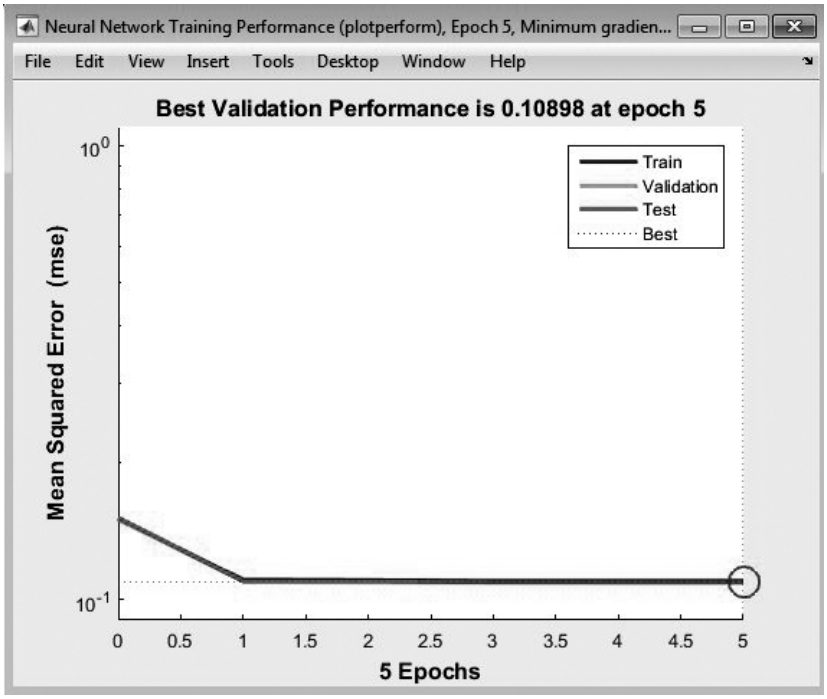

Рисунок 2. График обучения сети

Если k меньше 25%, значит наша сеть пригодна для статистической обработки и обучена правильно.

Из таблицы видно, что коэффициент искажения у всех данных меньше 25%, значит можем смело утверждать, что наша сеть пригодна для статистической обработки данных и правильно обучена.

Заключение

В данной статье мы рассмотрели искусственную нейронную сеть как метод, средство статистической классификации и обработки данных. Сеть была обучена с помощью типа обучения «с учителем». Было выявлено, что сеть обучилась правильно и пригоднадля решения задач статистической классификации.

Таблица 1.

Наименование данных	Кол-во искажений	Кол-во данных	k(%)
pkk.perm.ru	192	862	22.27
www.shareman.tv.mined	2931	13904	21.08
shareman.tv.mined	3272	14966	21.86
shareman_tv_mined	1793	10488	17.09
Shareman.tv.(combined)	4043	18870	21.42
omsk_domru_mined	733	3439	21.31

Примечания

1. Медведев В.С., Потемкин В.Г. Нейронные сети. MATLAB 6/ Под общ. ред. к. т. н.В.Г. Потемкина. — М. :ДИАЛОГ-МИФИ, 2002.— С. 496.

2. Круглов В.В., Борисов В.В. Искусственныенейронные сети. Теория и практика. - 2-е изд., стереотип. — М. :Горячая линия - Телеком, 2002.— С. 382.

3. Krotov l. N., Krotova e. L., Bogdanov N.V. Identification and counteractions to attacks of malefactors in the automated working system. – 2016.

Сорокин Андрей Станиславович, студент по направлению «Информационная безопасность» ПНИПУ. 614990, Пермский край, г. Пермь - ГСП, Комсомольский проспект, д. 29. E-mail: sly-kyper@yandex.ru

Бондарев Владислав Юрьевич, студент по направлению «Информационная безопасность» ПНИПУ. 614990, Пермский край, г. Пермь - ГСП, Комсомольский проспект, д. 29. E-mail: mr.bond1995@mail.ru

Кротова Елена Львовна, кандидат физико-математических наук, доцент кафедры высшей математики ПНИПУ. 614990, Пермский край, г. Пермь - ГСП, Комсомольский проспект, д. 29. E-mail: lenkakrotova@yandex.ru

Sorokin Andrew Stanislavovich, student in the direction of «Information Security» PNIPU, 29, Komsomolsky prospect, Perm, 614990. E-mail: sly-kyper@yandex.ru.

Bondarev Vladislav Yuryevich, student in the direction of «Information Security» PNIPU, 29, Komsomolsky prospect, Perm, 614990. E-mail: mr.bond1995@mail.ru

Krotova Elena Lvovna, Candidate of Physical and Mathematical Sciences, Associate Professor of the Department of Higher Mathematics PNIPU, 29, Komsomolsky prospekt, Perm , 614990. E-mail: lenkakrotova@yandex.ru

УДК 004.056.5 Вестник УрФО № 2(20) / 2016, стр. 23–28

Шабуров А. С., Журилова Е. Е.

ОСОБЕННОСТИ РЕАЛИЗАЦИИ АЛГОРИТМОВ МОРФОЛОГИЧЕСКОГО АНАЛИЗА В DLP-СИСТЕМАХ

В статье анализируется проблема выбора оптимального алгоритма морфологического анализа для DLP-систем. Рассматриваются основные алгоритмы, используемые для морфологического анализа: стеммер Портера, Stemka и Mystem, а так же алгоритм определения слова по суффиксам и аффиксам. Выявляются их возможности, достоинства и недостатки. Приводятся схемы работы этих алгоритмов и их описание. Рассматривается возможность применения этих алгоритмов в DLP-системах, на основе сравнения их характеристик и нахождения оптимальных вариантов. Предлагается структурная модель, определяющая место морфологического анализа в функционировании DLP-системы.

Ключевые слова: *утечка информации, DLP-система, морфологический анализ, определение слова, алгоритм, основа слова.*

Shaburov A. S., Zhurilova E. E.

FEATURES OF THE MORPHOLOGICAL ANALYSIS ALGORITHMS OF DLP-SYSTEMS

In the article analyzed the problem of choosing resembling algorithm of morphological analysis of DLP-system. It views the main algorithms of morphological analysis: Porter's stemmer, Stemka, Mystem, and also the algorithm of word determination by suffixes and affixes. Reveal its capabilities, strengths and weaknesses. It shows the scheme of this algorithms and its description. Considering the opportunity of using these algorithms in DLP-systems, by comparing its characteristics and finding the optimal variants. It gives a structural model, which determine the place of morphological analysis in functioning of DLP-system.

Keywords: *information leak, DLP-system, morphological analyses, word definition, algorithm, stem of a word.*

В современных условиях безопасность функционирования информационных систем зависит от многих факторов. Одной из актуальных проблем обеспечения функционирования систем различного назначения является создание защищенной информационной среды. Защищенность среды зависит в первую очередь от блокирования несанкционированного доступа, а так же защиты от утечек информации. На сегодняшний день одним из самых распространенных решений в области борьбы с утечками информации являются

DLP – системы. Рынок средств безопасности предоставляет достаточный выбор решений, в различных ценовых категориях. Основной функционал DLP – систем схож, но каждая компания разработчик подобных систем использует различные подходы в технологиях обнаружения каналы утечки информации и его блокирования. Кроме того, используются разнообразные формы представления полученной информации.

Не смотря на это, основой выявления утечек информации в DLP – системах является морфологический анализ текстов. Главным преимуществом этой технологи является универсальность алгоритмов анализа, которые позволяют проводить оценку как сообщений в различных мессенджерах, так и текста электронных документов [1]. Так же преимуществами использования этого метода являются возможность работы с содержимым, обучаемость лингвистического алгоритма, масштабируемость и простота настройки. К недостаткам можно отнести зависимость от используемого языка и необходимости применения вероятностного подхода [2].

Морфологический анализ представляет собой процесс определения грамматического значения словоформы и выделения ее основы, или, иными словами, выделение ключевых слов в потоке текста [3].

Любой алгоритм морфологического анализа состоит из двух основных компонентов – декларативного и процедурного. При этом, декларативный компонент подразумевает таблицы структурированных данных, требуемых для анализа, а процедурный компонент содержит сами алгоритмы анализа и вспомогательные процедуры [4].

В связи с особенностями русского языка и наличием большого количества слов исключений в нем, осуществление морфологического анализа может быть затруднено. Для преодоления этих затруднений существует возможность выбора метода морфологического анализа, среди которых, наиболее известными, являются три основных.

Первым методом является составление морфологического словаря для конкретного предприятия, вручную, с учетом всех ключевых слов, способных указать на утечку информации. Данный способ целесообразно использовать при небольшом объеме возможных ключевых слов, анализируя корень данных слов. Если информационная система предприятия (организации) сложная, содержит большое количество разнообразных ресурсов, то использование данного метода будет затруднительно, особенно на начальных этапах.

Особенностью второго метода является использование алгоритма стемминга, суть которого состоит в выделении основы слова, а не его корня.

Для русского языка наиболее популярными алгоритмами стемминга являются:

- стеммер Портера;
- Stemka;
- Mystem [5].

Стеммер Портера, иначе называемый «snowball», был разработан в 1979 году изначально для английского языка, впоследствии адаптирован под анализ на основе русского языка. При использовании данного алгоритма стемминг происходит на основе множества существующих суффиксов. Сам алгоритм состоит из четырех основных шагов и представлен на рис. 1.

Цифрой 1 обозначен блок операций для отсечения формообразующих суффиксов. Цифрой 2 обозначен блок операций для отсечения окончаний «и». Цифрой 3 обозначен блок операций для отсечения словообразующих суффиксов. Цифрой 4 обозначен блок операций для отсечения суффиксов превосходной формы, окончаний на «ь» и удвоенных «н».

В результате выполнения алгоритма получается требуемая для опознания часть слова.

Основным достоинством алгоритма Портера является отсутствие словарей основ, что существенно увеличивает быстродействие.

К отрицательным свойствам данного алгоритма можно отнести возможность потери части информации из анализируемого слова. Кроме того уязвимостью данного алгоритма является возможность ошибки со стороны оператора, задающего правила проверки.

Stemka – русско-украинский идентификатор морфологии, который был создан с помощью специально разработанного морфологического модуля [6]. Алгоритм основан на вероятностной модели. Составляется массив данных, который включает в себя пары «две последние буквы основы» и «суффикс», таким образом, получаются модели различных слов. После этого определяется вероятность появления моделей в тексте, и при вероятности 1/10000 модель отсекается. Результат представляет собой таблицу переходов ко-

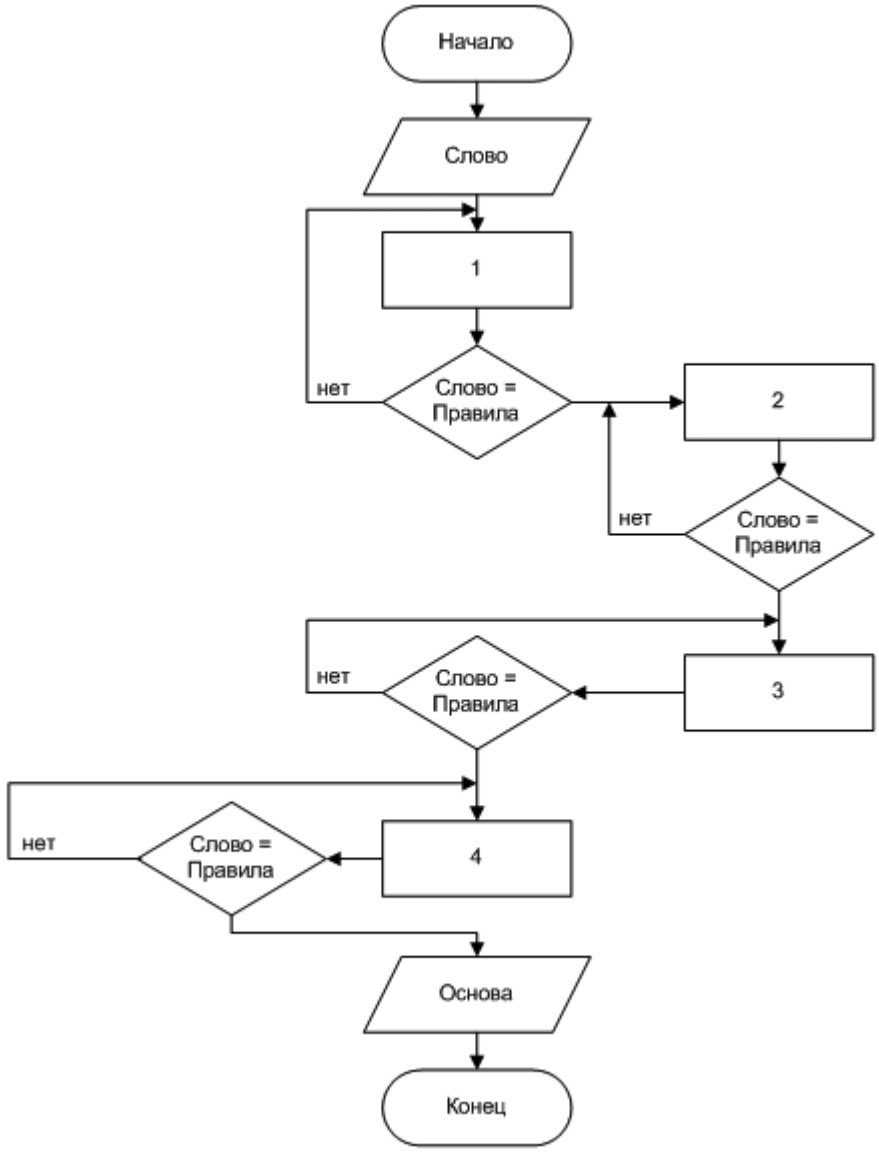

Рис. 1. Алгоритм работы стемминга Портера

нечного автомата, по которым сканируется слово [5].

Для рассмотренных алгоритмов Snowball и Stemka в процессе отладки было сформулировано правило, предусматривающее наличие хотя бы одной гласной буквы в основе.

Mystem был разработан в 1998 Ильей Сегаловичем. Модель строится в виде леса инвертированных префиксных деревьев суффиксов и инвертированного префиксного дерева для основ, для этого используется словарь с перечислением всех грамматических форм (парадигмы) слова [5].

На рис. 2 представлен алгоритм Mystem, функционирование которого заключается в следующем. Очередное анализируемое слово, подвергается разделению на стемму и суффикс. Такое разделение производится программой на основе уже имеющегося дерева суффиксов. Далее происходит сопоставление получившейся основы с уже имеющимися в словаре (блок 2), для нахождения соответствий. Если соответствие найдено, алгоритм заканчивает работу и результатом является гипотеза для словарного слова.

Если же соответствие найти не удалось, то алгоритм продолжает работу по поиску нужной гипотезы. Для этого происходит генерация гипотетической модели слова, базирующейся на основе слова, суффиксе и ближайшей основе из имеющегося словаря (блок 3). После этого полученная модель снова сверя-

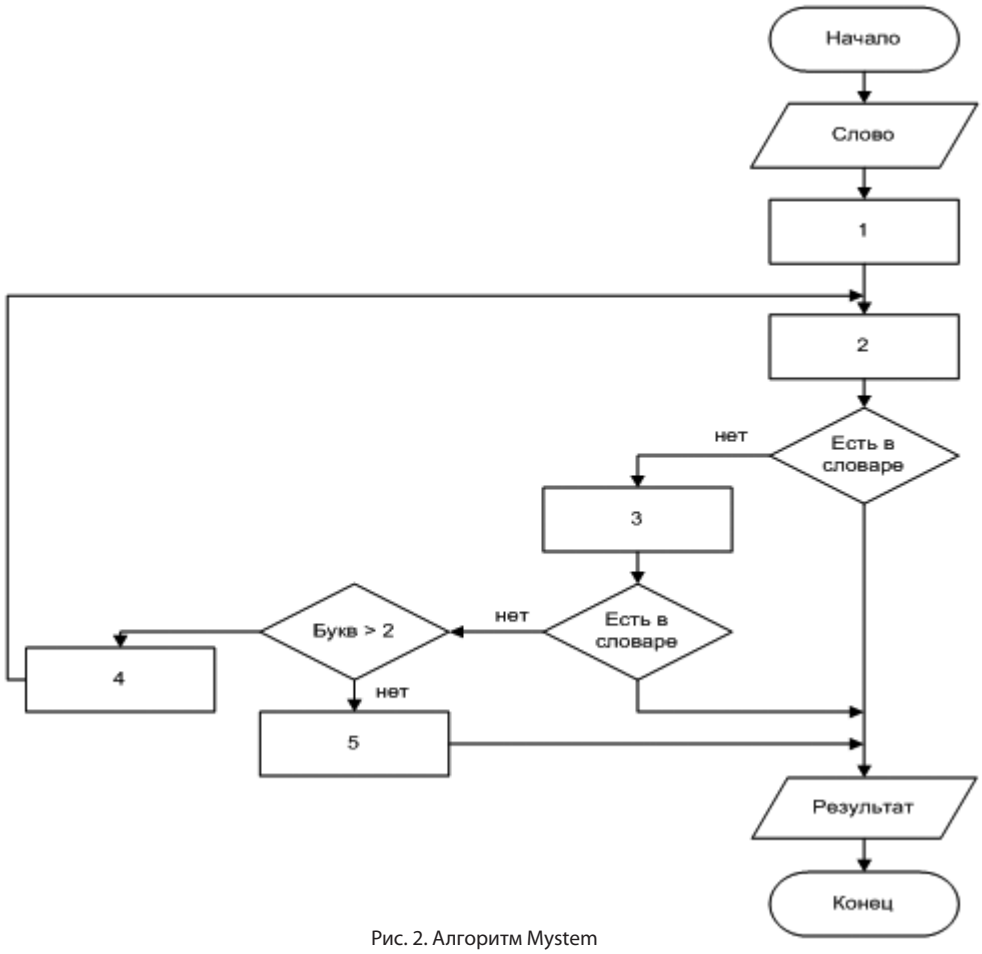

Рис. 2. Алгоритм Mystem

ется со словарем. При положительном результате алгоритм заканчивает работу.

Если результат снова отрицателен и совпадение не найдено, то алгоритм продолжает производить вышеуказанные действия, постепенно уменьшая основу на одну букву (блок 4) до тех пор, пока основа не будет найдена, либо пока количество букв не сократится до двух. В этом случае происходит ранжирование все полученных в ходе работы алгоритма гипотез (блок 5) по продуктивности, и отсекание менее продуктивных. В результате на выходе алгоритма получается набор гипотез для несуществующего в имеющемся словаре слова.

Преимуществами данного алгоритма являются простота реализации и словарей, а так же возможность определения форм слова отсутствующих в словаре. К недостаткам относятся ориентация только на русский язык и анализ по окончанию.

Третьим методом является определение слова по его суффиксу и аффиксу и приведение слова к его начальной форме. Данный способявляется наиболее рациональным, благодаря особенностям русского языка, однако для повышения качества работы алгоритма необходимо добавить как можно больше слов исключений [7].

Таким образом, использование одного из вышеперечисленных алгоритмов морфологического анализа позволяет распознать конфиденциальную информацию в потоке перехватываемой информации.

Существует несколько критериев влияющих на выбор алгоритма морфологического анализа для DLP-систем. К ним относятся точность определения слова при морфологическом анализе, возможность обучаемости, временные затраты на настройку системы. Согласно исследованиям точность определения должна быть не ниже 95-97%. Возможность обучаемости позволяет сымитировать на этапе настройки системы опасные ситуации, тем самым позволив системе самостоятельно адаптироваться под необходимые параметры, что существенно сокращает время ввода системы в эксплуатацию. Для сотрудни-

Таблица 1. Сравнение алгоритмов морфологического анализа

Название алгоритма	Точность определения слова при морфологическом анализе	Возможность обучаемости	Временные затраты на настройку
Составление морфологического словаря	80-85%	Отсутствует	1-2 дня
Стеммер Портера	85-90%	Отсутствует	3-5 часов
Stemka	87-95%	Присутствует	1-1,5 дня
Mystem	92-97%	Присутствует	2-3 дня
Определение по суффиксу и аффиксу	90-96%	Отсутствует	1-2 дня

ка, не имеющего навыков аналитика, создание словаря для морфологического анализа может занять достаточно большое количество времени, что существенно скажется на быстроте ввода системы в эксплуатацию. Проанализируем вышеуказанные алгоритмы по этим критериям (Таблица 1).

Исходя из данных представленных в таблице, наиболее подходящим алгоритмом морфологического анализа для использования в DLP-системах является алгоритм Mystem. Несмотря на длительность настройки, алгоритм имеет самую высокую, из перечисленных алгоритмов, вероятность определения слова и обладает важным свойством обучаемости.

На рис. 3 представлено место морфологического анализа в структуре работы DLP-системы. Информация, отправляемая пользователем перехватывается и передается на сервер, где подвергается морфологическому анализу. В процессе анализа определяются источники информации, конечные получатели, а так же иные характеристики, необходимые для принятия решения о принадлежности информации к конфиденциальной. При наличии признаков возможной утечки информации ограниченного доступа, администратору информационной безопасности передается отчет о нарушении, в который так же включаются данные выявленные при анализе. На основании политики информационной безопасности принимается решение по выявленному инциденту.

Таким образом, морфологический анализ является основой алгоритма выявления утечек информации в DLP – системах. Качество

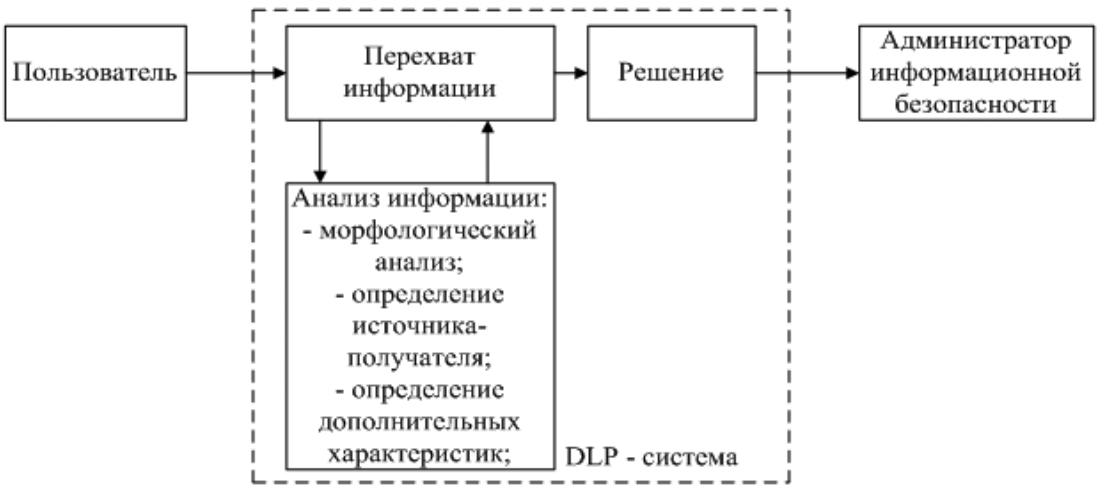

Рис. 3. Место морфологического анализа в структуре DLP-системы

реализации анализа определяет эффективность функционирования всей системы. В процессе исследования были рассмотрены различные алгоритмы морфологического анализа, используемые для выявления каналов утечки информации в DLP-системах. Анализ характеристик и функциональных возможностей позволил выявить оптимальный алгоритм, наиболее подходящий для использования, основным преимуществом которого является возможность получения не только слова имеющегося в словаре, но и нескольких гипотез для слова, которое в словаре отсутствует.

Примечания

1. Давлетханов М. Современные технологии обнаружения утечек [Электронный ресурс]. – URL: https://www.anti-malware.ru/node/8578#part2(дата обращения: 6.04.2016).

2. Жарников М. Обзор технологий и вендоров «Классического» DLP//Презентация компании НТКС Информационная безопасность. – Екатеринбург, 2014.

3. Шабуров А.С., Журилова Е.Е., Лужнов В.С. Технические аспекты внедрения DLP – системы на основе Falcongaze Secure Tower // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. – Пермь, 2015. - № 16. – С. 57 - 67.

4. Пруцков А.В., Розанов А.К. Методы морфологической обработки текстов // Прикаспийский журнал: управление и высокие технологии. Обработка сигналов и данных, распознавание образов, выявление закономерностей и прогнозирование. – Астрахань, 2014. № 3(27). URL: http://prutzkow.com/pdf/114.pdf (дата обращения: 6.04. 2016).

5. Астапова О.П. Исследование и разработка методов нормализации слов русского языка: курсовая работа. – М., 2012. URL: http://seminar.at.ispras.ru/wp-content/uploads/2012/10/Astapova-thesis.pdf (дата обращения: 6.04.2016).

6. Сегалович И. Быстрый морфологический алгоритм подбора неизвестного для поисковой системы слова с помощью словаря [Электронный ресурс]. – М., 2014 URL:http://wseob.ru/seo/morphological-algorithm (дата обращения: 6.04.2016).

7. Жаринов Р.Ф. Метод защиты от перлюстрации в DLP–системах // Доклады ТУСУРа. – Томск, 2012. - № 1 (25). URL: http://www.tusur.ru/filearchive/reports-magazine/2012-25-2/126.pdf (дата обращения: 6.04 2016).

8. Левцов В. Контроль подмены символов в системах борьбы с утечками конфиденциальных данных [Электронный ресурс] URL: http://www.leta.ru/press-center/publications/article_487.html (Дата обращения: 10.04.2016).

Шабуров Андрей Сергеевич, кандидат технических наук, доцент кафедры автоматики и телемеханики Пермского национального исследовательского политехнического университета. 614990, Пермь, Комсомольский пр., 29. E-mail: shans@at.pstu.ru

Журилова Елена Евгеньевна, студент кафедры автоматики и телемеханики Пермского национального исследовательского политехнического университета. 614990, Пермь, Комсомольский пр., 29. E-mail: ele11485995@yandex.ru

Shaburov Andrey Sergeevich, PhD of Technical Sciences at the Department of Automation and Telemechanics, Perm National Research Polytechnic University. 614990, 29, Komsomolsky prospect, Per. E-mail: shans@at.pstu.ru

Zhurilova Elena Evgen'evna, student at the Department of Automation and Telemechanics, Perm National Research Polytechnic University. 614990, 29, Komsomolsky prospect, Perm. E-mail: ele11485995@yandex.ru

УДК 004.056.5 Вестник УрФО № 2(20) / 2016, стр. 29–32

Сорокин А. С., Бондарев В. Ю., Кротова Е. Л.

СОЗДАНИЕ И ОБУЧЕНИЕ ИСКУССТВЕННОЙ НЕЙРОННОЙ СЕТИ ДЛЯ СТАТИСТИЧЕСКОГО ОЦЕНИВАНИЯ ДАННЫХ

В данной работе представлено использование искусственной нейронной сети для оценки предоставляемых услуг пользователям. Предлагаемая нами искусственная вычислительная модель решает задачи статистической классификации. Данная сеть позволяет сравнить полученные данные с поставленной целью, т.е. строится границы для значений параметров. В работе описывается подготовка данных для ввода их в сеть, создание самой сети и её обучение, а также проверка на правильность обучения и нахождение искажений. Также говорится о применении сети к другим независимым параметрам. Венчает нашу статью знакомство с искусственной нейронной сетью.

Ключевые слова: *искусственная нейронная сеть, статистическая классификация, статистическое оценивание, применение нейронной сети.*

Sorokin A. S., Bondarev V. Yu., Krotova E. L.

CREATING AND TRAINING ARTIFICIAL NEURAL NETWORK FOR STATISTICAL DATA EVALUATION

This paper presents the use of artificial neural networks to assess the services provided to users. Our proposed artificial computational model solves the problems of statistical classification. This network allows you to compare the data with the intended purpose, i.e. constructed boundary parameter values. The paper describes how to prepare data for input into the network, the establishment of the network itself and its training, as well as checking for proper training and finding distortion. Also it refers to the use of the network to the other independent parameters. Crowned our article familiarity with the artificial neural network.

Keywords: *artificial neural network, statistical classification, statistical estimation, the use of a neural network.*

Искусственные нейронные сети стали часто использовать для решения актуальных задач, таких как: прогнозирование, классификация, оценивание и управление. В нашей статье мы используем созданную нами нейронную сеть для оценки данных, после чего проанализируем полученный результат. Что же такое нейронные сети? Нейронные сети - это исключительно мощный метод имитации процессов и явлений, позволяющий воспроизводить чрезвычайно сложные зависимости [1]. Они представляют собой распределен-

ные и параллельные системы, способные к адаптивному обучению путем анализа положительных и отрицательных воздействий. Элементарным преобразователем в данных сетях является искусственный нейрон [2]. Проще говоря, имитируя модели сети нейронов, мы можем найти связь между входным вектором данных и выходным. Для нахождения этой зависимости, мы не будем программировать сеть, а обучим её, после чего можно выявить искаженность других данных к обученным данным по нейронной сети.

Разработка искусственной нейронной сети в пакете MATLAB.

Наша задача заключается в создании и обучении нейронной сети для оценки параметров пользователей. Сначала об источнике данных: есть данные shareman, где отображено количество визитов посетителей, самих посетителей будем трактовать как одно число, слепленное из вектора бинарных чисел, т.е. 0 и 1. Получается отображение f(x) –> R, где x - эта «сигнатура» посетителя, R - закодированный результат его посещения: 0 - не задержится больше чем на 15 секунд, 1 - задержится дольше.

И главная цель - это натренировать/выяснить то самое f(), чтобы при новом x было с «хорошей» вероятностью и попадало в правильное R: «произведёт целевое действие» (1) или «не произведёт» (0). Т.е. в совсем редуцированном виде Rтоже сопоставляем 0 или 1. На этих данных мы и будем обучать сеть.

```
001010111111101011011001 –> 1
101101010101010010010010 –> 0
001010100001000011010001 –> 0
......
```

Возьмем часть данных shareman, где их количество составляет около 28 - 29 тысяч значений, в нашем случаи 10000. Но так как»сигнатура» посетителя (входные данные) огромные, нужно их подготовить для нейронной сети. Берём первые 30 значений двоичного числа, и находим корреляцию, т.е. статистическую взаимосвязь между входными значениями и выходными. Для этого нам хорошо подойдет коэффициент Пирсона, где значения коэффициента больше, те значения мы и возьмем на вход.

В программе MATLABвызовем графический интерфейс пользователей для управления сетями и данными (nntool). Подаем входные и выходные данные в нашу сеть, и после чего наблюдаем, что сеть мы обучили за 2 секунды и 11 итераций.

Ниже на рисунке показано на оси абсцисс номер итерации, а на оси ординат - степень средней квадратичной ошибки.

На графике мы наблюдаем,что степень средней квадратичной ошибки маленькая, и наилучшая проверка представлена 0.09 на восьмой итерации.

Проверка созданной искусственной нейронной сети для пригодности к анализу других параметров. Выявление искаженности.

Теперь проверим правильно ли обучилась наша сеть, для этого мы возьмем оставшуюся часть данных shareman, это около 18 - 19 тысяч, и про симулируем их. Она должна нам показать, что получится на выходе, после этого мы сравниваем их с целевыми значениями, и выявляем количество ошибок.

Нейронная сеть будет пригодна для анализа данных, если коэффициент искажения будет не более 25%. Чтобы найти его, найдем отношение количества ошибок на количество всего значений. После обработки полученных данных коэффициент искажений составляет 21,39%. Значит сеть обучилась правильно.

Воспользуемся нашей созданной сетью для анализа других данных. У нас есть данные посещения сайта steklodom.com. Сделаем все те же операции подготовки данных для нейронной сети, а именно: возьмем 30 первых

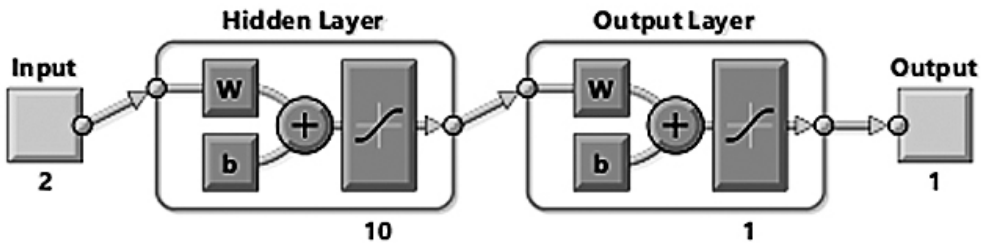

Рис. 1. Искусственная нейронная сеть

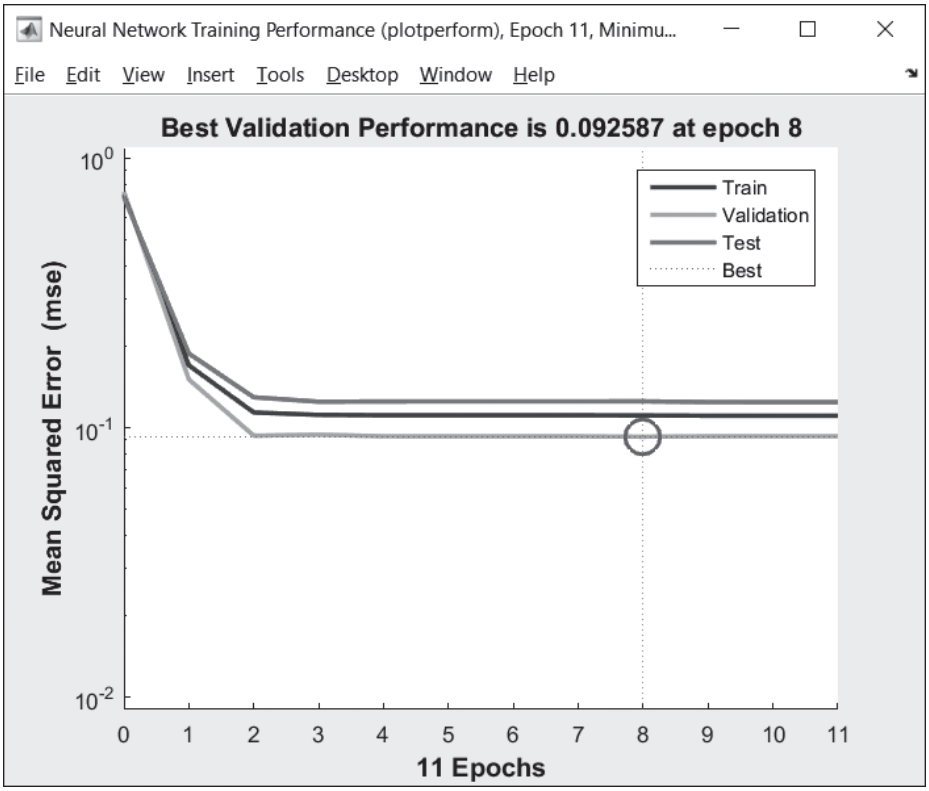

Рис. 2. Представление обучения нейронной сети

значений каждого бинарного числа, найдем наибольший коэффициент Пирсона, чтобы взять найденный вектор на вход. Далее про симулируем их и сравним с целевыми значениями. Нашли коэффициент искажения 36,27%. Значит, для этих данных целевые значения ставятся по-другому, т.е. наша сеть не подойдет для статистической классификации этих данных, так как надо, чтобы он составлял не более 25%.

Протестируем еще один сайт - omsk.dom.ru. Его коэффициент искажения составляет 39,52%. Наглядно видим, что нейронная сеть не предназначена для классификации всех данных, а только для некоторых из них.

Заключение

В рассмотренной статье, мы создали и обучили искусственную нейронную сеть. Также она была рассмотрена как один из способов классификации данных. Как мы уже говорили выше, после симулирования было выявлено, что не все данные подходят для нашей созданной сети. Нужно иметь другую сеть, обученную уже по этим данным, чтобы произвести их статистическое оценивание.

Примечания

1. Медведев В.С., Потемкин В.Г. Нейронные сети. MATLAB 6/ Под общ. ред. к. т. н.В.Г. Потемкина. — М. :ДИАЛОГ-МИФИ, 2002.— С. 496.

2. Круглов В.В., Борисов В.В. Искусственныенейронные сети. Теория и практика. - 2-е изд., стереотип. — М. :Горячая линия - Телеком, 2002.— С. 382.

3. Krotov l. N., Krotova e. L., Bogdanov N.V. Identification and counteractions to attacks of malefactors in the automated working system. – 2016.

Сорокин Андрей Станиславович, студент по направлению «Информационная безопасность» ПНИПУ. 614990, Пермский край, г. Пермь - ГСП, Комсомольский проспект, д. 29. E-mail: sly-kyper@yandex.ru

Бондарев Владислав Юрьевич, студент по направлению «Информационная безопасность» ПНИПУ. 614990, Пермский край, г. Пермь - ГСП, Комсомольский проспект, д. 29. E-mail: mr.bond1995@mail.ru

Кротова Елена Львовна, кандидат физико-математических наук, доцент кафедры высшей математики ПНИПУ. 614990, Пермский край, г. Пермь - ГСП, Комсомольский проспект, д. 29. E-mail: lenkakrotova@yandex.ru

Sorokin Andrew Stanislavovich, student in the direction of «Information Security» PNIPU, 29, Komsomolsky prospect, Perm, 614990. E-mail: sly-kyper@yandex.ru.

Bondarev Vladislav Yuryevich, student in the direction of «Information Security» PNIPU, 29, Komsomolsky prospect, Perm, 614990. E-mail: mr.bond1995@mail.ru

Krotova Elena Lvovna, Candidate of Physical and Mathematical Sciences, Associate Professor of the Department of Higher Mathematics PNIPU, 29, Komsomolsky prospekt, Perm , 614990. E-mail: lenkakrotova@yandex.ru

УДК 004.056 Вестник УрФО № 2(20) / 2016, стр. 33–38

Соколов А. Н., Лужнов В. С.

СПЕЦИАЛИЗИРОВАННЫЕ ИНСТРУМЕНТЫ АВТОМАТИЗИРОВАННОГО АНАЛИЗА ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

В работе рассмотрена проблема анализа защищенности автоматизированных систем, освещена нормативная и методическая база в области аудита, аттестации и оценки информационной безопасности таких систем. Выполнен обзор рынка программных средств, реализующих на практике методики анализа защищенности, рассмотрены основные актуальные проблемы средств анализа защищенности и возможные перспективы их развития. На основе проведенного анализа и разработанного математического аппарата сформулирован алгоритм проведения в полуавтоматическом режиме анализа защищенности корпоративных автоматизированных систем. Преимущество предложенного алгоритма заключается в возможности проводить анализ защищенности автоматизированных систем на базе операционных систем Windows и UNIX с применением принципиально новой методологии определения уязвимостей и способов их устранения.

Ключевые слова: *информационная безопасность, автоматизированные системы, безопасность автоматизированных систем, анализ защищенности автоматизированных систем, аудит безопасности, атаки на информационные ресурсы, уязвимости системного программного обеспечения*

N. Sokolov, V. S. Luznov

SPECIALIZED TOOLS FOR AUTOMATED ANALYSIS OF INFORMATION SYSTEMS SECURITY

The paper considers the problem of security analysis of automated systems, illuminated by the regulatory and methodological framework in the field of audit, appraisal and evaluation of information security of such systems. Made a review of the software market, realizing in practice the techniques of security analysis, analyzed the basic topical problems of security analysis tools and possible prospects for their development. Developed an algorithm of the semi-automatic analysis of security of corporate automated systems, based on analysis of current software and developed mathematic model. The advantage of the proposed algorithm is the ability to analyze the security of automated systems based on Windows and UNIX

operating systems using a new methodology for determining and resection vulnerabilities of automated systems.

Keywords: *information security, automated systems, security, specialized software, security automation systems, security analysis of automated systems, security audit, attacks on information resources, the vulnerabilities of the system software.*

Тенденции развития систем автоматизации в настоящее время движутся в направлении создания таких систем, которые способны выполнять заданные функции или процедуры без участия человека (автоматических систем). Однако присутствие в решаемых задачах эвристических или сложно программируемых процедур объясняет широкое распространение полуавтоматических систем, так называемых автоматизированных систем [1]. Широкое распространение таких систем, их интенсивная интеграция в деятельность большинства государственных и коммерческих организаций приводит к тому, что от полноценного, стабильного и надежного функционирования автоматизированных систем, как государственных, так и коммерческих, напрямую зависит качество и результат всех процессов, происходящих в указанных организациях.

Одной из приоритетных задач при разработке автоматизированных систем является обеспечение их комплексной безопасности. В связи с этим к автоматизированным системам должны предъявляться особые требования по качественной и адекватной оценке степени защищенности всех процессов, протекающих в системе, оценке эффективности применяемых мер защиты информации, выявлению потенциальных уязвимостей в инструментах и средствах, т.е. по проведению полноценного анализа защищенности всей автоматизированной системы в целом. Под защищенностью автоматизированной системы здесь понимается степень адекватности реализованных в ней механизмов защиты информации существующим в данной среде функционирования рискам, связанным с осуществлением угроз безопасности информации [2].

С учетом сложности и комплексности как самих процессов, так и применяемых мер защиты, процесс анализа защищенности без применения специализированных средств аудита, аттестации и обследования безопасности является на практике сложно осуществимым. В предложенной работе рассмотрены основные средства и инструменты, специально разработанные и предназначенные для проведения комплексного анализа защищенности автоматизированных систем, проблемы и перспективы их развития и использования.

Проведение мероприятий по организации защиты информации в автоматизированных системах и анализу степени эффективности этой защиты должно происходить в соответствии с принятыми в отрасли нормативными и методическими документами, в силу ценности защищаемой информации и объема потенциального ущерба от реализации в отношении нее тех или иных угроз. На международном уровне такими документами являются:

• общие критерии оценки безопасности ИТ (The Common Criteria for Information Technology Security Evaluation/ISO 15408). Стандарт содержит два основных вида требований безопасности: функциональные, предъявляемые к функциям безопасности и реализующим их механизмам, и требования доверия, предъявляемые к технологии и процессу разработки и эксплуатации;

• информационные технологии – Технологии безопасности – Практические правила менеджмента информационной безопасности (Information technology – Security techniques – Code of practice for information security management/ISO/IEC 17799). Стандарт предоставляет лучшие практические советы по менеджменту информационной безопасности для тех, кто отвечает за создание, реализацию или обслуживание систем менеджмента информационной безопасности.

В Российской Федерации к таким нормативным и методическим документам относятся:

• ГОСТ Р 51583 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении»;

• Руководящий документ (РД) «Положение по аттестации объектов информатизации по требованиям безопасности информации» (Утверждено Председателем Гостехкомиссии России 25.11.1994 г.);

• РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация АС и требования к защите информации» (1997);

• «Положение о сертификации средств защиты информации по требованиям безопасности информации» (Постановление Правительства РФ № 608, 1995 г.);

• РД «Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации» (1992 г.);

• РД «Концепция защиты средств вычислительной техники от НСД к информации» (1992 г.);

• РД «Защита от НСД к информации. Термины и определения» (1992 г.);

• РД «Средства вычислительной техники. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации» (1997 г.);

• РД «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (1999 г.).

Практической реализацией требований перечисленных документов являются специализированные программы и программные комплексы, которые, опираясь на критерии и параметры нормативов, предназначены для формирования качественной оценки защищенности автоматизированных систем.

На сегодняшний день подавляющее большинство программного обеспечения в сфере анализа защищенности вычислительных систем разрабатывается и распространяется за рубежом. Наиболее популярными программными средствами [2,3] являются:

• Windows Security Scoring Tool (поставляемое для операционных систем семейства Windows NT средство анализа локальных политик безопасности. Позволяет осуществлять проверку соответствия настроек ОС MS Windows минимальному набору требований безопасности, определяющих базовый уровень защищенности, который в общем случае является достаточным для коммерческих систем.);

• Security Configuration and Analysis Snap-In (стандартное средство операционной системы Windows для осуществления анализа и настройки параметров безопасности);

• NetRecon (сетевой сканер. Является инструментом администратора безопасности, предназначенным для исследования структуры сетей и 123 сетевых сервисов и анализа защищенности сетевых сред. NetRecon позволяет осуществлять поиск уязвимостей в сетевых сервисах, ОС, МЭ, маршрутизаторах и других сетевых компонентах);

• NESSUS (сетевой сканер. Предназначен для автоматического поиска известных изъянов в защите информационных систем. Способен обнаружить наиболее часто встречающиеся виды уязвимостей: наличие уязвимых версий служб или доменов, ошибки в конфигурации (например, отсутствие необходимости авторизации на SMTP-сервере), наличие паролей по умолчанию, пустых, или слабых паролей);

• Enterprise Security Manager (автоматизированная система управления безопасностью предприятия);

• SAFEsuite (программные средства компании ISS (Internet Security Systems Inc.), предназначенные для анализа защищенности сетевых сервисов и протоколов Internet Scanner; операционных систем System Security Scanner; баз данных Database Scanner; обнаружения атак на сегменты и узлы сети RealSecure; поддержки принятия решения SAFEsuite Decisions).

На отечественном рынке в ходе его обзорного анализа среди всех представленных программных средств можно выделить программный комплекс «Сканер-ВС» [4] от разработчика «НПО Эшелон». Данный программный комплекс представляет собой дистрибутив операционной системы семейства GNU\Linux с предустановленным набором программного обеспечения для анализа отдельных аспектов защищенности автоматизированных систем5, прошедший сертификацию ФСТЭК России и Министерства Обороны6. К его основным функциям относятся: определение топологии и инвентаризация ресурсов сети, поиск уязвимостей, локальный и сетевой аудит стойкости паролей, поиск остаточной информации на жестком диске, перехват и анализ сетевого трафика, аудит ПО и аппаратной конфигурации, контроль целостности, аудит WI-FI сетей, модуль гарантированной очистки информации.

Исходя из перечисленных выше фактов, можно сформулировать следующие актуальные проблемы в области программных средств анализа защищенности автоматизированных систем на отечественном рынке:

• нормативно-методическая база требует определенной актуализации;

• отсутствуют утвержденные уполномоченными органами методики анализа защищенности автоматизированных систем;

• малый объем рынка комплексных программных средств анализа защищенности;

• разобщенность действующих в отрасли стандартов и подходов к оценке защищенности автоматизированных систем;

• не полностью реализуемый потенциал разработчиков по заполнению рынка актуальными программными продуктами.

На пути решения перечисленных проблемных вопросов поставлена задача разработки комплексной методики анализа защищенности автоматизированных систем и ее практическая реализация в виде программного комплекса, способного учесть наиболее полные и актуальные мировые и отечественные практики в области обеспечения информационной безопасности автоматизированных систем. Методика базируется на математическом аппарате, который может быть реализован в виде ряда программных алгоритмов.

Математическая модель программного комплекса по анализу атак на информационные ресурсы автоматизированной системы [7] может быть представлена в виде графа $G = <L,E>$, где L – множество вершин графа, а $E \subset L^2$ – множество дуг графа. Для графа G определено отношение $T \in \{E \times W\}$, которое каждой дуге из множества E ставит в соответствие один или более элементов отношения W.

Предлагаемая модель атак на информационные ресурсы в своей основе состоит из трех базовых множеств: V – множества уязвимостей информационных ресурсов автоматизированной системы, A – множества способов реализации атак на информационные ресурсы, C – множества последствий реализации атак на информационные ресурсы. Основные положения рассмотренной модели приведены в [8].

Для описания связей, существующих между элементами множеств A, V и C, необходимо определить n-арное алгебраическое отношение (тернарное при $n = 3$) W на множестве:

$$W = A \times V \times C$$

Тогда элемент (a, v, c), принадлежащий отношению W, где $a \in A$, $v \in V$, $c \in C$, в рамках модели представляет собой логическую структуру вида «Атака на информационные ресурсы, которая реализуется способом a через эксплуатацию уязвимости v, приводящая к последствию c».

Использование отношения T позволяет интерпретировать каждую дугу графа G как один из типов моделируемой атаки на информационные ресурсы автоматизированной системы. При этом в отношении T одной дуге $e \in E$ может соответствовать одновременно несколько элементов множества W только при условии, что эти элементы обозначают атаки, приводящие к одним и тем же последствиям, т. е.:

$$(\forall e \in E), (\forall w' \in W), (\forall w'' \in W)\ \exists\ (e,w') \in T,$$
$$\exists\,(e,w'') \in T \leftrightarrow c' = c'',$$

где $w' = (a', v', c')$, $w'' = (a'', v'', c'')$ - элементы, принадлежащие множеству W, a' и a'' - способы реализации атак, v' и v'' - уязвимости, c' и c'' - последствия реализации атак.

В каждую вершину графа G может входить одновременно несколько дуг только при условии, что в отношении T каждой такой дуге соответствуют элементы множества W, описывающие атаки на информационные ресурсы автоматизированной системы, которые приводят к одинаковым последствиям. Таким образом, вершины графа G могут объединять различные этапы атаки на информационные ресурсы, приводящие к идентичным последствиям.

Пример описанного графа G приведен на рис. 1.

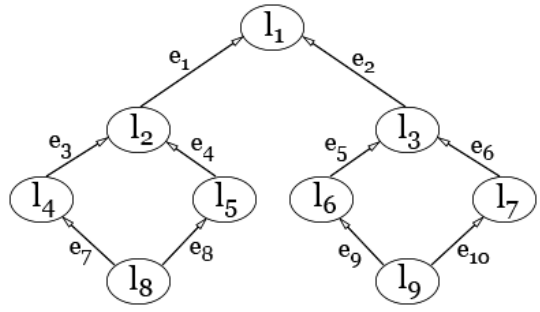

Рис. 1. Пример графа

На рис. 1: $l_1 \ldots l_9$ - вершины графа G, $e_1 \ldots e_{10}$ – дуги графа G. К графу применимо отношение T:

$$T = \{(e_1, (a_1, v_2, c_1)), (e_2, (a_2, v_1, c_1)),$$
$$(e_3, (a_2, v_1, c_2)), (e_4, (a_3, v_4, c_2)),$$
$$(e_5, (a_4, v_3, c_3)), (e_6, (a_5, v_5, c_3)),$$
$$(e_7, (a_5, v_6, c_4)), (e_8, (a_6, v_7, c_5)),$$
$$(e_9, (a_7, v_7, c_6)), (e_{10}, (a_8, v_3, c_7))\}$$

Описанная математическая модель атак на информационные ресурсы автоматизированных систем может использоваться для реализации на ее основе алгоритмов и, как следствие, программного обеспечения, позволяющего проводить анализ защищенности автоматизированных систем.

Примером такого алгоритма анализа защищенности может выступать следующий набор инструкций:

1. Для построения модели атак на информационные ресурсы составляются списки уязвимостей, способов реализации угроз и последствий от их реализации. Данные списки выступают основой для формирования множеств V, A, C.

2. Исходя из условий $0 < |A_i| < |A|, 0 < |V_j| < |V|, 0 < |C_j| < |C|, 0 < |A_k| < |A|$ и $W = A \times V \times C$ формируется множество всех возможных комбинаций из элементов множеств V, A, C.

3. Полученное множество подвергается фильтрации для исключения из него элементов, не соответствующих тернарному отношению $W = A \times V \times C$.

4. По результату фильтрации формируется множество W', содержащее в себе возможные и невозможные элементы-сочетания (a_i, v_j ,c_k). Для исключения из W' элементов, описывающих невозможный сценарий атаки, проводится второй этап фильтрации. Для его реализации формируются множества элементов (a,v), (a,c), (v,c), описывающие невозможные сочетания атак и уязвимостей, атак и последствий, уязвимостей и последствий соответственно.

5. На основе сформированных множеств множество W' фильтруется до состояния W, пригодного для построения модели атак.

На основе множества W строится граф $G = < L,E >$, путем формирования множества $T \in \{E \times W\}$ с учетом правила, что в отношении T одной дуге $e \in E$ может соответствовать одновременно несколько элементов множества W только при условии, что эти элементы обозначают атаки, приводящие к одним и тем же последствиям.

6. В результате множество T содержит в себе все возможные сценарии проведения атак на информационные ресурсы. Для реализации анализа защищенности каждому из последствий множества C задается вес r, прямо пропорциональный ущербу ресурсам системы от наступления последствия, такой, что $0 < r_i < 1$ и $\sum_1^i r_i = 1$, т. е. каждое последствие имеет вес, отличный от нуля, при этом суммарный вес всех последствий не превышает 1.

Приведенный алгоритм может быть формализован в виде схемы по ГОСТ 19.701-90 в виде схемы алгоритма (рис. 2).

Описанный алгоритм на момент проведения данного анализа находится на стадии реализации в виде прикладного программного обеспечения для операционных систем семейства Windows и UNIX, разрабатываемый на языке C++ для обеспечения эффективной скорости работы и необходимого уровня кроссплатформенного переноса программного кода. С учетом проведенного анализа рынка описанный в работе алгоритм представляется перспективным направлением разработок, способным обеспечить компенсацию основных узких моментов функционирования существующих программных средств.

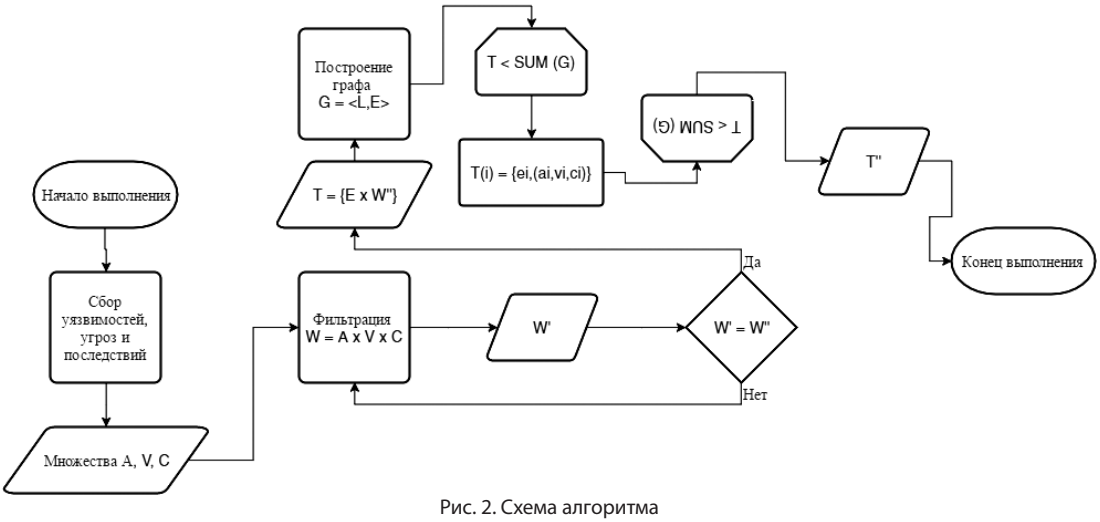

Рис. 2. Схема алгоритма

Примечания

1. Капустин, Н. М. Автоматизация производственных процессов в машиностроении: Учеб. для втузов / Под ред. Н. М. Капустина. – М.: Высшая школа, 2004. – 415 с.

2. Астахов А. Анализ защищенности корпоративных автоматизированных систем. / А. Астахов. // Информационный бюллетень Jet Info №7 (110)/2002. – Режим доступа: http://www.jetinfo.ru/Sites/new/Uploads/2002_7.DF9C812FFBD9496BAE9694E27F2D9D1D.pdf, свободный. – Загл. с экрана.

3. Суханов А.В. Автоматизированные средства анализа защищенности информационных систем. / А.В. Суханов. // Журнал научных публикаций аспирантов и докторантов, 2008 – Режим доступа: http://www.jurnal.org/ articles/2008/inf31.html, свободный. – Загл. с экрана.

4. Средство анализа защищенности «Сканер-ВС». / Электрон. дан. – М.: ЗАО «НПО Эшелон», 2012. – Режим доступа: http://scaner–vs.ru/, свободный. – Загл. с экрана.

5. Программный комплекс «Средство анализа защищенности «Сканер- ВС». Описание программы. / Электрон. дан. – М.: ЗАО «НПО Эшелон», 2012. – Режим доступа: http://scaner-vs.ru/data/description_sca.pdf, свободный. – Загл. с экрана.

6. Разработки НПО «Эшелон». Сканер-ВС. / Электрон. дан. – М.: ЗАО «НПО Эшелон», 2014. – Режим доступа: http://www.npo-echelon.ru/ production/65/4291, свободный. – Загл. с экрана.

7. Лужнов В.С., Соколов А.Н. Анализ защищенности корпоративных автоматизированных систем на основе модели атак на информационные ресурсы / В.С. Лужнов, А.Н. Соколов. I Международная научно–техническая конференция «Вопросы кибербезопасности, моделирования и обработки информации в современных социотехнических системах «Информ–2015»: сборник трудов. – Курск: Изд–во КГУ, 2015

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

Лужнов Василий Сергеевич, аспирант, ассистент кафедры «Безопасность информационных систем», Южно-Уральский государственный университет. E-mail: ua9stz@gmail.com.

Alexander Sokolov, a. M. N., Associate Professor, Head. the Department of Information Systems Security "South Ural State University", Chelyabinsk. E-mail: ANSokolov@inbox.ru

Vasiliy Luzhnov, Graduate Student, Assistant of the Department «Information Systems Security», South Ural State University, Chelyabinsk, Russian Federation. E-mail: ua9stz@gmail.com

УДК УДК 366.54(470) + 338.439:366.54

Вестник УрФО № 2(20) / 2016, стр. 39–46

Вожакин Т. А.

СИСТЕМА МЕР ОТВЕТСТВЕННОСТИ ЗА НЕПРАВОМЕРНОЕ ИСПОЛЬЗОВАНИЕ ИНСАЙДЕРСКОЙ ИНФОРМАЦИИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

В статье анализируется система мер ответственности за неправомерное использование инсайдерской информации в РФ. Рассматриваются проблемы реализации механизма привлечения к ответственности за неправомерное использование инсайдерской информации. Делается вывод, что существующий порядок привлечения нарушителей – инсайдеров к ответственности за неправомерное использование инсайдерской информации является неэффективным и не отвечает целям и задачам Закона № 224-ФЗ. Вносятся предложения по улучшению сложившейся ситуации в области ответственности за неправомерное использование инсайдерской информации.

Ключевые слова: *инсайдерская информация, неправомерное использование инсайдерской информации, ответственность за неправомерное использование инсайдерской информации, механизм привлечения к ответственности за неправомерное использование инсайдерской информации.*

Vozhakin T. A.

THE SYSTEM OF MEASURES OF RESPONSIBILITY FOR ILLEGAL USE OF INSIDER INFORMATION IN RUSSIA

The article analyzes the system of measures of responsibility for illegal use of insider information in Russia. Examines the problems of realization of mechanism of bringing liable for illegal use of insider information. It is concluded that the existing procedure for bringing offend-

ers – insiders liable for illegal use of insider information is inefficient and does not meet the goals and objectives of the Law No. 224-FZ. Proposes for improvement of the current situation in the field of bringing liable for illegal use of insider information.

Keywords: *insider information, illegal use of insider information, responsibility for illegal use of insider information, mechanism of bringing liable for illegal use of insider information.*

В настоящее время большое количество изданий, которые зани-маются публикацией материалов об информационной безопасности, привлекают внимание своих читателей сообщениями и аналити¬ческими статьями о том, что большую угрозу рынку ценных бумаг представляют сделки, совершенные с использованием инсайдерской информации. По оценкам экспертов сейчас более 50 % сделок от общего количества совершаются с использованием инсайдерской информации [1].

Понятие инсайдерской торговли в российском законодательстве, как и во многих законодательствах зарубежных стран, изначально, отсутствует. Законодатель употребляет термин «неправомерное использование инсайдерской информации», однако не раскрывает его значение, что, несомненно, вызовет сложности в правоприменении, насколько можно судить по практике зарубежных стран.

В п. 1 ст. 6 Федерального закона «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком» [2] к неправомерному использованию инсайдерской информации относит следующее: 1) совершение операций с финансовыми инструментами, иностранной валютой, товарами на основе инсайдерской информации; 2) неправомерная передача инсайдерской информации третьим лицам; 3) дача рекомендаций на совершение сделок с финансовыми инструментами, иностранной валютой, товарами или склонение к совершению этих сделок любым способом.

Значительным шагом в борьбе с неправомерным использованием инсайдерской информации и манипулированием рынком стал Федеральный закон № 241-ФЗ [3] от 30 октября 2009 г., который с 14 ноября 2009 г. ввел уголовную ответственность за новые составы преступлений на рынке ценных бумаг. Среди введенных в УК РФ новых составов преступлений необходимо отдельно выделить ст. 185.3 УК РФ «Манипулирование ценами на рынке ценных бумаг». Под это понятие подпадают действия, в результате которых повышается, понижается и поддерживается цена ценных бумаг, спрос на них или объем торгов ими. Ответственность манипуляторов по новому законодательству предусматривает штраф от 300 тыс. руб. до 4-х лет лишения свободы. До введения этой статьи в Уголовный кодекс за манипулирование ценами на рынке ценных бумаг была предусмотрена всего лишь декларативная административная ответственность, которая применялась редко.

Также отдельно стоит выделить ст. 185.6 УК РФ «Неправомерное использование инсайдерской информации». Под этот состав подпадает умышленное использование инсайдерской информации для осуществления операций с финансовыми инструментами, иностранной валютой и (или) товарами, к которым относится такая информация, за свой счет или за счет третьего лица, а равно умышленное использование инсайдерской информации путем дачи рекомендаций третьим лицам, обязывания или побуждения их иным образом к приобретению или продаже финансовых инструментов, иностранной валюты и (или) товаров, если такое использование причинило крупный ущерб гражданам, организациям или государству либо сопряжено с извлечением дохода или избежанием убытков в крупном размере. Ответственность по этой статье предусматривает штраф от 300 тыс. руб. до 4-х лет лишения свободы. Данная статья содержит примечание о крупном ущербе, в котором такими убытками признается ущерб, доход, убытки в сумме, превышающей два с половиной миллиона рублей.

Учёные сходятся во мнении о том, что вина в случае осуществления, в частности, инсайдерской торговли для привлечения именно к уголовной ответственности может быть только в форме прямого умысла. Именно поэтому издаются и уточняются списки инсайдеров, статьёй 6 224-ФЗ устанавливается запрет неправомерного использования инсайдерской информации.

Представляется, что не только наличие или отсутствие крупного ущерба, причинённого гражданам, организациям и государству, должно быть основанием для разграничения видов ответственности за данное деяние. Необходимо чётко выделять форму вины, поскольку в противном случае придет-

ся привлекать к ответственности даже таксистов, случайно услышавших о заключении сделки – классический пример в американской научной литературе [4].

Федеральный закон № 241-ФЗ от 30 октября 2009 г. также ввел административную ответственность за новые составы правонарушений на рынке ценных бумаг. Законом были введены новые составы административных правонарушений в КоАП РФ [5].

Среди них ст. 15.21 КоАП РФ «Неправомерное использование инсайдерской информации». Ответственность предусматривает штраф на граждан от 3 тыс. руб. до 5-ти тыс. руб., на должностных лиц – от 30 тыс. руб. до 50 тыс. руб. или дисквалификацию на срок до одного года до двух лет, на юридических лиц – в размере суммы излишнего дохода либо суммы убытков, которых гражданин, должностное лицо или юридическое лицо избежали в результате неправомерного использования инсайдерской информации, но не менее семисот тысяч рублей. В примечании статьи указывается, что излишним доходом признается доход, определяемый как разница между доходом, который был получен в результате незаконных действий, и доходом, который сформировался бы без учета незаконных действий, предусмотренных ст. 15.21 КоАП РФ.

Статья 15.30 КоАП РФ «Манипулирование рынком» предусматривает идентичную ответственность, как в ст. 15.21 КоАП РФ.

Статья 15.35 КоАП РФ «Нарушение требований законодательства о противодействии неправомерному использованию инсайдерской информации и манипулированию рынком».

Пункт 1 статьи 15.35 устанавливает неисполнение или ненадлежащее исполнение лицом, обязанным раскрывать инсайдерскую информацию, обязанности по раскрытию инсайдерской информации, за исключением случаев, предусмотренных ст. 15.19 КоАП РФ «Нарушение требований законодательства, касающихся представления и раскрытия информации на финансовых рынках». Ответственность предусматривает наложение штрафа на должностных лиц в размере от 20 тыс. руб. до 30 тыс. руб. или дисквалификацию на срок до одного года, на юридических лиц – от 500 тыс. руб. до 700 тыс. руб.

Пункт 2 статьи 15.35 устанавливает неисполнение или ненадлежащее исполнение лицами, обязанными вести список инсайдеров, обязанностей по ведению списка инсайдеров и уведомлению лиц, включенных в список инсайдеров. Ответственность предусматривает наложение штрафа на должностных лиц в размере от 20 тыс. руб. до 30 тыс. руб., на юридических лиц - от 300 тыс. руб. до 500 тыс.руб.

Пункт 3 статьи 15.35 предусматривает неисполнение или ненадлежащее исполнение инсайдерами обязанности по уведомлению Банка России об осуществленных ими операциях с финансовыми инструментами, иностранной валютой и (или) товарами. Ответственность – наложение штрафа на граждан в размере от 3-х тыс. руб. до 5 тыс.руб., на должностных лиц – в размере от 20 тыс.руб. до 30 тыс. руб., на юридических лиц – в размере от 300 тыс.руб. до 500 тыс.руб.

И наконец, п. 4 ст. 15.35 содержит указание на неисполнение или ненадлежащее исполнение лицом обязанностей по принятию установленных законодательством мер, направленных на предотвращение, выявление и пресечение злоупотреблений на финансовых и товарных рынках. Ответственность предусматривает наложение штрафа на должностных лиц в размере от 20 тыс. руб. до 30 тыс. руб. или дисквалификацию на срок до одного года, на юридических лиц – наложение штрафа в размере от 300 тыс.руб. до 700 тыс. руб.

Указанные составы могут применяться в том случае, если действия лица, признаваемого виновным, не содержат в себе уголовно наказуемого действия.

Очень слабо развиты положения о гражданско-правовой ответственности за незаконное использование инсайдерской информации, но все же они есть.

В статье 7 Федерального закона № 241-ФЗ от 30 октября 2009 г «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации» содержатся следующие сведения о гражданско-правовых последствиях в случае манипулирования рынком и неправомерного использования инсайдерской информации:

1) лица, которым в результате неправомерного использования инсайдерской информации и (или) манипулирования рынком причинены убытки, вправе требовать их возмещение от лиц, в результате действий которых были причинены такие убытки (пункт 7 статьи 7);

2) совершение операций, сопровождающихся использованием инсайдерской информации и (или) являющихся манипулированием рынком, не является основанием для признания их недействительными (пункт 8 статьи 7).

Данная норма позволяет говорить о том, что ст. 168 ГК РФ не применяется по отношению к сделкам, которые совершаются при манипулировании рынком или с использованием инсайдерской информации.

В настоящий момент на практике при привлечении инсайдеров к ответственности за нарушение Закона № 224-ФЗ (в т. ч. за неправомерное использование инсайдерской информации) возникают существенные проблемы. Прежде всего, они связаны с большими сложностями, с которыми сталкивается уполномоченный орган по финансовым рынкам (далее – УОФР) (до 1 сентября 2013 г. таким уполномоченным органом являлась ФСФР. В соответствии с Указом Президента РФ от 25.07.2013 № 645 ФСФР была упразднена, а ее функции переданы к Банку России, а именно службе Банка России по финансовым рынкам) при попытке запросить сведения, необходимые для расследования случаев неправомерного использования инсайдерской информации (это могут быть и детализация телефонных звонков, и переписка по электронной почте).

В результате за время действия Закона № 224-ФЗ, вступившего в силу в начале 2011 г., инсайдеры ни разу не привлекались к ответственности за неправомерное использование инсайдерской информации.

УОФР несколько раз, отследив сделки (заявки), имеющие признаки неправомерного использования инсайдерской информации и (или) манипулирования рынком, совершаемые инсайдерами на финансовом рынке, приходила к предварительному выводу о наличии в них признаков неправомерного использования инсайдерской информации и пыталась инициировать процесс сбора соответствующих доказательств с целью привлечения нарушителей к административной ответственности по ст. 15.21 КоАП РФ.

Однако каждый раз события развивались фактически по одному и тому же сценарию.

При проведении камеральной проверки в отношении неправомерного использования инсайдерской информации УОФР направляла в адрес различных организаций (интернет-провайдеров, операторов сотовой связи, обслуживающих лиц, подозреваемых в неправомерном использовании ИИ, эмитентов и др.) предписания о предоставлении необходимых ей сведений, таких как данных, указанных определенным лицом (пользователем) при регистрации учетной записи в сервисе электронной почты; IP-адресов, с которых, по мнению УОФР, совершались действия, связанные с неправомерным использованием инсайдерской информации; адресов электронной почты, с которых, по мнению УОФР, предположительно отправлялись сообщения, связанные с неправомерным использованием инсайдерской информации; детализации телефонных звонков, сделанных предполагаемыми нарушителями – инсайдерами с определенного номера в период совершения нестандартных сделок.

Однако адресаты либо сразу оспаривали соответствующее предписание УОФР как незаконное (Решение Арбитражного суда города Москвы от 12 ноября 2012 года и Постановление Девятого арбитражного апелляционного суда от 27 марта 2013 года № 09АП-6488/2013 по делу № А40-132583/12-119-12686, где в удовлетворении заявления о признании недействительным предписания о представлении документов отказано правомерно, поскольку запрошенная информация необходима органу по финансовым рынкам для реализации возложенных на него обязанностей по контролю за соблюдением законодательства РФ о противодействии неправомерному использованию инсайдерской информации и манипулированию рынком) либо под различными предлогами отказывались предоставлять запрашиваемые сведения в надлежащие сроки. Одним из самых популярных «оправданий» служила ссылка на нарушение законодательства о персональных данных (Решение Арбитражного суда города Москвы от 12 ноября 2012 года и Постановление Девятого арбитражного апелляционного суда от 27 марта 2013 года № 09АП-6488/2013 по делу № А40-132583/12-119-1268), тайну переписки (Решение Арбитражного суда города Москвы от 26 июля 2013 года по делу № А40-56844/2013 [7], в котором заявление о признании незаконным и отмене постановления о привлечении к административной ответственности по ч. 9 ст. 19.5 КоАП РФ удовлетворено, так как административным органом не установлено событие и состав правонарушения, а также вина заявителя в связи с невозможностью исполне-

ния предписания без нарушения требований законодательства о тайне связи) и тайну телефонных переговоров (Решение Арбитражного суда города Москвы от 12 июля 2013 года по делу № А40-56142/2013 [8], в котором в удовлетворении заявления о признании незаконным и отмене постановления о привлечении к административной ответственности по ч. 9 ст. 19.5 КоАП РФ отказано, поскольку наличие состава административного правонарушения в действиях заявителя подтверждено материалами дела, сроки и порядок привлечения общества к административной ответственности административным органом соблюдены).

Не получив ответа на запрос, УОФР привлекала указанные организации к административной ответственности по ч. 9 ст. 19.5 КоАП РФ за невыполнение в установленный срок ее законного предписания и налагала на нарушителей крупные штрафы.

Однако те обжаловали указанные предписания и постановления УОФР в суд. В трех случаях из четырех суды пришли к выводу об их правомерности (Решение Арбитражного суда города Москвы от 7 августа 2012 года и Постановление Девятого арбитражного апелляционного суда от 4 октября 2012 года № 09АП-27522/2012 по делу № А40-89126/12-92-814 [9], где в удовлетворении заявления об отмене постановления о привлечении к административной ответственности за невыполнение в установленный срок законного предписания органа исполнительной власти в области финансовых рынков отказано правомерно, поскольку состав вменяемого заявителю административного правонарушения доказан материалами дела об административном правонарушении, процедура привлечения к административной ответственности соблюдена, Решение Арбитражного суда города Москвы от 12 ноября 2012 года и Постановление Девятого арбитражного апелляционного суда от 27 марта 2013 года № 09АП-6488/2013 по делу № А40-132583/12-119-1268 [10], в котором в удовлетворении заявления о признании недействительным предписания о представлении документов отказано правомерно, поскольку запрошенная информация необходима органу по финансовым рынкам для реализации возложенных на него обязанностей по контролю за соблюдением законодательства РФ о противодействии неправомерному использованию инсайдерской информации и манипулированию рынком, Решение Арбитражного суда города Москвы от 12 июля 2013 года по делу № А40-56142/2013 [11], где в удовлетворении заявления о признании незаконным и отмене постановления о привлечении к административной ответственности по ч. 9 ст. 19.5 КоАП РФ отказано, поскольку наличие состава административного правонарушения в действиях заявителя подтверждено материалами дела, сроки и порядок привлечения общества к административной ответственности административным органом соблюдены).

Только в одном деле суд пришел к выводу о неправомерности предписания УОФР, указав, что информация об адресах электронной почты, с которыми пользователь осуществлял переписку в период с 1 января 2012 г. до даты получения предписания, может быть предоставлена исключительно через доступ к информации, содержащейся непосредственно в сообщениях пользователя, которые относятся к тайне переписки и охраняются Конституцией РФ.

Однако, не углубляясь в вопросы правомерности предписаний УОФР в части их соответствия нормам законодательства о тайне переписки, телефонных переговоров и т. д., мы, тем не менее, на основании анализа упомянутых четырех судебных дел можем сделать вывод о том, что механизм привлечения к ответственности за неправомерное использование инсайдерской информации дает сбои уже на стадии сбора информации о предполагаемых правонарушениях, что резко снижает вероятность привлечения к ней инсайдеров.

В большинстве данных споров УОФР сумела доказать правомерность своих предписаний, однако ни в одном их случаев дело не продвинулось дальше стадии сбора возможных доказательств, равно как и ни в одном из них лица, подозреваемые в неправомерном использовании инсайдерской информации, не были в итоге привлечены к административной ответственности.

Причина описанных проблем кроется в том, что законодатель, предусматривая полномочия УОФР в области борьбы с инсайдом, в полной мере не учел спе¬цифики привлечения к ответственности за правонарушения, совершаемые на финансовых рынках.

Поскольку неправомерное использование инсайдерской информации имеет место при заключении сделок на финансовых рынках, то очевидно, что при совершении

данного нарушения инсайдеры используют все современные средства связи (мобильные телефоны, электронную почту и т. д.). Следовательно, расследование дел о неправомерном использовании инсайдерской информации будет неизбежно и неразрывно связано с необходимостью оперативного истребования различных сведений с ограниченным доступом (в т. ч. переписки по электронной почте, детализации телефонных звонков).

В таких условиях ключевую роль при расследовании случаев неправомерного использования ИИ играет слаженное взаимодействие УОФР с лицами, которые обладают сведениями об использовании инсайдерами средств связи и технической возможностью представить их по его запросу. К указанным лицам относятся, например, операторы сотовой связи и интернет-провайдеры, обслуживающие потенциальных нарушителей – инсайдеров.

В идеале УОФР при проведении камеральной проверки нестандартных сделок на предмет наличия в них признаков неправомерного использования инсайдерской информации должен максимально оперативно получать запрошенные им сведения, проводить «по горячим следам» проверку в полном объеме и уже по ее итогам привлекать инсайдеров к ответственности.

Операторы сотовой связи и интернет-провайдеры имеют техническую возможность оперативно представить в УОФР указанную информацию на осно¬вании соответствующего запроса. Однако, как следует из изученной практики, его адресат, получив соответствующее предписание, как правило, оказывается в патовой ситуации. С одной стороны, исполнение предписания может обернуться для него привлечением к ответственности (в т. ч. уголовной) за нарушение тайны переписки и телефонных переговоров, законодательства о персональных данных. С другой стороны, неисполнение предписания УОФР может повлечь административную ответственность по ч. 9 ст. 19.5 КоАП РФ. Все это является результатом того, что при принятии Закона № 224-ФЗ законодатель упустил из виду проблему соотнесения его норм, касающихся полномочий УОФР запрашивать у организаций необходимую информацию, и положений законодательства о тайне переписки и телефонных переговоров, защите персональных данных и т. д.

В итоге отсутствие четких норм в отношении сведений, которые УОФР вправе запрашивать с целью расследования случаев неправомерного использования ИИ, приводит к тому, что большинство адресатов предписаний предпочитают их не выполнять, тем самым лишая УОФР возможности оперативно получить необходимые данные и «блокируя» дальнейшее расследование.

Кроме того, следует отметить, что полномочия УОФР ограничены в вопросах, где требуется проведение оперативных мероприятий по сбору требуемой информации. В случае необходимости ее получения оперативным путем УОФР в соответствии с п. 7 ст. 14 Закона № 224-ФЗ обязан обратиться в компетентный орган внутренних дел, взаимодействие с которым будет осуще¬ствляться на основании совместного (межведомственного) нормативного правового акта МВД и УОФР (Банком России) о сотрудничестве и взаимодействии в целях пресечения неправомерно использования инсайдерской информации.

К настоящему моменту такой межведомственный нормативный правовой акт не принят, следовательно, УОФР не имеет реальной возможности «поймать» инсайдеров и манипуляторов «по горячим следам». В то же время любое промедление при расследовании случаев неправомерного использования инсайдерской информации чревато утратой доказательств их вины, которые предусмотрительные нарушители попросту успеют удалить (например, определенную часть переписки по электронной почте).

Как итог, мы имеем многочисленные дела, в которых оспаривается правомерность предписаний УОФР, и не имеем ни одного дела, закончившегося привлечением инсайдера к ответственности.

Чтобы исправить сложившееся положение необходимо внести несколько предложений по его улучшению:

Во-первых, необходимо прояснить вопрос в отношении сведений, которые вправе запрашивать УОФР, с учетом положений Конституции РФ и законодательства о тайне переписки и телефонных переговоров, защите персональных данных и т. п.

Данный вопрос может быть разрешен как на законодательном уровне, так и на уровне толкования положений Закона № 224-ФЗ высшими судами (в т. ч. КС РФ, поскольку анализ судебной практики свидетельствует о том, что рано или поздно он по-

лучит запрос либо жалобу о соответствии (несоответствии) норм Закона № 224-ФЗ ст. 23 Конституции РФ).

Представляется, что наиболее эффективным и разумным решением данной проблемы будет определение перечня сведений, которые вправе запрашивать УОФР в целях борьбы с неправомерным использованием инсайдерской информации, на основе его правоприменительной практики.

Во-вторых, для эффективного расследования дел о неправомерном использовании инсайдерской информации, необходим механизм максимально оперативного получения необходимых сведений и доказательств. Таким образом, должен быть разработан нормативный акт, предусматривающий механизм эффективного взаимодействия между УОФР и правоохранительными органами в ходе мероприятий по предотвращению, выявлению и пресечению фактов неправомерного использования инсайдерской информации и (или) манипулирования рынком.

При его разработке возможно использование опыта зарубежных стран, в частности, США, где расследование случаев неправомерного использования инсайдерской информации осуществляется Комиссией по ценным бумагам и биржам в тесном сотрудничестве с ФБР. Последнее на основании полученных от нее сведений участвует в оперативном сборе требуемых для расследования сведений и доказательств.

В нашей стране эту роль могла бы выполнять финансовая полиция, идея создания которой выдвигалась руководством СК РФ, но была отвергнута Президентом РФ, Правительством РФ, а также ведущими силовыми министерствами и ведомствами, которые посчитали это предложение преждевременным и требующим проработки.

В-третьих, после определения четкого перечня сведений, которые могут быть запрошены УОФР в целях борьбы с неправомерным использованием инсайдерской информации, целесообразно рассмотреть возможность ужесточения санкций за неисполнение его предписаний.

В частности, следует изучить возможность закрепления в КоАП РФ нового специального состава административного правонарушения – непредставление уполномоченному органу в области финансовых рынков сведений, необходимых для предотвращения, выявления и пресечения фактов неправомерного использования инсайдерской информации и (или) манипулирования рынком в установленные законом сроки, а также введения более жестких финансовых санкций за указанное правонарушение.

При этом санкции должны быть значительными по размеру, поскольку ныне действующий штраф, предусмотренный ч. 9 ст. 19.5 КоАП РФ за неисполнение предписаний УОФР (до 700 тыс. руб.), фактически позволяет нарушителям «откупаться» от него относительно небольшими суммами и таким образом не давать хода делам о привлечении к административной ответственности за неправомерное использование инсайдерской информации по ст. 15.21 КоАП РФ, которая предполагает более серьезный штраф (от 700 тыс. руб. для юридических лиц).

Существующий порядок привлечения нарушителей – инсайдеров к ответственности за неправомерное использование инсайдерской информации является неэффективным и не отвечает целям и задачам Закона № 224-ФЗ. В последнее время в деловой прессе все чаще появляются публикации, сообщавшие об обнаружении УОФР фактов неправомерного использования инсайдерской информации. Однако, по нашему мнению, до тех пор, пока хотя бы один инсайдер не понесет реального наказания по ст. 15.21 КоАП РФ, говорить как об эффективности правового механизма привлечения к ответственности за неправомерное использование инсайдерской информации, так и о сложившейся правоприменительной практике УОФР по данному вопросу преждевременно.

Примечания

1. Зверев, В. Некоторые комментарии к закону об инсайдерской информации / В. Зверев // Ценные бумаги. – 2009. – № 12 [Электронный ресурс] . URL: http://gaap.ru/articles/51141/(дата обращения 05.05.2014).

2. Федеральный закон от 27 июля 2010 г. № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации» // СЗ РФ. – 2010 – № 31. – Ст. 4193.

3. Федеральный закон «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации» от 30 октября 2009 г. № 241-ФЗ // СЗ РФ. – 2009. – № 44. – Ст. 5170.

4. Carlton W.D., Fischel D.R. The regulation of insider trading // An Economic analysis of the law: selected readings. Ed. by D.A. Wittman. Oxford: Blackwell Publishing, 2003.

5. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ // СЗ РФ. – 2002. – № 1 (ч. 1). – Ст. 1.

6. Постановление Девятого арбитражного апелляционного суда от 27 марта 2013 г. № 09АП-6488/2013 по делу № А40-132583/12-119-1268. Документ опубликован не был. СПС «Консультант» (дата обращения 05.05.2014)., Решение Арбитражного суда города Москвы от 12 ноября 2012 г. Документ опубликован не был. СПС «Консультант» (дата обращения 05.05.2014).

7. Решение Арбитражного суда города Москвы от 26 июля 2013 г. по делу № А40-56844/2013. Документ опубликован не был. СПС «Консультант» (дата обращения 05.05.2014).

8. Решение Арбитражного суда города Москвы от 12 июля 2013 г. по делу № А40-56142/2013. Документ опубликован не был. СПС «Консультант» (дата обращения 05.05.2014).

9. Постановление Девятого арбитражного апелляционного суда от 4 октября 2012 г. № 09АП-27522/2012 по делу № А40-89126/12-92-814. Документ опубликован не был. СПС «Консультант» (дата обращения 05.05.2014)., Решение Арбитражного суда города Москвы от 7 августа 2012 г. Документ опубликован не был. СПС «Консультант» (дата обращения 05.05.2014).

10. Постановление Девятого арбитражного апелляционного суда от 27 марта 2013 г. № 09АП-6488/2013 по делу № А40-132583/12-119-1268. Документ опубликован не был. СПС «Консультант» (дата обращения 05.05.2014).

11. Решение Арбитражного суда города Москвы от 12 июля 2013 г. по делу № А40-56142/2013. Документ опубликован не был. СПС «Консультант» (дата обращения 05.05.2014).

Вожакин Тимофей Александрович, аспирант кафедры конституционного и административного права юридического факультета Южно-Уральского государственного университета. 454004, г. Челябинск. ул. Университетская набережная, д.88. E-mail: vozhakin_ta@mail.ru

Vozhakin Timofey, postgraduate student of Constitutional and Administrative Law of the South Ural State University. Bld. 88, Universitetskaja naberezhnaja Str., Chelyabinsk, 454004. E-mail: vozhakin_ta@mail.ru

УДК 343. 353 Вестник УрФО № 2(20) / 2016, стр. 47–53

Волков Ю. В.

О ПОДХОДАХ ПОНИМАНИЯ «ТАЙНЫ СВЯЗИ»

В статье представлены основные подходы к вопросу «тайны связи». Общее количество исследований не отражает реальной потребности и значения данного вопроса. Основное течение в исследованиях представляет концепция тайны связи как составной части прав личности на приватность. Другим направлением в исследованиях является идея о происхождении тайны связи от служебной тайны. Одновременно высказывается мнение о том, что тайна связи должна быть классифицирована как профессиональная тайна. В статье рассмотрен состав нормы о тайне связи на основе классических представлениях о норме права (с гипотезой, диспозицией и санкцией). Одновременно представлены дополнения основной нормы и исключения из основного правила о тайне связи. Кроме перечисленных подходов рассмотрены разные варианты формирования тайны связи как правового режима. Режим тайны связи может быть сформирован как часть общего отраслевого режима (режима отрасли связи). Для практических целей правовой режим тайны связи может быть сформирован из множества базовых элементов информационной безопасности: организационных, технических и технологических.

Ключевые слова: *общение, право, почта, связь, секрет, тайна, телефон, телекоммуникации.*

Volkov Y.

ABOUT APPROACHES TO UNDERSTANDING "COMMUNICATIONS PRIVACY"

The article presents the main approaches to the question of "Communications Privacy". The total number of investigations does not reflect the real need and importance of this issue. The main trend in research is the concept of Communications Privacy as part of the Human Privacy Rights. Another area of research is the idea that the Communications Privacy is the part of official secrets. At the same time it expressed the view that the mystery of communication should be classified as a Trade Secret. The article describes the structure of the rules on Communications Privacy on the basis of classical conceptions of the rule of law (with the hypothesis, disposition and sanctions). At the same time presented the basic rules of additions and exceptions to the basic rule of the Communications Privacy. In addition to these approaches are considered different variants of formation of Communications Privacy as a Legal Regime. The Regime of Communications Privacy can be formed as part of the Legal Regime branch (Regime of the telecommunications industry). For practical purposes, the legal regime of the of Communications Privacy may be formed from basic elements of information security: organizational, technical and technological.

Keywords: *Communications Privacy, communications, mail privacy, law, secret, chat, post, telecommunications.*

Чем шире применяем мы современные средства связи, тем острее встаёт вопрос о сохранности отправленных сообщений, о тайне связи. Наиболее остро эта проблема воспринимается молодым поколением, как наиболее активными пользователями сетей, и в числе авторов, исследователей данной проблемы, начинающие авторы составляют большинство. Незначительный объем публикаций не отражает реальной актуальности вопроса. Полагаем, что в ближайшее десятилетие вопрос о тайне связи, о качестве защиты передаваемой информации, займёт одну из ведущих позиций в рейтингах правовых, технических, политических и социальных исследований.

I

Происхождение «тайны связи» как понятия и правового института — одна из наиболее популярных тем. Спектр мнений по поводу природы происхождения и принадлежности тайны связи весьма широк и содержит правовые концепции от частных до публично-правовых. Так, один из наиболее активных исследователей данного вопроса, Н. Ю. Рязанов придерживается преимущественно частно-правовой концепции, при этом констатирует «взаимопроникновение»[1] конституционных и частных начал в тайне связи. Развивая данную тему, он делает упор на термины, а именно: «учитывая, что слова «частное» и «личное» являются синонимами, мы обнаруживаем, что данная норма является скорее не определением, а перечислением прав». В результате автор приходит к выводу о том, что сложилось «историческое несоответствие между первоначальным толкованием права на тайну связи и современным развитием системы связи»[2]. Фактически он констатировал разрыв между техническим развитием и правовой рефлексией. Действительно, и конституционные основания, и естественные права имеют значение для формирования тайны связи. Что же касается источников тайны связи, то можно согласиться лишь частично. Однако имеет место и весьма дискуссионный момент. Длительное время (в советский период) разграничение *частного* и *личного*, как минимум на уровне теории права, было достаточно точным и не смешивалось. *Личное,* как принадлежность индивида в правовой и социальной сферах, не подлежит отчуждению, а *частное*, напротив, признак имущественного объекта преобладало в экономическом (и соответственно, правовом) обороте. Н. Ю. Рязанов данные понятия обозначил как синонимы. В итоге, тайна связи квалифицирована автором как объект в составе личных прав. Полагаем, что данное утверждение является неполной характеристикой.

Концепция личных прав, как основы тайны связи, имеет весьма авторитетного сторонника профессора Н. В. Витрука, позицию которого также необходимо учитывать. Он констатирует, что «в состав правового статуса личной свободы согласно Конституции РФ входят следующие конституционные права, свободы и законные интересы: <...> право каждого на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (ч. 2 ст. 23)»[3]. Это бесспорный аргумент. Действительно, согласно части 2 статьи 23 Конституции: «Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений»[4]. Данное право мы кратко именуем — тайна связи. Однако в Конституции ничего не говорится о субъектах которые обеспечивают тайну связи, об обязанностях по поводу защиты тайны связи и т. д. Данное положение, не оспаривая его связь с личными правами, можно именовать как гипотезу нормы права, как базовое основание. Положения о тайне связи содержат также отдельные законы. В части 1-ой статьи 63 Федерального закона «О связи» (далее ЗОС) содержатся общие положения о тайне связи[5], которые практически полностью повторяют соответствующие положения Конституции РФ. Право отправителя на тайну связи закреплено в статье 62 ЗОС, обязанность оператора соблюдать тайну связи закреплено в пункте 2-ом статьи 63 ЗОС. Общие процедурные моменты обеспечения тайны связи содержатся в пунктах 3, 4 статьи 63 названного закона. Тайна связи в почтовой сфере закреплена специальным законом «О почтовой связи»[6]. Каждое почтовое сообщение содержит сведения об отправителе и получателе. Эти сведения и само сообщение являются объектами защиты тайны связи. Такая особенность обуславливает более обширный режим тайны связи применительно к почтовым отправлениям. Защищать (в том числе вооружённым путём) необходимо не только все отправления, но и всю инфраструктуру почтовой связи, поскольку сами отправления имеют материальную ценность и являются объектами страхования. Телекоммуникационные линии общего пользования,

как правило, не снабжаются вооружённой охраной. По той причине важной составляющей описания тайны связи является статья 20 Обеспечение сохранности почтовых отправлений и денежных средств Федерального закона «О почтовой связи». Ответственность за нарушение тайны связи (нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений) предусмотрена статьёй 138 УК РФ[7].

Ещё один сторонник личностного подхода к природе тайны связи Н. В. Федотова. В результате весьма объемного исследования автор приходит к выводу о том, что «тайна личной переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений человека лежит в основе интереса обеспечения неприкосновенности частной жизни, на которую посягает не только преступление, состав которого содержится в частях 1 и 2 ст. 138 УК РФ, а целый ряд преступлений против конституционных и иных прав человека»[8]. Иными словами, автор полагает, что не права личности является основой тайны связи, а тайна связи основа прав личности. Но из анализа запрещающих норм уголовного права весьма сложно определить кто, собственно, кроме оператора обязан защищать тайну связи. А сам пользователь услуг связи не несёт такой обязанности? А почему нет? Например, собственник имущества в соответствии со статьёй 210 Гражданского кодекса РФ «несет бремя содержания принадлежащего ему имущества»[9]. Почему пользователь услуг связи не обременён аналогичной обязанностью? Почему бремя по защите личной тайны конвертированной в тайну связи должен нести преимущественно оператор связи? Получается, что оператор предпринимает все возможные меры по защите тайны связи, а пользователь может читать письма, развевающиеся на ветру, или бродить по городу не прикрывая экран абонентского терминала (смартфона, планшета), годами не менять пароли к аккаунтам социальных сетей.

Перечисленные положения законодательства позволяют утверждать о формировании базовой нормы, общеобязательного правила о тайне связи. Классическое представление о норме (с гипотезой, диспозицией и санкцией) связано также с базовым отраслевым правилом. В нашем случае ситуация следующая Конституция России содержит гипотезу, диспозиция содержится в отраслевом законодательстве о связи, а санкция в Уголовном кодексе РФ. Перечисленные положения статей нормативных актов (в рамках учебного процесса) могут служить наглядной иллюстрацией системы источников информационного права в виде «вертикального среза», а также как пример комплексности норм информационного права. Однако ограничиться анализом тайны связи на этапе формирования правового института означало бы остановиться в начале пути. Имеются и иные вопросы. Как влияет на правовой институт тайны связи иное законодательство? Тайна связи это правовой институт или правовой режим?

II.

Кроме общих норм о тайне связи следует учитывать и наличие специальных норм, например о правительственной связи. Другой пример, осужденные, как специальная категория субъектов, предусмотренных исполнительным законодательством[10], имеет пониженный уровень тайны связи. Например, статья 90 Уголовно-исполнительный кодекс Российской Федерации предусматривает порядок получения осужденными к лишению свободы посылок, передач и бандеролей, которые подвергаются досмотру. Статья 92 Уголовно-исполнительный кодекс Российской Федерации предусматривает порядок контролируемых телефонных разговоров осужденных к лишению свободы. В контексте классификации правил на общие и специальные нами исследована позиция А. Е. Чечетина, который проанализировал статьи 63 и 64 ФЗ «О связи» и обратил внимание на обязанности операторов связи «предоставлять уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность, информацию о пользователях услугами связи и об оказанных им услугах связи»[11]. Автор отметил также, что, Конституционный Суд РФ исходит из расширительного толкования понятия тайны Федерального закона «О связи». В другой работе автор полагает, что часть сведений об абонентах (клиентах) отрасли связи, а именно сведения о фактах отправки сообщений и некоторые другие «не попадают под защиту»[12] статьи 23 Конституции России, т. е. не входят в состав тайны связи. Ошибочность данного предположения очевидна, если в методику анализа включить понятие материальных и процессуальных норм. При их сопоставлении станет ясно, что

статья 63 ЗОС о тайне связи имеет общее и, преимущественно, материальное содержание, а статья 64 ЗОС, соответственно процессуальное (и частное). Устанавливая общий режим тайны связи и порядок его поддержания, законодатель предусматривает и случаи исключения. Пример интересен ещё и другим контекстом. Почта как отдельный вид деятельности существует на земле несколько тысячелетий. В современном представлении её оформление связано в реализацией нескольких функций (социальных заказов). Первое и преобладающее направление, — обслуживание государственных интересов в управленческой сфере. Это актуально для любой юрисдикции. Второе направление, переписка между населением (простыми, негосударственными людьми), доставка будущих студентов к месту обучения, сформировалось в период становления первых европейских университетов. Актуальность тайны связи была присуща, в основном, первому направлению. Это и обусловило формирование особой культуры и атрибутики (печати, тайнопись и т. д.). Для второго направления более актуальным было фактическое выполнение услуги и её доступность. В современных условиях недоступность содержания почтового (документального) и электронного отправления обеспечиваются, как правило, на уровне технологии. А вот нестандартные, оперативно-розыскные мероприятия, как правило, входят в тот перечень событий, которые происходят нечасто. И для администрации связи сложнее обеспечить не тайну связи, а событие, связанное с исключением из режима тайны связи. Этот момент практически не рассматривается исследователями, а он как раз и требует особой профессиональной дисциплины и должен быть сохранён в тайне. Вопрос о нарушениях работниками операторов связи, как правило, не исследуется на фактическом материале, поскольку судебной практики по данной категории дел практически нет. Тем не менее, практические работники знают, что нарушение тайны связи событие весьма частое, особенно в транспортных подразделениях (в почтовых вагонах и на автотранспорте). Однако будучи выявленными в недрах оператора связи такие события становятся предметом ведомственных расследований и часто заканчиваются увольнением виновников. Поэтому они не приобретают широкого резонанса. В этой связи формирование особого технологического и правового режима в отрасли связи может способствовать решению задачи тайны связи.

Дополнение нормы положениями, которые формируют исключения из общего правила или дополняют общее правило в части специальных субъектов и ситуаций, позволяет также констатировать формирование института (специального множества однородных норм) тайны связи. Кроме общего порядка защиты тайны связи предусмотрены исключения из общих правил. К таковым следует относить нормы об обязанностях операторов связи при проведении оперативно-розыскных мероприятий, мероприятий по обеспечению безопасности Российской Федерации и осуществлении следственных действий, которые предусмотрены статьёй 64 закона о связи.

В России тайны индивида (личности) ещё не принято делить на два основных компонента: на личную — сведения о личности, которыми обладает сама личность, и иные тайны (адвокатская, врачебная, персональные данные, тайна связи и др.) о личности, которыми обладают иные лица, и которые обязаны предпринять меры по защите тайны в соответствии с законодательством и в соответствии со своими функциональными обязанностями. Данную проблему в современных условиях пытался решить Д. Н. Сухих. Однако, он ограничился констатацией проблемы[13]. В советский период вопросами защиты личности авторы занимались, как правило в рамках гражданского права. Современное представление о правах личности базируется на информационной безопасности. Именно в рамках концепции информационной безопасности (отсутствие внешних и внутренних угроз) может быть найдено решение проблемы гармонизации тайны связи.

III.

Ещё одно направление в исследованиях — это отнесение тайны связи к служебной тайне, как функции государственных органов. Например, О. И. Чеботарева полагает, что «можно выделить, например, такие составляющие служебной тайны: <...> тайна связи»[14]. Авторы П. Н. Кораблев и Т. М. Занина прямо включают тайну связи в служебную тайну, утверждая, что «служебная тайна как комплекс сведений с ограниченным до-

ступом носит не только ведомственный характер — определенные категории информации должны защищаться субъектами государственной сферы во всех случаях. К ним должны относиться: <…> сведения, охватываемые понятием «тайна связи» (в той мере, в какой операторами связи являются органы государственной власти и подведомственные им организации, учреждения)»[15]. Аналогична позиция С. Н. Братановского, который отмечает, что «в процессе государственного управления различными сферами общественной жизни субъекты этого управления становятся осведомленными в отношении сведений, функционирующих в режиме врачебной, адвокатской тайны, тайны связи...»[16]. Ещё одно подключение к теме Н. Ю. Рязанова свидетельствует об изменении его позиции. Он отмечает, что «на сегодняшний день, фактически, универсальная защита тайны связи, не нуждаясь в презумпции принадлежности тех или иных отправлений именно к физическим лицам, тем не менее, обусловлена презумпцией того, что отправление содержит письменное вложение, содержание которого относится к охраняемой уголовным законом тайне (личной, коммерческой, государственной)»[17]. В этой связи естественно возникает вопрос о тех операторах связи, которые, не подведомственны государственной власти. И таких операторов, в количественном исчислении, большинство. Тайна связи в режиме таких операторов будет относиться к служебной или иной тайне? М. В. Бундин в этом видит следующую задачу: «установление принципов иерархии в системе тайн и согласование их с нормами об ответственности»[18]. В результате полной приватизации для оператора связи тайна связи будет служебная или коммерческая? И как она будет включаться в иерархическую систему тайн? А может она будет включаться в систему защиты информации?

Генезис взглядов исследователей на проблему весьма показателен для освещения вопроса о тайне связи. Динамика исследований постепенно теряет субъектно-имущественное нормативное содержание. Очевидно, что вопрос о тайне связи заключается не в форме собственности и не в личной принадлежности. Это позволяет рассматривать тайну связи как объект не связанный с определёнными формами собственности или определёнными субъектами. Однако возложение на государство или оператора обязанности по защите чуждой ему тайны также не решит проблему. Следовательно надо искать иные критерии и аргументы.

IV.

Вопрос о тайне связи как специальном или особом режиме представляется нам отдельным и весьма объемным вопросом, который должно решать в монографическом или диссертационном исследовании. В рамках данной публикации он решается конспективно. Наши общие представления о том, что отрасль связи – это отдельный правовой режим изложены в отдельной работе[19], которая базируется на классических представлениях о правовом режиме. С. С. Алексеев определяет правовой режим как «порядок регулирования, который выражен в комплексе правовых средств, характеризующих особое сочетание взаимодействующих между собой дозволений, запретов, а также позитивных обязываний и создающих особую направленность регулирования»[20]. Правоведы теоретики Н. И. Матузов и А. В. Малько рассматривают правовой режим, как особый порядок правового регулирования, выражающийся в определенном сочетании юридических средств и создающих желаемое социальное состояние и конкретную степень благоприятности или неблагоприятности для удовлетворения интересов субъектов права[21]. Определение правового режима, сформированное в советский период, получило развитие и в российской науке. Д. Н. Бахрах под правовым режимом понимает совокупность правил, регулирующих определенную деятельность людей[22]. Правовой режим информации весьма тщательно исследовала Л. К. Терещенко. Автор отметила в составе правового режима информации наличие отдельных элементов: его целевое назначение; объект правового регулирования; правовое положение субъектов правового режима; комплекс способов правового регулирования и средств юридического воздействия[23]. Это описание режима сближает его с понятием состава правоотношений (субъект, объект содержание). В ряде случаев (например, при описании правовых институтов и режимов) разделить их будет весьма затруднительно. В авторской конструкции общего правового режима информации нет права на защиту информации, он состоит из: «права свободно получать информацию; права свободно передавать информацию; права свободно распространять ин-

формацию»[24]; она выводит «конфиденциальность информации» в специальный правовой режим. Несмотря на то, что специального режима тайны связи в названной работе не описано, его конструкция может быть обусловлена наличием общих правовых режимов информации и правовых отраслевых режимов. Задачу показать зависимость тайны связи от внешних факторов, которые относятся не к нормам как таковым, а к режиму в широком смысле и к определённому правовому режиму в частности, - решил В. И. Руднев. Автор и не ставил такую задачу изначально, но в процессе исследования вопроса о праве осужденных лиц на тайну связи в условиях цензуры и перлюстрации, он несколькими примерами показал, что тайна связи весьма зависима от режима содержания и технических условий места содержания[25].

А. И. Наговицын отмечает ещё один аспект технического плана, который представляет непосредственную угрозу тайне связи. Автор отмечает, что во многих телекоммуникационных устройствах производства иностранных компаний, которые преобладают на российском рынке, монтируются специальные приспособления для прослушивания телефонных переговоров, дешифраторы данных[26]. Технические и технологические составляющие, как элементы системы правил, которые формируют условия формирования оборота и защиты информации, существенно влияют и на тайну связи. Они также должны быть приняты во внимание в процессе правового регулирования.

Подводя итог, необходимо отметить, что одним из направлений исследования должны стать новые элементы правового режима тайны связи: организационные, технические и технологические. Обозначение их в качестве дополнительных критериев позволяет произвести разграничение режимов в составе общего режима тайны связи. По большому счёту практически каждому понятно, что процедуры обеспечения тайны связи в почтовом отделении и на линии телефонной связи имеют существенные отличия. Но произвести классификацию и разграничение режимов, что называется «сверху», позволяет именно набор дополнительных признаков режима.

Примечания

1. Рязанов Н. Ю. Некоторые вопросы самоценности тайны связи // Вестник Московского государственного областного гуманитарного института.– 2012.– № 1.– С. 84–86.

2. Рязанов Н. Ю. Исторические особенности возникновения права на тайну связи // Вестник Московского государственного областного гуманитарного института. Серия: История, философия, политология, право.– 2013.– № 2.– С. 15.

3. Витрук Н. В. Общая теория правового положения личности.– М.: Норма.– 2008.– С. 134.

4. «Конституция Российской Федерации» (принята всенародным голосованием 12.12.1993; с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ) // Собрании законодательства РФ. 2014. № 31. Ст. 4398.

5. См.: Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» (ред. От 13.07.2015) // Собрание законодательства РФ. 2003. № 28. Ст. 2895.

6. См.: Федеральный закон от 17.07.1999 № 176-ФЗ (ред. От 06.12.2011) «О почтовой связи» // Собрание законодательства РФ. 1999. № 29. Ст. 3697.

7. См.: «Уголовный кодекс Российской Федерации» от 13.06.1996 № 63-ФЗ // Собрание законодательства РФ. 1996. № 25. Ст. 2954

8. Федотова Н. В. О субъекте преступления нарушения тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений // Бизнес в законе.– 2008.– № 3.– С. 98–101.

9. «Гражданский кодекс Российской Федерации (часть первая)» от 30.11.1994 № 51-ФЗ (ред.от 13.07.2015) // Собрание законодательства РФ, 1994. № 32. Ст. 3301.

10. См.: «Уголовно-исполнительный кодекс Российской Федерации» от 08.01.1997 № 1-ФЗ (ред. от 28.11.2015) // Собрание законодательства РФ. 1997. № 2. Ст. 198.

11. Чечетин А. Е. Полицейское право на ограничение тайны связи // Полицейское право.– 2005.– № 1.– С. 75–77.

12. Чечетин А. Е. Правовой режим доступа правоохранительных органов к информации операторов связи // Вестник Воронежского института МВД России.– 2014.– № 3.– С. 98–105.

13. См.: Сухих Д. Н. Правовые проблемы регулирования и применения личной и семейной тайны в Российской Федерации // Ленинградский юридический журнал.– 2012.– № 4 (30).– С. 250–256.

14. Чеботарева О. И. О правовой регламентации государственной коммерческой и служебной тайны в законодательстве // Современное право.– 2004.– № 8.– С. 12–15.

15. Кораблев П. Н., Занина Т. М. Особенности правовой защиты служебной тайны // Вестник Воронежского института МВД России.– 2005.– № 5.– С. 88–93.

16. Братановский С. Н. Правовые режимы и соотношение служебной и профессиональной тайны // Гражданин и право.– 2013.– № 1.– С. 13–23.

17. Рязанов Н. Ю. Эволюция права на тайну связи // Право и государство: теория и практика.– 2015.– № 8 (128).– С. 111–115.

18. Бундин М. В. Система информации ограниченного доступа и конфиденциальность // Вестник Нижегородского университета им. Н. И. Лобачевского: Серия Право.– 2015.– № 1.– С. 120–130.

19. См.: Волков Ю. В. Правовые режимы в отрасли связи // Современная наука.– 2010.– № 3.– С. 16–19.

20. Алексеев С. С. Общие дозволения и общие запреты в советском праве.–– М.: Юрид.лит., 1989.– С. 185.

21. См.: Матузов Н. И., Малько А.В. Правовые режимы: вопросы теории и практики // Правоведение.– 1996.– № 1.– С. 6.

22. См.: Бахрах Д. Н. Административное право: Учебник для вузов. - М: БЕК, 1996. С. 201.

23. См.: Терещенко Л. К. Правовой режим информации: автореф. ...дисс. док.юрид. наук. – М., 2011. – С. 15.

24. Терещенко Л. К. Правовой режим информации: автореф. ...дисс. док.юрид. наук.– М., 2011.– С. 17–18.

25. См.: Руднев В. И. О реализации лицами, содержащимися под стражей, права на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений // Журнал российского права.– 2006.– № 3.– С. 72–77.

26. См.: Наговицын А. И. За гранью информационной безопасности // Защита и безопасность.– 2010.– № 52.– С. 21–23.

Волков Юрий Викторович, доцент, кандидат юридических наук, доцент кафедры информационного права Уральского государственного юридического университета. Россия, 620137, г. Екатеринбург, ул.Комсомольская, 23. E-mail: yuriivolkov@yandex.ru.

Volkov Yuriy Victorovich, associate professor in the Department of Information Law at the Ural State Law University, Candidate of law. Russia, 620137, Ekaterinburg, Komsomolskaya, 23. E-mail: yuriivolkov@yandex.ru.

УДК 342.31 + 321.011 Вестник УрФО № 2(20) / 2016, стр. 54–60

Ефремов А. А.

ПРОБЛЕМЫ РЕАЛИЗАЦИИ ГОСУДАРСТВЕННОГО СУВЕРЕНИТЕТА В ИНФОРМАЦИОННОЙ СФЕРЕ

В статье рассматриваются современные проблемы реализации государственного суверенитета в информационной сфере в условиях глобализации. Проведен междисциплинарный анализ подходов к изменению сущности государственного суверенитета под влиянием глобализации. Рассмотрено соотношение различных пространств как сфер реализации суверенитета, в том числе информационного пространства.

Проведен анализ закрепления положений о суверенитете в ключевых документах стратегического планирования в Российской Федерации.

Значительное место уделено анализу международно-правовых проблем реализации суверенитета, в том числе активного развития регулирования в рамках международных организаций.

Ключевые слова: *информационная безопасность; суверенитет; информационное пространство; информационная сфера; международное право*

Yefremov A. A.

PROBLEMS OF REALIZATION OF THE STATE SOVEREIGNTY IN THE INFORMATION SPHERE

In article modern problems of realization of the state sovereignty in the information sphere in the conditions of globalization are considered. The interdisciplinary analysis of approaches to change of essence of the state sovereignty under the influence of globalization is carried out. The ratio of various spaces as spheres of realization of the sovereignty, including information space is considered.

The analysis of fixing of regulations on the sovereignty in key documents of strategic planning in the Russian Federation is carried out.

The important place is given to the analysis of international legal problems of realization of the sovereignty, including active development of regulation within the international organizations.

Keywords: *information security; sovereignty; information space; information sphere; international law*

Актуальность настоящей статьи обусловлена активным формированием документов стратегического планирования в сфере национальной безопасности, в том числе Стратегией национальной безопасности Российской Федерации, утв. Указом Президента Российской Федерации от 31 декабря 2015 года N 683.[1]

В последние годы в СМИ и интернет-сообществе активно обсуждаются и используются понятия «информационный суверенитет», «цифровой суверенитет».

По данным Википедии[2], «информационный суверенитет (цифровой суверенитет, электронный суверенитет) — концепция, подразумевающая контроль государства над распространением информации на своей территории, независимость от влияние извне. Реализована в ряде стран Азии и Ближнего Востока. На территории России активно продвигается российскими властями и поддерживающими их людьми (с 2012 года). Один из основных разработчиков концепции — Игорь Ашманов».

Вместе с тем, конъюнктурность таких «обывательских» определений не должна формировать мнение о некой «новизне» данной проблематики. Вопросы реализации суверенитета в информационной сфере начали подниматься как в России, так и за рубежом еще на рубеже тысячелетий. В.Б. Наумов еще в 1999 г. одним из первых акцентировал внимание на данной проблематике в российской науке,[3] а в 2002 г. вышла монография М.Э. Прайса в США.[4]

Сущностное изменение правового регулирования всех общественных отношений под влиянием глобализации связано с сутью самой глобализации, которую Д. Харвей характеризует как процесс *сжатия (компрессии) временных и пространственных дистанций*. Это означает, что *для определенных видов действия, например, индивидуальной языковой коммуникации, категория пространства как среды этого действия во многих случаях просто исчезает.*[5] При этом если *для экономики и ее организаций пространственное измерение действия становится все более иррелевантным*, то организации политической и правовой системы, напротив, не могут освободиться от *территориального* принципа[6].

Тем самым возникают качественные изменения в сущности и возможностях государственного регулирования общественных отношений посредством национального позитивного права, содержанию такой базовой категории как «*государственный суверенитет*».

В научной среде в настоящее время достаточно активно идет дискуссия и об изменении содержания этой категории. Российские и зарубежные экономисты и политологи обосновывают выводы о том, что «экономический суверенитет уже не находится исключительно в ведении государств, а смещается по отраслевому принципу на региональные, *надгосударственные или мировые уровни*»[7], «геоэкономика, где ведущую роль играют транснациональные экономические и финансовые структуры, *размывает … государственный суверенитет*»[8]. Для научных работ в юриспруденции, наоборот, характерна «апологетика» государственного суверенитета[9], утверждения, что «*социальная роль и значимость государственного суверенитета не только не ослабевает,* а, наоборот, еще больше возрастает»[10], происходит «осуществление суверенитета»[11] в новых формах, изменение содержания этого понятия[12], а само понятие суверенитета, как правило, включает ***территориальную*** составляющую[13].

Если значение *территории* как сферы регулирования снижается, то сферой регулирования становятся *иные «пространства»* – экономическое, информационное, которые не совпадают с конкретными государственными *территориями*.

Данная проблематика пока активнее разрабатывается в экономической и политической науке - целый ряд исследований посвящен таким категориям, как «информационно-экономическое пространство»[14], «информационная экономика»[15], «коммуникационная экономика»[16], «информационно-сетевая экономика»[17], «сетевая экономика»[18], «экономика знаний»[19], созданию *глобального информационного поля* благодаря развитию и совершенствованию современных информационных технологий[20].

В правовой науке также рассматривается категория «*правовое пространство*»[21]. Однако при его раскрытии преобладает привязка к территории - под пространством подразумевают в виду весь объем общественных отношений, возникающих и подвергающихся правовому регулированию *в территориальных пределах* Российского государства[22], сферу регламентации юридическими нормами

моделей правомерного поведения государства, его составных частей и граждан *в границах территории данного государства* и конкретного исторического времени[23], область действия всех элементов правовой системы *конкретного государства*, имеющая социально-юридические (пределы правового регулирования) и *политико-географические (территориально-государственные) границы*[24].

Автором настоящей статьи предприняты попытки обоснования механизма реализации государственного суверенитета в финансовой сфере.[25]

По мнению Д.А. Савельева, *глобальное информационное пространство* является объектом международно-правового регулирования.[26] *Исходя из современного представления о суверенитете государства, согласно которому права человека не могут быть исключительно внутренним делом государства*, следует сделать вывод о том, что *основная роль в установлении принципов правового регулирования информационного пространства должна принадлежать международному праву*[27]. И.Л. Бачило обращает внимание на проблему соотношения информационного и правового пространства, однако указывает на необходимость ее «дальнейшего исследования».[28]

Таким образом, в информационных отношениях происходит изменение сферы регулирования – *территория* государства заменяется на определенное *пространство* как сферу действия суверенитета.

На протяжении достаточно длительного периода в документах стратегического планирования - Стратегии развития информационного общества в Российской Федерации (утв. Президентом РФ 07.02.2008 № Пр-212), Концепции формирования в Российской Федерации электронного правительства до 2010 года (одобрена распоряжением Правительства РФ от 06.05.2008 № 632-р) об обеспечении государственного суверенитета *вообще не упоминалось.*[29]

Отдельные положения о взаимосвязи суверенитета и интересов государства в информационной сфере есть в Доктрине информационной безопасности РФ и Стратегии национальной безопасности Российской Федерации до 2020 года, утв. указом Президента РФ от 12.05.2009 N 537, однако они носят общий характер, а в п. 108 Стратегии *вообще заложено противоречие* – «для развития системы распределенных ситуационных центров … потребуется преодолеть технологическое отставание …. *разработать и внедрить технологии информационной безопасности* в системах государственного и военного управления, … *а также обеспечить условия для гармонизации национальной информационной инфраструктуры с глобальными информационными сетями и системами*».

Новая Стратегия национальной безопасности Российской Федерации, утв. Указом Президента Российской Федерации от 31 декабря 2015 года N 683, упоминает «технологический суверенитет в энергетической сфере», «суверенитет финансовой системы», «культурный суверенитет»

В диссертационных работах по регулированию информационных отношений категория «суверенитет» рассматривается только по отношению к охране государственной тайны как средству его обеспечения.[30]

По нашему мнению, *информационный суверенитет государства заключается в возможности государства осуществлять посредством национального и международного права регулирование определенного информационного пространства.*

Следует отметить, что формирование правовой теории информационного пространства, киберпространства еще только начинается.[31]

В российском законодательстве термин «кибернетическое пространство» не употребляется, но он используется в нескольких международных документах, например в Окинавской хартии глобального информационного общества 2000 г. и в Конвенции о преступности в сфере компьютерной информации 2001 г.

Д.В. Грибанов[32] дает следующее определение кибернетическому пространству.

Кибернетическое пространство - это совокупность общественных отношений, возникающих в процессе использования функционирующей электронной компьютерной сети, складывающихся по поводу информации (информационных ресурсов), обрабатываемой с помощью ЭВМ и услуг информационного характера, предоставляемых с помощью ЭВМ и средств связи компьютерной сети, совокупность отношений, участвовать в которых можно только посредством ЭВМ и средств связи компьютерной сети.

По его мнению, основные признаки кибернетического пространства как объекта правового регулирования:

1. Это - совокупность общественных отношений. Киберпространство - многочисленные социальные связи между людьми.

2. Это - совокупность отношений по поводу информации и информационных услуг. По содержанию информация в кибернетическом пространстве может быть самая различная - от простого электронного сообщения до опубликованного произведения. Главное - это те информационные отношения, которые нуждаются в правовом регулировании и которые можно организовать с помощью норм права.

3. Объектом выступает только та информация, которая обработана с помощью ЭВМ. Речь идет не об информации, которая может быть обработана компьютером (а это практически любая информация), но об информации, которая уже внесена в память компьютера и существует в оцифрованной форме. Это - один из главных технических признаков информации, имеющийся в кибернетическом пространстве.

4. Кибернетическое пространство существует на основе технического средства - функционирующей электронной компьютерной сети. Один компьютер не создает кибернетического пространства.

Д.В. Грибанов считает, что система норм, направленных на регулирование кибернетического пространства, носит комплексный характер и находится на стыке различных отраслей права. Определяя место этих норм в системе права, можно рассматривать их как институт отрасли информационного права.[33]

По нашему мнению, данный подход является узким, поскольку правовое регулирование информационного пространства охватывается нормами ***не только разных отраслей, но и систем права*** – т.е. не только национальным, но и международным правом.

В Рекомендациях Парламентских слушаний «О совершенствовании федерального законодательства по обеспечению информационной безопасности при использовании информационно-коммуникационных технологий для оказания государственных услуг и осуществления межведомственного электронного документооборота», которые состоялись 28.06.2010, содержится положение об информационном суверенитете, предложенное автором[34] данной работы:

«Совету Безопасности Российской Федерации, Совету при Президенте Российской Федерации по развитию информационного общества в Российской Федерации:

рассмотреть возможность изменения Стратегии развития информационного общества в Российской Федерации, Плана реализации Стратегии развития информационного общества в Российской Федерации до 2011 г. и Основ стратегического планирования в Российской Федерации в части включения согласованных положений, направленных на обеспечение ***информационного суверенитета*** Российской Федерации на основе использования в сфере госуправления ИКТ российских производителей».[35]

Еще одной проблемой обеспечения информационного суверенитета, на которую практически не обращается внимание в научных исследованиях, является *зависимость государственного управления* (на уровне документов стратегического планирования) *от иностранных и международных рейтингов*. В частности, в Стратегии развития информационного общества в Российской Федерации, именно международные рейтинги используются для определения *контрольных значений показателей развития информационного общества* в РФ. Безусловно, что оценка развития электронного государства, в том числе и его рейтинги, могут являться важным направлением деятельности международных организаций, однако методика их составления и сам процесс должны быть максимально прозрачны и основаны на широком участии представителей всех государств, которые оцениваются.

Реализация государственного суверенитета в информационной сфере на международно-правовом уровне обусловлена следующими обстоятельствами.

Процесс гармонизации национального законодательства и международно-правовых документов обусловлен необходимостью учета характера документов различных международных организаций (МСЭ, ОЭСР и т.п.), которые в значительной части по своей международно-правовой природе относятся к так называемому «мягкому праву», а также в большей мере содержат принципы развития и положения стратегического характера.

Эти обстоятельства обуславливают с одной стороны, необходимость постоянного анализа на предмет соответствия документам международных организаций и последующей корректировки российских национальных документов стратегического планирования, а с другой – глубокого анализа внедряемых положений в контексте обеспечения государственного суверенитета.

Формирование системы правового регулирования в данном случае идет по схеме «документы международных организаций – национальные концепции, стратегии и доктрины - законодательство». Тем самым происходит «обход» конституционных норм (ч. 4 ст. 15, ст. 79 Конституции РФ), устанавливающих, что именно международные договоры являются составной частью правовой системы, а участие в межгосударственных объединениях и передача им части полномочий РФ возможна только в соответствии с международными договорами, если это не влечет ограничения прав и свобод человека и гражданина и не противоречит основам конституционного строя РФ. При такой схеме не применяется и механизм ратификации, действующий в отношении международных договоров, а также конституционный контроль (проверка соответствия Конституции РФ не вступивших в силу международных договоров РФ – ст. 125 Конституции РФ).

Еще одним проблемным аспектом гармонизации российского национального законодательства с документами международных организаций является необходимость учета существующих международно-правовых обязательств в рамках иных интеграционных объединений – ЕАЭС (в том числе документы ЕЭК), СНГ, БРИКС, ШОС и т.п., а также идущих параллельно в указанных международных организациях процессах подготовки международно-правовых документов в области информационных отношений.

Поэтому необходимо проведение постоянного мониторинга как процессов разработки и реализации документов ОЭСР, так и российских национальных документов стратегического планирования и документов иных интеграционных объединений – ЕАЭС (в том числе документы ЕЭК), СНГ, БРИКС, ШОС и т.п., в области информационных отношений с последующей корректировкой предлагаемых изменений и дополнений российских нормативных правовых актов и документов стратегического планирования.

Нуждаются в дополнительном уточнении и положения Концепции внешней политики Российской Федерации, утв. Президентом Российской Федерации 12 февраля 2013 г.[36] В Концепции указывается, что «на передний план выдвигаются, наряду с военной мощью, такие важные факторы влияния государств на международную политику, как экономические, правовые, научно-технические, экологические, демографические и информационные» (п. 10).

Российская Федерация, согласно Концепции, будет принимать необходимые меры в интересах обеспечения национальной и международной информационной безопасности, будет добиваться выработки под эгидой ООН правил поведения в области обеспечения международной информационной безопасности (п. 32).

Но при этом практические меры по реализации указанных положений отражены исключительно в п. 41 Концепции – «Информационное сопровождение внешнеполитической деятельности», согласно которому в рамках публичной дипломатии Россия будет добиваться объективного восприятия ее в мире, развивать собственные эффективные средства информационного влияния на общественное мнение за рубежом, обеспечивать усиление позиций российских средств массовой информации в мировом информационном пространстве, предоставляя им необходимую государственную поддержку, *активно участвовать в международном сотрудничестве в информационной сфере, принимать необходимые меры по отражению информационных угроз ее суверенитету и безопасности*.

Перспективными направлениями реализации суверенитета в информационной сфере на уровне международных организаций также являются:

• гармонизация информационно-правового регулирования в государствах ЕАЭС на основе работы ЕЭК, в которой создан новый Департамент, однако решаемые им задачи по созданию единого информационного пространства пока носят фрагментарный характер;

• активизация участия в работе ОЭСР по направлению digital (в том числе с учетом документов ОЭСР - Рекомендации ОЭСР по стратегиям цифрового правительства (Recommendation on Digital government strategies. 15 July 2014), Рекомендации и сопроводительный документ ОЭСР по управлению рисками цифровой безопасности для экономического и социального процветания (Digital security risk management for economic and social prosperity. OECD Recommendation and Companion Document. 17 September 2015 – C(2015)115);

• активизация гармонизации национального законодательства с Рекомендациями Ко-

митета Министров Совета Европы, а также активное участие в разработке новых рекомендаций.

Рассмотренные подходы к реализации государственного суверенитета в информационной сфере позволят уйти от конъюнктурности к полноценной системной регуляторной политике в информационной сфере, как на национальном, так и международно-правовом уровнях.

Примечания

1. Указ Президента Российской Федерации от 31 декабря 2015 года N 683 "О Стратегии национальной безопасности Российской Федерации" // Рос.газета. - 2015. - 31 дек.

2. http://www.wikireality.ru/wiki/Информационный_суверенитет

3. Наумов В.Б. Интернет и государственный суверенитет // I Всероссийская конференция "Право и Интернет: теория и практика" 2 ноября 1999 г. URL http://www.ifap.ru/pi/01/r16.htm

4. Price, M.E. Media and sovereignty: The global information revolution and its challenge to state power. - Cambridge, MA: MIT Press, 2002. - 352 pp.

5. Цит. по: Назарчук А. В. Этика глобализирующегося общества. - М.: Директмедиа Паблишинг, 2002. - С. 207.

6. Там же. - С. 208.

7. Жан К. Геоэкономика: теоретические аспекты, методы, стратегия и техника // Геоэкономика. Господство экономического пространства / К. Жан, П. Савона. - М.: Ad Marginem, 2007.- С. 36.

8. Тыква В.А. Взаимосвязь экономической и военной безопасности Российской Федерации в современных экономических условиях: Автореф. дисс… канд. экон. наук. - М., 2008. - С. 3.

9. Зорькин В. Апология Вестфальской системы // Российская газ. - 2004. - 13 июля.

10. Марченко М. Н. Государство и право в условиях глобализации. - М.: Проспект, 2008. - С. 100.

11. Айбазов Р.У. Конституция и управление федеративным строительством России в условиях глобализации. - М.: Формула права, 2005. - С. 83; Крылов Б.С. Государственный суверенитет: современные проблемы // Конституционное и муниципальное право. - 2008. - N 6. - С. 2-6; Хабиров Р.Ф. Глобализация, государственный суверенитет, права человека // Юридический мир. - 2007. - N 10.

12. Лукашук И. И. Глобализация, государство, право, XXI век. - М.: Спарк, 2000. - С. 142-143.

13. См. подробнее: Моисеев А.А. Соотношение суверенитета и надгосударственности в современном международном праве (в контексте глобализации): Автореф. дисс… доктора юрид. наук.- М., 2006. - С. 15; Крылов Б.С. Государственный суверенитет: современные проблемы // Конституционное и муниципальное право. - 2008. - N 6. - С. 2; Горюнов В.В. Суверенитет Российской Федерации: сущность, содержание, гарантии: Автореф. дисс… канд. юрид. наук. - Екатеринбург, 2007. - С. 7.

14. Переверзев С.В. Единое информационно-экономическое пространство в макроэкономической системе России: Автореф. дисс… канд. экон. наук. - Ростов-на-Дону, 2005; Григорьева Ю.Ю. Информационно-экономическое пространство России и особенности его государственного регулирования в условиях трансформируемой экономики: Автореф. дисс… канд. экон. наук. - Ростов-на-Дону, 2003.

15. Баранова Н.В. Теоретико-методологические аспекты формирования информационной экономики: Автореф. дисс… канд. экон. наук. - Челябинск, 2007; Шевелева Ю.И. Фирма в информационной экономике: оптимизация организационной структуры: Автореф. дисс… канд. экон. наук. - Спб., 2007; Китаев А.В. Информация в системе факторов общественного производства: Автореф. дисс… канд. экон. наук. - Ростов-на-Дону, 2007.

16. Чекунов А.Ю. Эволюция постиндустриальной экономики в коммуникационную: Автореф. дисс… канд. экон. наук. - Томск, 2005.

17. Коновалова О.Н. Информационно-сетевая экономика и переход России к инновационному типу развития: Автореф. дисс… канд. экон. наук. - Омск, 2007.

18. Юнусов А.М. Теоретические основы формирования и становления сетевой экономики в России: Автореф. дисс… канд. экон. наук. - М., 2008.

19. Гавричков А.В. Развитие экономики знаний в России в условиях глобализации: Автореф. дисс… канд. экон. наук. - М., 2007; Ченцова М.В. Особенности формирования экономики знаний в современных условиях: Автореф. дисс… канд. экон. наук. - М., 2008.

20. Галюта О.Н. Теоретические основы формирования информационной экономики: Автореф. дисс… канд. экон. наук. - Сургут, 2007. С. 6; Дьячков В.В. Информационное поле взаимодействия экономических систем: Автореф. дисс… канд. экон. наук. - Тамбов, 2007.

21. Суханов В.В. Правовое пространство и его формы: Автореф. дис… канд. юрид. наук. - М., 2005; Барциц И.Н. Конституционно-правовое пространство Российской Федерации: Автореф. дис… доктора юрид. наук. - М., 2001.

22. Балмасов О.В. Обеспечение единого правового пространства как функция современного Российского государства: Автореф. дис… канд. юрид. наук. - Н.Новгород, 2006. - С. 21.

23. Барциц И.Н.Правовое пространство России: вопросы конституционной теории и практики. - М., 2000. - С. 24

24. Егорова Ю.В. Системность российского законодательства в контексте единого правового пространства России // История государства и права. - 2007. - № 1.

25. См.: Ефремов А.А. Конституция и финансовый рынок: краеугольные камни регулирования // Вестник НАУФОР. - 2005. - № 10. С. 24-29; Ефремов А.А. Глобализация финансовых рынков: соотношение международно-правового и национального регулирования // Вестник Воронеж. гос. ун-та: Серия Право. - 2007. - № 2. - С. 347-352.

26. Савельев Д.А. Права человека в области информации (международно-правовые аспекты): Автореф. дис… канд. юрид. наук. – СПб, 2002. С. 7.

27. Там же. - С. 11.

28. Бачило И.Л. Проблемы теории информационного права // Теоретические проблемы информационного права - М., 2006. - С. 16-18.

29. См.: Ефремов А.А. Проблемы регулирования информационных отношений // Наследие юридической науки и современность: Материалы заседаний V Международной школы-практикума молодых ученых-юристов (Москва, 26-28 мая 2010 г.). Отв. редактор В.И. Лафитский. -М.: ИД «Юриспруденция», 2011. - С. 155-164; Ефремов А.А. Электронное правительство и международное право // Интернет и современное общество: Сборник научных статей. Материалы XIV Всероссийской объединенной конференции «Интернет и современное общество». Санкт-Петербург, 12 -14 октября 2011 г. - СПб:, 2011. - С. 190-196; Ефремов А.А. Электронное государство в международном праве: формирование нового межотраслевого института // Международно-правовые чтения. Вып. 10 / Отв. ред. П.Н. Бирюков. - Воронеж: Изд.-полиграф. центр Воронеж. гос. ун-та, 2012. - С. 82-92.

30. Мартышин М.Ю. Государственная тайна как объект конституционно-правового регулирования: Автореф. дисс… канд. юрид. наук. - М., 2009. - С. 3; Скопец П.С. Государственно-правовое регулирование конституционного права граждан России на информацию и его ограничений: Автореф. дисс… канд. юрид. наук. - СПб, 2006. - С. 18

31. См., например: Рассолов И.М. Киберпространство и позитивное право // Российское право в Интернете. – 2010. - № 1. URL http://www.rpi.msal.ru/prints/201001rassolov.html

32. Грибанов Д.В. К вопросу о правовой теории кибернетического пространства // Государство и право. - 2010. - № 4. - С. 60.

33. Там же. - С. 60.

34. Ефремов А.А. Предложения для включения в проект Рекомендаций Парламентских слушаний «О совершенствовании федерального законодательства по обеспечению информационной безопасности при использовании информационно-коммуникационных технологий для оказания государственных услуг и осуществления межведомственного электронного документооборота» 28.06.2010 // Информация для всех, URL http://www.ifap.ru/pr/2010/n100622a.pdf

35. См. подробнее: http://www.gosbook.ru/node/6046

36. Концепция внешней политики Российской Федерации // Официальный сайт Министерства иностранных дел Российской Федерации. URL http://archive.mid.ru//bdomp/ns-osndoc.nsf/e2f289bea62097f9c325787a0034c255/c32577ca0017434944257b160051bf7f!OpenDocument .

Ефремов Алексей Александрович, ведущий научный сотрудник Центра технологий государственного управления ИПЭИ РАНХиГС, кандидат юридических наук, доцент. 119571, г. Москва, проспект Вернадского, д. 82. E-mail: yefremov@law.vsu.ru

Yefremov Alexey, Senior Researcher of the Center for Public Administration Technologies in RANEPA Institute of Applied Economic Research, Candidate of Law, Associate Professor. Vernadskogo Prospect, 82, Moscow, 11957, Russia. E-mail: yefremov@law.vsu.ru

УДК 342.5 Вестник УрФО № 2(20) / 2016, стр. 61–70

Камалова Г. Г.

ГОСУДАРСТВЕННАЯ И МУНИЦИПАЛЬНАЯ СЛУЖАЩИЕ В СИСТЕМЕ СУБЪЕКТОВ ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ СЛУЖЕБНЫХ СВЕДЕНИЙ

В статье анализируются состав и особенности правового статуса государственных и муниципальных служащих как представителей субъектов-держателей сведений, охраняемых в режиме служебной тайны. Автор отмечает, что публичные служащие и иные сотрудники органов государственного управления являются субъектами отношений в сфере создания и использования служебной информации в силу выполнения служебных и трудовых функций. Их статус в системе охраны служебных сведений определяется занимаемой должностью и выполняемой работой.

В статье рассматривается понятие «служба». Отмечается, что служба в аспекте законодательства, регулирующего государственную службу и ее информационное обеспечение, должна пониматься в смысле профессиональная служебная деятельность, то есть интеллектуальная деятельность лица, осуществляемая профессионально в органе государственного управления.

Автор отмечает, что в ходе служебной деятельности сотрудники государственных и муниципальных органов получают доступ к широкому спектру различной информации. Рассматриваются права и обязанности публичных служащих в процессе сбора, обработки и обеспечения конфиденциальности служебных сведений.

Отмечается, что далеко не все лица, участвующие в процессе сбора и обработки служебных сведений, имеют статус государственного или муниципального служащего, что не исключает их участия в информационных процессах, происходящих в органах государственного управления.

Ключевые слова: *информация ограниченного доступа, тайна, конфиденциальность, служебная тайна, государственная служба, муниципальная служба.*

Kamalova G. G.

STATE AND MUNICIPAL EMPLOYEES IN THE SYSTEM OF SUBJECTS ENSURE OF THE CONFIDENTIALITY OF OFFICIAL INFORMATION

The author analyzes the structure and features of the legal status of state and municipal employees as the representatives of the subjects-holders of official information. He noted that public servants and other employees of public administration are subject relations in the sphere

of creation and use of confidential information by reason of service and employment functions. Their status in the system of protection of official information is predetermined by the position and the work performed.

The author considers the concept of "service". He notes that the service in the aspect of the legislation governing the civil service and its information provision, should be understood in the sense of professional service activity, that is intellectual activity entity carried out in government.

During the performance the employees of state and municipal agencies have access to a wide range of different information. The author considers the rights and obligations of public servants in the process of collecting, processing and guarantee of confidentiality service information.

He notes that not all the persons involved in the process of collecting and processing information service, have the status of a state or municipal employee. The latter does not exclude their participation in information processes taking place in the public administration.

Keywords: *restricted information, secret, privacy, official secrecy, public service, municipal service.*

Под служебной тайной будем понимать специальный режим информации ограниченного доступа, устанавливаемый в отношении сведений, получаемых или разрабатываемых органами государственного управления в целях эффективной реализации ими государственных функций.

Одним из элементов правового режима служебной тайны выступает характеристика правового статуса субъектов режима. Традиционно выделяют доверителей и держателей сведений, составляющих служебную тайну. Рассмотрим подробнее держателей тайны, так как в вопросе их состава имеются различия в позициях специалистов и ученых.

Основными субъектами-держателями служебной тайны являются органы государственного управления, деятельность которых определяется целями, задачами государственного управления, реализацией делегированных государственных функций. Определение совокупности структур, осуществляющих функции государства, выступает основой для определения круга субъектов-держателей служебной тайны.

Существуют несколько позиций о составе субъектов-держателей служебной тайны[1]. Согласно первой, к ним относятся только государственные органы и их сотрудники, среди которых особо выделяют государственных служащих и данная позиция соответствует нормам Указа Президента РФ от 06.03.1997 № 188[2] и Постановления Правительства РФ от 03.11.1994 года № 1233[3]. К другой относится включение в состав субъектов-держателей также органов местного самоуправления. Кроме того, нередко можно встретить мнение, что сведения служебного характера могут собираться и использоваться в любых организациях, в том числе частных[4]. Последняя позиция наиболее характерна для исследований-цивилистов и специалистов уголовного права. Так, Д.В. Бушков, анализируя уголовно-правовую охрану личной корреспонденции пишет, что «под служащими … понимаются работники нефизического труда, получающие жалование, фиксированную заработную плату»[5]. Соответственно к служащим он относит: начальника почты, почтальона, телефонистку и технических работников операторов связи.

Рассматривая систему субъектов права на служебную тайну следует особо отметить то, что основными держателями являются органы государственного управления и публично-правовые организации, реализующие государственные функции. Но нельзя игнорировать и то обстоятельство, что основными фактическими носителями служебных сведений и непосредственными участниками отношений выступают сотрудники органов государственного управления. Вместе с тем, их правовой статус производен от статуса организаций, где осуществляется их служебная и трудовая деятельность. Следовательно, служащие являются представителями держателя служебной тайны.

Весьма спорной представляется позиция по отнесению государственных и муниципальных служащих напрямую к субъектам режима служебной тайны. Так, Е.Н. Яковец и И.Н.Смирнова считают, что «особенность служебной тайны заключается в том, что ее субъектами могут являться исключительно госу-

дарственные или муниципальные служащие»[6]. Думается, что служащие и иные сотрудники органов государственного управления являются субъектами отношений в сфере создания и использования служебной информации постольку, поскольку выполняют служебные или трудовые функции. Их статус предопределяется занимаемой должностью и выполняемой работой. Лишь небольшая часть государственных служащих из общей массы обладает правом самостоятельно реализовывать функции государства, непосредственно принимая властные решения[7] и может быть отнесена к субъектам режима служебной тайны непосредственно. Служебная деятельность большей части служащих направлена на обеспечение деятельности публичных органов, что не позволяет их рассматривать как самостоятельных субъектов режима служебной тайны. По справедливому замечанию И.В. Черепановой «Государственная служба … реализация власти (властных полномочий), но не непосредственно, а опосредованно, путем реализации делегированных властных (служебных) полномочий по управлению государством. Исполнители не являются носителями государственной власти, но выступают как её представители через предоставленные им служебные полномочия»[8].

Сформировавшиеся в Российской Империи традиции службы государству в советский период во многом были нарушены. В Российской Империи активно использовалось понятие «чиновник», которое в настоящее время не имеет однозначного правового аналога. В советский период стройная структурированная система организации деятельности чиновников Российской Империи, в которой была реализована модель служения государству, была разрушена и получила развитие советская (номенклатурная) модель, которая характеризовалась политической обусловленностью, выведенностью из сферы действия законодательства и информационной закрытостью для общества[9].

С начала девяностых годов началось построение новой системы российского государственного управления в сложных экономических и социально-политических условиях, а также формирование законодательства, отвечающего современным реалиям.

Обобщенно характеризуя статус государственного и муниципального служащего, нередко используют словосочетание «публичная служба», которое является собирательным понятием, охватывающим как служебную деятельность лиц, замещающих государственные и муниципальные должности (носителей публичной власти), так и службу, объединяющую в себе характеристики служебной и трудовой деятельности[10].

Наименование служебной тайны непосредственно связано с осуществлением служебной деятельности. Понятие и слово «служба» являются весьма многозначными. В толковом словаре В. Даль пишет, что служба – это работа, занятия, должность служащего; место такой работы и само пребывание на ней; исполнение воинских обязанностей, должность военнослужащего, пребывание в рядах армии, флота[11]. Специалисты также выделяют двоякое понимание термина «служба»: деятельность и (или) организация. В понимании деятельность может рассматриваться как любая профессиональная умственная деятельность в любых организациях (в широком смысле) и как деятельность в органах государственной власти (в узком смысле)[12].

Возможность интерпретации службы как любой интеллектуальной (умственной) деятельности способствует применению слова «служба» по отношению к работе в любых организациях и пониманию служебной тайной как конфиденциальной информации, доверенной работнику такой организации. Думается, что предпочтительнее понимание слова «служба» в смысле «профессиональная служебная деятельность» лица, осуществляемая в органе государственного управления. Г.В. Атамчук писал, что «государственная служба – это практическое и профессиональное участие граждан в осуществлении целей и функций государства посредством исполнения государственных должностей, учрежденных в государственных органах»[13].

Внесение соответствующих изменений в законодательство России позволит избежать смешения возможных смыслов[14] и разделить публичную служебную и трудовую интеллектуальную деятельность.

Законодатель государственную службу трактует в узком смысле, определяя ее как профессиональную служебную деятельность граждан России по обеспечению исполнения полномочий государства, органов государственной власти, иных государственных органов, лиц, замещающих должности, устанавливаемые Конституцией РФ, конституциями, уставами, законами субъектов РФ, федераль-

ными законами для непосредственного исполнения полномочий государственных органов.

Государственная служба – это сложный комплексный правовой институт[15]. Система государственной службы России включает в себя государственную военную, гражданскую и правоохранительную службы, каждая из которых имеет свою специфику. В своей сущности публичная служба является служением обществу и государству. Одной из основных характеристик взаимосвязь и взаимообусловленность публичной службы с государственным управлением. Как отмечают специалисты, главным для государственного служащего является служение людям, обществу, качественная реализация целей и функций государства путем практического исполнения должностных правомочий и обязанностей[16].

Признаки муниципальной службы во многом совпадают с приведенными для государственной службы. И хотя, муниципальная служба выделяется особой организационной структурой и имеет определенную независимость, муниципальные служащие также являются носителями служебных сведений.

Гражданский служащий в соответствие со ст. 13 Федерального закона «О государственной гражданской службе Российской Федерации»[17] – это гражданин России, взявший на себя обязательства по прохождению гражданской службы. В соответствии с п. 1, 2 ст. 2 и ст. 10 Федерального закона «О муниципальной службе в Российской Федерации»18, муниципальная служба – это профессиональная деятельность граждан, которая осуществляется на постоянной основе на должностях муниципальной службы, замещаемых путем заключения трудового договора (контракта), а муниципальным служащим является гражданин, исполняющий в порядке обязанности по должности муниципальной службы за денежное содержание, выплачиваемое за счет средств местного бюджета.

Государственный и муниципальный служащие активно участвуют в реализации функций государства, включая информационную, и осуществляют создание, сбор, систематизацию, обеспечение хранения, использования, предоставления, раскрытия и защиты служебной информации, полученной и генерированной органом государственного управления. Законодательство содержит целый ряд норм, регулирующих информационное обеспечение государственной и муниципальной службы. Государственный гражданский и муниципальный служащий имеет право:

- на получение в установленном порядке информации и материалов, необходимых для исполнения должностных обязанностей. Он может запрашивать требуемые сведения в установленном порядке;
- на ознакомление с документами и материалами, определяющими права и обязанности сотрудника государственного или муниципального органа (уставы, положения, порядок обработки информации, должностные инструкции и т.д.);
- в установленном порядке посещать государственные и муниципальные органы, общественные объединения, организации и граждан в связи с исполнением должностных обязанностей;
- на проведение служебных контрольных и надзорных проверок;
- на ознакомление в установленном порядке с информацией ограниченного доступа, включая сведения, составляющие государственную тайну, если исполнение должностных обязанностей связано с использованием таких сведений;
- на защиту своих информационных прав и законных интересов в информационной сфере.

В ходе служебной деятельности сотрудники государственных и муниципальных органов получают доступ к широкому спектру различной информации. Права служащего носят обеспечивающих характер по отношению к его служебной деятельности в государственном или муниципальном органе и производны от функций реализуемых органом.

Обязанности, возлагаемые на сотрудников государственных и муниципальных органов в информационной сфере, сформулированы значительно лаконичнее:

- соблюдать законодательство об информационной безопасности;
- обеспечивать доступность сведений о деятельности публичных органов;
- соблюдать режимы информации ограниченного доступа, в том числе не разглашать сведения, составляющие государственную и иную охраняемую федеральным законом тайну, а также сведения, ставшие ему известными в связи с исполнением должностных обязанно-

стей, в том числе сведения, касающиеся частной жизни и здоровья граждан или затрагивающие их честь и достоинство. Данная обязанность сохраняется и после увольнения со службы;

- соблюдать при исполнении должностных обязанностей права и законные интересы граждан и организаций.

Все сказанное позволяет утверждать, что государственные и муниципальные служащие являются основными субъектами-носителями служебных сведений и, следовательно, основными представителями субъекта-держателя служебной тайны.

Сотрудник публичного органа является элементарной частицей (атомом) своими действиями реализует основные направления деятельности государства, фактически материализуя его функции. Правовой статус публичных служащих в самом общем виде характеризуются тем, что права и обязанности служащего устанавливаются в пределах компетенции соответствующего органа государственного управления.

Законодательство предусматривает ограничения общегражданских прав публичных служащих в целях обеспечения эффективности их служебной деятельности, для них предусмотрены определенные льготы, а также повышенная ответственность за совершенные ими правонарушения[19].

Любая публичная служба осуществляется на профессиональной основе. Характер и степень участия публичного служащего в реализации полномочий органа определяется занимаемой им должностью. Последняя, в свою очередь, определяется профессиональными компетенциями служащего, его профессиональными знаниями и навыками. Профессия человека выражается в приобретенных им специальных трудовых компетенциях, которые характеризуются определенной направленностью в системе разделения труда и являются источником существования человека и его семьи. Профессионализм и компетентность является одним из основополагающих принципов служебной деятельности.

С данной позиции, вполне справедливо говорить о государственном и муниципальном служащем как носителе профессиональной тайны. В то же время следует различать публично-правовую профессиональную тайну как составную часть служебной информации ограниченного доступа и профессиональную тайну частноправового характера. Так, сотрудник министерства, уполномоченного в области охраны здоровья граждан, профессиональный врач, осуществляя контроль за учреждениями здравоохранения получает сведения, составляющие врачебную тайну. Данные сведения, с одной стороны, являются для него врачебной тайной, так как он имеет профессиональное медицинское образование, с другой, включаются в круг служебных сведений, поскольку он имеет статус государственного служащего.

Исходя из буквального толкования норм законодательства о государственной и муниципальной службе получается, что помимо не разглашения охраняемой законом тайны государственный и муниципальный служащий также обязан не разглашать любую ставшую ему известной в ходе служебной профессиональной деятельности служебную информацию. Полагаем, что следует законодательно определить понятие «служебная информация», с выделением и разграничением понятий «общедоступная служебная информация» и «служебная информация ограниченного доступа», а также установить соотношение «служебной информации» и «информации о деятельности государственных органов и органов местного самоуправления».

Современное российское законодательство не в достаточной степени учитывает особенности различных видов служебной деятельности в системе государственного управления. Е.Г. Крылова отмечает, что законодательство о государственной службе не учитывает специфики службы во многих государственных органах[20]. Так, государственная служба в аппаратах законодательных органах системно сочетает в себе характерные особенности деятельности государственного гражданского служащего и взаимодействие с депутатским корпусом. Организация данной службы строится исходя из интересов как представительного органа в целом, так и интересов депутатского корпуса. В деятельности данной категории служащих используются наряду с традиционными служебными сведениями и сведения, имеющие определенную партийную значимость.

Государственная служба в судебных органах также характеризуется определенной спецификой, не учитываемой в нормах законодательства России о государственной службе: исключительно важное значение имеет соблюдение принципов справедливости и законности, реализуется обеспечение

процесса осуществления функции судопроизводства, наличие дополнительных ограничений в статусе судей и другие[21].

Сотрудники аппарата суда, будучи не вправе вмешиваться в деятельность судей, в тоже время, осуществляют информационное, финансовое, материально-техническое и иное обеспечение деятельности суда и, соответственно, активно участвуют процессах внутренней циркуляции служебной информации, а также во взаимодействии с гражданами и организациями.

Отсутствие учета специфики службы в различных публичных органах в законодательстве, регулирующем государственную службу, отображается и на информационном законодательстве Российской Федерации. Не разработанность сущности понятия «служебная информация» усугубляется не достаточной изученностью специфики информационного обеспечения и информационной деятельности государственных структур различных видов. Полагаем, что возможно выделение разновидностей режимов служебной тайны на основе особенностей компетенции органов государственного управления с последующим их оформлением в виде ее разновидностей.

Публичный служащий не может быть принят на службу, а принятый не может находиться на гражданской службе в случае отказа от прохождения процедуры оформления допуска к сведениям, составляющим государственную и иную охраняемую федеральным законом тайну, если исполнение должностных обязанностей по должности связано с использованием таких сведений. Служащему запрещено:

- разглашать или использовать в целях, не связанных с гражданской службой, сведения, отнесенные в соответствии с законом к сведениям конфиденциального характера, или служебную информацию, ставшие ему известными в связи с исполнением должностных обязанностей;
- допускать публичные высказывания, суждения и оценки, в том числе в средствах массовой информации, в отношении деятельности государственных органов, их руководителей, включая решения вышестоящего государственного органа либо государственного органа, в котором он замещает должность гражданской службы, если это не входит в его должностные обязанности.

Установленные законодательством требования к служебному поведению публичного служащего, следует рассматривать, исходя из того, что признание, соблюдение и защита прав и свобод человека и гражданина определяют смысл и содержание его профессиональной служебной деятельности.

Исходя из сказанного полагаем, что норма о недопустимости разглашения служебных сведений ограниченного доступа в федеральных законах, регулирующих различную государственную службу, должна быть сформулирована следующим образом: «государственный служащий, осуществляющий гражданскую, правоохранительную или военную службу, в интересах обеспечения прав физических и юридических лиц, эффективности государственного управления обязан не разглашать сведения, ставшие ему известными в связи с исполнением должностных обязанностей, в установленном федеральным законом порядке отнесенные к государственной, служебной и иной охраняемой тайне. Нарушение данной обязанности и запрета разглашения сведений ограниченного доступа влечет наступление предусмотренной законом ответственности».

В содержании служебного контракта государственного гражданского служащего могут предусматриваться условия о неразглашении сведений, составляющих охраняемую федеральным законом тайну, и служебной информации, если должностным регламентом предусмотрено использование таких сведений.

В части правового регулирования информационных прав и обязанностей государственных и муниципальных служащих их статус абсолютно аналогичен. Обязательство о неразглашении сведений, составляющих охраняемую законом тайну, согласно законодательства относится к факультативным (дополнительным) условиям служебного контракта, включаемым в контракт по соглашению сторон. Однако в том случае, когда исполнение обязанностей по соответствующей должности предполагает работу со сведениями, составляющими государственную или иную охраняемую законом тайну, допуск к такого рода сведениям становится обязательным условием замещения соответствующей должности. В условиях действующего законодательства следует согласиться с отнесением совокупности таких условий специалистами к «условно-обязательным» или «казуально обязательным»[22].

Вместе с тем, возможна ситуация при которой гражданин успешно пройдя конкурсный отбор на замещение вакантной должности гражданской службы откажется включить в служебный контракт условие о неразглашении государственной или иной охраняемой тайны. С одной стороны, по результатам конкурса он должен быть назначен на вакантную должность и нет оснований для отмены акта о назначении, а с другой – его невозможно допустить к исполнению служебных обязанностей и к работе со сведениями, составляющими охраняемую законом тайну[23].

Законодательство, регулирующее охрану государственной тайны, содержит определенный порядок допуска к сведениям, составляющим государственную тайну, который предусматривает возможность заключения договора (контракта) только после оформления допуска к государственной тайне, если трудовые или служебные обязанности оформляемого лица предполагают работу с названными сведениями.

Думается, что условия о неразглашении охраняемой законом тайны для должностей, исполнение которых невозможно без доступа к служебным сведениям ограниченного доступа, должны быть включены в служебный контракт в качестве существенного (обязательного) условия. В законодательство о государственной службе должна быть внесена норма, предусматривающая допуск претендентов к прохождению конкурса на вакантную должность государственного гражданского служащего только после подписания о неразглашении охраняемой законом тайны.

Мероприятия по допуску к охраняемой законом тайне проводятся с согласия государственного или муниципального служащего, что согласуется с действующим законодательством о государственной тайне.

Права и обязанности государственных и муниципальных служащих конкретизируются в типовых и индивидуальных должностных инструкциях. В публичных органах фактически действует разрешительная система ознакомления со сведениями, составляющими служебную тайну.

Анализ норм законодательства, регулирующего статус государственного и муниципального служащего, создают основания для отнесения его к базовому представителю держателя служебной тайны. Однако не всегда лицо, представляющее государственный орган управления, имеет статус публичного служащего. Например, лица, имеющие статус судьи, не включены в систему государственной службы. По справедливому замечанию Е.Г. Крыловой, «признание непосредственного осуществления правосудия государственной службой вступило бы в непримиримое противоречие с основополагающими идеями, основными общепризнанными принципами организации и деятельности независимого суда»[24].

Статус публичного служащего отсутствует также у сотрудников публично-правовых образований, не включенных в систему органов государства и вместе с тем реализующих отдельные элементы государственных функций, на основании договоров с государственными и муниципальными органами.

Особый специфический статус имеют государственные правоохранительные и государственные военные служащие. В служебной деятельности военнослужащих большое место занимает обеспечение конфиденциальности государственно значимой информации ограниченного доступа: служебных сведений военного характера, охраняемых в режиме государственной и служебной тайны. Военнослужащие, призванные по призыву, не имеют статуса государственных служащих, что, однако, также не освобождает их от обязанности обеспечения конфиденциальности сведений, охраняемых законом в режиме государственной или служебной тайны.

Понятие «государственная правоохранительная служба» или «служащий правоохранительной службы» законодательством не определено. В своей деятельности сотрудники правоохранительной службы по обеспечению правопорядка и общественного порядка, борьбы с административными правонарушениями и преступлениями имеют более широкие по сравнению с иными государственными служащими права по сбору, систематизации, хранению и использованию сведений, прямо или косвенно затрагивающими права, свободы и законные интересы других лиц. Поэтому в их служебной деятельности традиционно используется широкий круг сведений, охраняемых в режиме служебной тайны. Примечательно, что в системе правоохранительной и военной службы не нашел отражения принцип открытости и транспорентности, что не исключает применение ими общих начал государственной службы в информационной сфере.

Разглашение служебной информации рассматривается законодательством как грубое нарушение должностных обязанностей. Формулировка обязанности служащего не разглашать всякую служебную информацию на фоне отсутствия адекватного регулирования режима служебной тайны ставит публичного служащего в затруднительное положение.

Всех служащих органов государственного управления можно разделить на представителей власти (государственные должности), специалистов (государственные и муниципальные служащие) и вспомогательный технический персонал.

Так как в информационных процессах органов государственного управления участвуют практически все сотрудники органа, выполняющие профессиональную интеллектуальную деятельность, вне зависимости являются они публичными служащими или работниками, исполняющими трудовые обязанности на основе трудового договора, то полагаем, что права и обязанности служащих в части обеспечения конфиденциальности сведений, составляющих служебную тайну, должны быть распространены на всех сотрудников публичного органа. Поэтому любую интеллектуальную профессиональную деятельность гражданина, протекающую в публичном органе или ином публично-правовом образовании, реализующем отдельные элементы государственных функций, можно считать достаточным основанием для отнесения к потенциальным носителям сведений, составляющих служебную тайну.

Разграничение между публичными служащими и лицами, работающими в органе государственного управления и не имеющими такого статуса, лежит в непосредственном обеспечении выполнения функций государственных органов. Обеспечивающих специалистов и работников традиционно во всех странах выводятся за пределы системы публичной службы. Однако это не дает оснований вывести их из системы информационного обеспечения публичного органа.

С.В. Качушкин предлагает служебные отношения публичной гражданской службе разделять на внутренние и внешние[25]. Технические и обеспечивающие сотрудники не участвуют во внешне-властных информационных отношениях, но, являются субъектами внутренних информационных отношений публичного органа.

Государственные органы могут привлекать к своей деятельности экспертов и специалистов. Полученная экспертом или специалистом информация, составляющая коммерческую, банковскую или иную охраняемую законом тайну и переданная органам власти, а также иная конфиденциальная информация не должна ими разглашаться, использоваться в личных или иных целях. Привлечение лица в качестве специалиста или эксперта осуществляется на основе договора, в котором должны быть предусмотрены соответствующую обязанность.

В процессе своего функционирования органы государственного управления принимают активное участие в процессе подготовки бакалавров, специалистов и студентов-магистрантов различных направлений, в том числе выступая базами учебных, производственных, научно-исследовательских и преддипломных практик. В ходе практики студенты-практиканты могут получить и фактически получают доступ к материалам и документам, содержащим персональные данные различных лиц и иную информацию ограниченного доступа. Однако за исключением ситуаций допуска к государственной тайне данный вопрос практически никак не урегулирован.

Суммируя все вышесказанное, можно утверждать, что обеспечение конфиденциальности сведений, охраняемых в режиме служебной тайны, обязаны обеспечивать:

- лица, имеющие статус государственного и муниципального служащего;
- работники органов государственного управления и иных публично-правовых образований, включенные в систему информационно- служебных отношений;
- лица, привлекаемые к деятельности публичных органов на договорной основе и иные, ознакомленные со служебными сведениями ограниченного доступа.

Элементом статуса публичной службы выступает соответствие господствующим в обществе нормами этики и морали. В данном аспекте следует поддержать предложение ряда депутатов Государственной Думы Российской Федерации о введении обязательной присяги граждан поступающих на государственные должности, что позволит повысить персональную ответственность за принимаемые и реализуемые решения в информационной сфере[26].

Государственная и муниципальная служба современной России нуждается в укреплении ее авторитета, повышении профессионализма, открытости, преодолении коррупционной составляющей. Считаем, что одним из важнейших направлений решения перечисленных проблем является конкретизация статуса государственного и муниципального служащего как носителя служебных сведений.

Примечания

1. См: Лопатин В.Н. Правовая охрана и защита служебной тайны // Государство и право. – 2000. № – 6. – С. 85-91; Пономарева Ю.В. Актуальные вопросы служебной тайны // Вестник УрФО. Безопасность в информационной сфере. – 2013. – № 4 (10). – С. 23.

2. Указ Президента РФ от 06.03.1997 № 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера» // Собрание законодательства РФ. 10.03.1997. № 10. Ст. 1127.

3. Постановление Правительства РФ от 03.11.1994 № 1233 (ред. от 20.07.2012) «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти и уполномоченном органе управления использованием атомной энергии» // Собрание законодательства РФ. 25.07.2005. № 30 (ч. II). Ст. 3165.

4. См.: Гудимов В. Ответственность за разглашение коммерческой тайны // Российская юстиция. – 1998. – № 2. Информационно-правовой портал ГАРАНТ.РУ. URL: http://base.garant.ru/986925/ (дата обращения: 11.11.2015); Гаврилов Э. К вопросу об охране коммерческой, служебной и личной тайны. Гражданско-правовые аспекты // Хозяйство и право. – 2003. – № 5. – С. 29; Городов О.А. Информационное право: учебник для бакалавров. – М.: Проспект, 2014. – С. 71; Братановский С.Н., Лапин С.Ю. Типы и виды информации в деятельности органов государственной власти и местного самоуправления // Гражданин и право. – 2014. – № 1. – С. 21 и др.

5. Бушков Д.В. Тайна личной корреспонденции в уголовном праве: дис. … канд. юрид. наук . – Ставрополь, 2003. – С. 121.

6. Яковец Е.Н., Смирнова И.Н. Нормативное регулирование оборота сведений, составляющих служебную тайну // Информационное право. – 2009. – № 4. – С. 18.

7. См.: Чаннов С.Е. Административно-правовая модель регулирования служебных отношений в Российской Федерации: понятие и основные черты: автореф. дис. ... докт. юрид. наук. – Саратов, 2010. – С. 24.

8. Черепанова И.В. Фактическая и юридическая природа государственной гражданской службы (часть 1) // Вестник Омского университета. Серия Право. – 2015. – № 1 (42). – С. 71.

9. См.: Качушкин С.В. Конституционно-правовые основы государственной гражданской службы: автореф. дис. … докт. юрид. наук. – М., 2011. – С. 20.

10. См.: Гусев А.В. Государственная гражданская служба Российской Федерации: Проблемы правового регулирования: автореф.: дис … докт. юрид. наук. – Екатеринбург, 2009. – С. 8.

11. См.: Толковый словарь живого великорусского языка Владимира Даля. URL: http://slovari.yandex.ru/ (дата обращения: 06.08.2013).

12. См.: Граждан В.Д. Теория управления: Учебное пособие. – М.: Гардарики, 2005. – С. 269-273.

13. Атамчук Г.В. Сущность государственной службы: история, теория, закон, практика / Атаманчук Г.В.– М.: Изд-во РАГС, 2002. – С. 113.

14. Напр., в положениях Уголовного кодекса Российской Федерации. Данное обстоятельство отмечалось специалистами (В.Н. Лопатин) еще в начале века.

15. См.: Старилов Ю.Н. Служебное право: уже реальность или пока научная гипотеза // Правовая наука и реформа юридического образования. – 2013. – № 3 (26). – С. 99-116.

16. См: Атаманчук Г.В. Указ. соч. – С. 54; Чаннов С.Е. Особенности юридической природы государственной службы // Алтайский вестник государственной и муниципальной службы. – 2008. – №1. – С. 55.

17. Федеральный закон от 27.07.2004 № 79-ФЗ (ред. от 30.12.2015) «О государственной гражданской службе Российской Федерации» // Собрание законодательства Российской Федерации. 02.08.2004. № 31. Ст. 3215; Официальный интернет-портал правовой информации http://www.pravo.gov.ru - 30.12.2015.

18. Федеральный закон от 02.03.2007 № 25-ФЗ (ред. от 04.03.2014) «О муниципальной службе в Российской Федерации» // Собрание законодательства Российской Федерации. 05.03.2007. № 10. Ст. 1152.

19. См.: Хатюшенко О.М. Административно-правовой статус государственного служащего РФ: дис. ... канд. юрид. наук. – М., 1999. – С. 38; Кулешов Г.Н. Информационное обеспечение статуса государственного гражданского служащего // Административное и муниципальное право. – 2009. – № 12. – С. 28-33.

20. См: Крылова Е.Г. Формирование системы государственной службы Российской Федерации в контексте реализации концепции правового государства: автореф. дис. … докт. юрид. наук. – М., 2009. – С. 14.

21. Там же.

22. См: Гарячук И. Содержание служебного контракта о прохождении государственной гражданской службы // Вопросы трудового права. – 2010. – № 9. Информационно-правовой портал ГАРАНТ.РУ. URL: http://base.garant.ru/ 55061528/ (дата обращения: 11.11.2015).

23. Там же.

24. Крылова Е.Г. Формирование системы государственной службы Российской Федерации в контексте реализации концепции правового государства: автореф. дис. … докт. юрид. наук. – М., 2009. – С. 30.

25. См.: Качушкин С.В. Конституционно-правовые основы государственной гражданской службы: Автореф. дис. … докт. юрид. наук. – М., 2011. – С. 25.

26. См.: В Госдуму внесен законопроект об обязательной присяге при вступлении в государственные должности // ГАРАНТ.РУ: URL: http://www.garant.ru/ news/609381/#ixzz3TPbqmSd6 (дата обращения: 04.03.2015).

Камалова Гульфия Гафиятовна, доцент кафедры криминалистики и судебных экспертиз ФГБОУ ВПО «Удмуртский государственный университет», кандидат юридических наук. 426000, г. Ижевск. ул. Университетская, д.1, корп. 4. E-mail: gulfia.kamalova@gmail.com

Kamalova Gulfiia, PhD, Associate Professor Udmurt State University of Department of Criminalistics and Forensic Expertise. Udmurt State University. 426034, Russia, Izhevsk, Universitetskaya st., 1/4. E-mail: gulfia.kamalova@gmail.com

УДК 366.54(470) + 338.439:366.54 Вестник УрФО № 2(20) / 2016, стр. 71–74

Пономарева Ю. В.

СООТНОШЕНИЕ ПРАВОВОГО РЕЖИМА ИНСАЙДЕРСКОЙ ИНФОРМАЦИИ С ИНЫМИ РЕЖИМАМИ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА

Статья посвящена проблемам режима инсайдерской информации в контексте существующих правовых режимов информации ограниченного доступа. Автор ставит вопрос о том, на каком основании режим инсайдерской информации может иметь приоритетный статус по отношению к иным режимам информации ограниченного доступа, устанавливаемого иными федеральными законами. Автор делает вывод о том, что правовая конструкция инсайдерской информации недостаточно проработана в системе законодательства Российской Федерации и плохо соотносится с другими правовыми конструкции информации ограниченного доступа.

Ключевые слова: *инсайдерская информация, режим информации.*

Ponomareva J. V.

LEGAL REGIME OF INSIDER INFORMATION AND OTHER MODES LIMITED ACCESS INFORMATION

The article is devoted to the problems of insider information regime in the context of the existing legal regimes restricted information. The author raises the question of on what basis of insider information regime may have priority status in relation to other modes of limited access information identifying other federal laws. The author concludes that the legal structure of insider information is not well designed in the Russian legislation system and poorly correlated with other legal structure of restricted information.

Keywords: *insider information, the information mode.*

На пороге принятия закона «О противодействии неправомерному использованию инсайдерской информации» велись активные споры об обоснованности применения такого инородного понятия как «инсайдерская информация» в российском законодательстве. Как отмечают исследователи[1], до принятия указанного закона фактическим аналогом понятия «инсайдерская информация» было понятие «служебная информация», которое определялось в законе «о Рынке ценных бумаг» как «любая, не являющаяся общедоступной информация об эмитенте и выпущенных им эмиссионных ценных бумагах, которая ставит лиц, обладающих в силу своего служебного положения, трудовых

обязанностей или договора, заключенного с эмитентом, такой информацией, в преимущественное положение по сравнению с другими субъектами рынка ценных бумаг», а в Гражданском кодексе как «информация, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности». Исследовав указанные формулировки, стоит отметить, что в результате смены политического и общественного строя, в праве понятие «служебная информация» перешло из сферы государственных секретов в сферу коммерческого оборота и одним из новых институтов, вошедших правовую систему Российской Федерации, является институт инсайдерской информации – информации о деятельности предприятий, организаций, которая способна в значительной степени повлиять на цены финансовых инструментов, иностранной валюты и (или) товаров. Вместе с тем, как отмечает ряд исследователей, режим инсайдерской информации достаточно специфичен и неоднороден по своей сути: с одной стороны, это определенное ограничение на доступ к той или иной информации, с другой же стороны, это ограничение носит временный характер. Кроме того, для ряда инсайдеров раскрытие информации, которая образовалась, является обязательным в кратчайшие сроки (пункт 9 ст. 4 ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты российской федерации») – не позднее следующего рабочего дня с момента образования инсайдерской информации. Кроме того, помимо достаточной неординарности представленнной конструкции ограничения доступа к информации, возникает вопрос о соотношении режимов инсайдерской информации и других режимов информации ограниченного доступа. Закон дает следующее определение инсайдерской информации:

Инсайдерская информация - точная и конкретная информация, которая не была распространена или предоставлена (в том числе сведения, составляющие коммерческую, служебную, банковскую тайну, тайну связи (в части информации о почтовых переводах денежных средств) и иную охраняемую законом тайну), распространение или предоставление которой может оказать существенное влияние на цены финансовых инструментов, иностранной валюты и (или) товаров (в том числе сведения, касающиеся одного или нескольких эмитентов эмиссионных ценных бумаг (далее - эмитент), одной или нескольких управляющих компаний инвестиционных фондов, паевых инвестиционных фондов и негосударственных пенсионных фондов (далее - управляющая компания), одного или нескольких хозяйствующих субъектов, указанных в пункте 2 статьи 4 настоящего Федерального закона, либо одного или нескольких финансовых инструментов, иностранной валюты и (или) товаров) и которая относится к информации, включенной в соответствующий перечень инсайдерской информации, указанный в статье 3 настоящего Федерального закона. Отметим, что в определении инсайдерской информации фигурирует упоминание о том, что к такой информации может быть отнесены и сведения, относящиеся к охраняемой законом тайне. Такое пересечение правовых режимов, а главное, их соотношение, вызывает множество вопросов. В период принятия указанного закона велось много споров о том, насколько соотносится понятие «инсайдерская информация» с понятием «служебной информации», какое из понятий шире, насколько оправданно использование в законодательстве понятия «служебной информации»[2]. Такие споры велись на фоне существующего в то время законодательного определения «служебной информации» в законе «О рынке ценных бумаг» (В соответствии с Законом «О рынке ценных бумаг» Служебной информацией для целей настоящего Федерального закона признается любая не являющаяся общедоступной информация об эмитенте и выпущенных им эмиссионных ценных бумагах, которая ставит лиц, обладающих в силу своего служебного положения, трудовых обязанностей или договора, заключенного с эмитентом, такой информацией, в преимущественное положение по сравнению с другими субъектами рынка ценных бумаг). Кроме того, велись споры о соотношении понятий «служебная тайна» и «служебная информация», а также о круге общественных отношений, которые должны охватываться указанными понятиями. После же принятия закона «О противодействии…» было исключено понятие «служебная информация» из закона «о рынке ценных бумаг», однако во-

прос о соотношении понятий и приоритете правовых режимов не был до конца снят.

В том виде, в котором сейчас существует институт «инсайдерской информации», он практически не сохранил черт и свойств «служебной тайны», в том смысле, в котором она понималась еще в первоначальной редакции федерального закона «О рынке ценных бумаг».

До сих пор неясно соотношение правовых режимов инсайдерской информации и иной охраняемой законом тайны. Исходя из формулировки, указанной в законе, можно прийти к выводу о частичном «поглощении» режимом инсайдерской информации иных режимов охраняемых законом тайн. Так, некоторые исследователи считают, что «В случае же с инсайдерской информацией при совпадении содержания сведений происходит поглощение одного режима другим и «приоритет» отдается правовому режиму инсайдерской информации».[3] Однако на наш взгляд, для такого однозначного утверждения нет достаточных предпосылок: во-первых, с формально-юридической стороны, Федеральный Закон «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты российской федерации» имеет одинаковую юридическую силу по сравнению с иными федеральными законами, устанавливающими режим тайны. Кроме того, он не отменяет действия иных федеральных законов, он не является специальным законом по отношению к иным федеральным законам о тайнах, который бы мог иметь приоритет перед ними, более того, из формулировок названного закона следует, что режим инсайдерской информации действует наряду с иными режимами ограничения доступа к информации. Вместе с тем не ясно, как же происходит такое «сосуществование режимов»: так, к примеру, неясно, на каком основании информация, отнесенная, к примеру, к коммерческой или банковской тайне, должна распространяться и каким образом режим такой «коммерческой тайны» в отношении указанной информации может сохраниться. Кроме того, сосуществование режима инсайдерской информации и режима служебной тайны представить крайне сложно. Исходя из прямых нормативных предписаний, инсайдеры, указанные в п. 9 ст.4, коими являются федеральные органы исполнительной власти, исполнительные органы государственной власти субъектов Российской Федерации, органы местного самоуправления, иные осуществляющие функции указанных органов органы или организации, органы управления государственных внебюджетных фондов, имеющих в соответствии с федеральными законами и иными нормативными правовыми актами Российской Федерации право размещать временно свободные средства в финансовые инструмент, Банк России, обязаны раскрывать или предоставлять инсайдерскую информацию на их официальных сайтах в информационно-телекоммуникационной сети «Интернет» не позднее следующего рабочего дня с момента ее появления (возникновения). И если вспомнить, что, исходя из теоретических подходов к определению служебной тайны, к ней относится информация, которая стала известна в силу указаний закона, являющейся конфиденциальной информацией о юридических и физических лицах, а также информация, вырабатываемая внутри государственных органов и органов местного самоуправления, возникает вопрос относительно того, как информация, которая сама по себе является коммерческой, служебной тайной может быть обязательной для публикации?

Также возникает вопрос относительно того, любая ли информация, попадающая под категорию «инсайдерской» должна быть раскрыта в обязательном порядке. Неясно, почему законодатель в определении перечисляет отдельные виды информации ограниченного доступа, такие как служебная, коммерческая тайна, банковская тайна, тайна связи (изъятие) и обобщает иные виды информации под категорией «иная охраняемая законом тайна». В данном случае представляется недопустимым распространение режима инсайдерской информации на сведения, составляющие, к примеру, государственную тайну. Поскольку в этом случае наступление уголовной ответственности за разглашение такой информации никак не зависит от того, подпадали ли такие сведения под категорию «инсайдерской информации». Налицо неразрешенная правовая коллизия, которая не имеет однозначного ответа.

Стоит отметить, что указанный правовой институт в нашем правопорядке не сформировался однозначно. Поскольку если обратиться к зарубежному опыту, то в отношении инсайдерской информации там существует

иное регулирование. На международном уровне функционирует Международная организация комиссий по ценным бумагам, которая выработала цели и принципы регулирования.[4] Указанные цели и принципы подразумевают соблюдение интересов инвесторов, повышение прозрачности рынка и снижение рисков. Регулирование должно быть в рамках баланса между экономической прозрачностью и сохранением фидуциарности договорных отношений.[5]

И в данном случае цели и принципы регулирования инсайдерской информации чрезвычайно важны, поскольку позволяют определять разумные меры для соблюдения интересов общественных и частных. Так, в США запрещается использование инсайдерской информации для оперирования финансовыми инструментами и совершение сделок с ценными бумагами. При этом требование раскрытие такой информации достаточно узко. Закон требует немедленного раскрытия информации только в случае, когда такая информация была частично разглашена либо передана (умышленно либо неумышленно). Для раскрытия такой информации дается всего лишь сутки в законодательстве США. Однако такое требование касается достаточно узкой категории сведений, которые были переданы третьему лицу.[6]

В странах Европы же существует требование инсайдерской информации для общественности, однако закон предусматривает возможность задержать компанией выход такой информации с целью соблюдения интересов компании. В некоторых же случаях закон говорит о возможности требования государственных органов о приостановлении распространения такой информации.[7]

Стоит отметить, что в зарубежных правопорядках нет прямого указания на приоритет режима инсайдерской информации над другими режимами ограниченного доступа, что снимает вопрос противоречия различных режимов тайн. Кроме того, такое регулирование (что Американская, что Европейская модель) позволяет соблюдать как интересы прозрачности торговли ценными бумагами, так и интересы прав инвесторов, что немаловажно. В нашей же правовой системе институт инсайдерской информации плохо согласован с другими режимами информации ограниченного доступа и не отвечает требованиям баланса интересов сторон.

Примечания

1. Вавулин Д.А. Комментарий к Федеральному закону «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации. М.: Деловой двор, – 2015

2. Погосова (Фролова) А.С. Инсайдерская и служебная информация: соотношение понятий. / А.С. Погосова (Фролова). Электронный ресурс, 2010. URL: http://www.juristlib.ru/book_9079.html

3. Ахмадуллина А.Ф. К вопросу о правовом режиме инсайдерской информации / А.Ф. Ахмадуллина // Вестник ВУиТ, ¬¬ – 2014. № 2. – С. 62-73.

4. IOSCO Objectives and Principles of Securities Regulation URL: [http://www.iosco.org/library/pubdocs/pdf/IOSCOPD154.pdf]

5. Comparing Insider Trading in the US and Europe URL:[https://corpgov.law.harvard.edu/2014/06/19/comparing-insider-trading-in-the-us-and-europe/]

6. Final Rule: Selective Disclosure and Insider Trading URL: [https://www.sec.gov/rules/final/33-7881.htm]

7. Directive 2003/6/EC of the European Parliament and of the Council of 28 January 2003 on insider dealing and market manipulation (market abuse) URL: [http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32003L0006&rid=1]

Пономарева Юлия Владимировна, аспирант кафедры конституционного и административного права юридического факультета Южно-Уральского государственного университета. 454084, г. Челябинск. E-mail: julia.ponomareva17@mail.ru

Ponomareva Julia, postgraduate student of Constitutional and Administrative Law of the South Ural State University. 454084, Chelyabinsk. E-mail: julia.ponomareva17@mail.ru

ВИКТИМОЛОГИЯ

Новый научно-практический журнал **ВИКТИМОЛОГИЯ** посвящен актуальным проблемам отечественной виктимологии – вполне сложившейся подотрасли криминологии, имеющей признаки самостоятельной правовой дисциплины – криминальная виктимология, а также как самостоятельное научное направление, изучающее лиц, ставших жертвами несчастных случаев, стихийных бедствий, катастроф и т. д., изучение которых охватывает широкий спектр познаний в области социологии, психологии, педагогики и других научных направлений.

Виктимология сегодня – это развивающееся комплексное учение о лицах, находящихся в кризисном состоянии и обладающих определенной степенью виктимности, о причинах и условиях виктимизации, о жертвах преступности, стихийных бедствий, катастроф и пр., а также о мерах и способах обеспечения защищенности и оказания помощи таким жертвам.

Особое внимание предполагается уделить исследованию предмета и источников виктимологии, международных правовых норм и норм отечественного законодательства в области защиты жертв; рассмотрению проблем, связанных не только с обеспечением правовой и иной безопасности жертв преступности, но и вопросов, связанных с их реабилитацией; анализу причин виктимного поведения и виктимизации современного общества; характеристике субъектов государственной и негосударственной деятельности в области виктимологической профилактики и защиты; возможностям самих граждан как субъектов виктимологического противодействия преступности. Данный журнал может стать полезным не только ученым в различных отраслях знаний, изучающих жертв, но и практикующим психологам, юристам, педагогам и широкому кругу читателей.

РУБРИКИ ЖУРНАЛА:

- Теория учения о жертве
- Современная виктимология
- Виктимология и безопасность
- Виктимологическая профилактика
- Криминальная виктимология
- Психология поведения жертв
- Ювенальная виктимология
- Зарубежная виктимология
- Обзор виктимологического законодательства

Подготовленные статьи необходимо отправить на E-mail: victimologiy@mail.ru

ВЕСТНИК УрФО
Безопасность в информационной сфере № 2(20) / 2016

Дата выхода в свет 20.06.2016. Формат 70×108 1/16. Печать трафаретная.
Усл.-печ. л. 6,3. Тираж 100 экз. Заказ 179/256.
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. 2(20) / 2016

Date of publication of the 20.06.2016. Format 70×108 1/16. Screen printing.
Conventional printed sheet 6,3. Circulation – 100 issues. Order 179/256. Open price.

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