ISSN 2225-5435

Вестник УрФО

БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ

№ 2(16) / 2015

УЧРЕДИТЕЛЬ
ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ГЛАВНЫЙ РЕДАКТОР
ШЕСТАКОВ А. Л.,
д. т. н., проф., ректор ЮУрГУ

ОТВЕТСТВЕННЫЙ РЕДАКТОР
РАДИОНОВ А. А.,
д. т. н., проф., проректор ЮУрГУ

ВЫПУСКАЮЩИЙ РЕДАКТОР
СОГРИН Е. К.

ВЁРСТКА
ПЕЧЁНКИН В. А.

КОРРЕКТОР
БЫТОВ А. М.

Подписной индекс 73852 в каталоге «Почта России»

16+

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

TECHNICAL MEANS AND METHODS OF INFORMATION PROTECTION

COMPUTER SECURITY

ORGANIZATIONAL AND LEGAL PROTECTION INFORMATION

LEGAL REGULATION OF INFORMATION SECURITY

ACTUAL PROBLEMS OF CYBERSECURITY

REVIEWS, REVIEWS

THE PRACTICAL ASPECT

УДК + 004.056.5

Антясов И. С., Соколов А. Н.

ГРАНИЧНЫЕ УСЛОВИЯ ДЛЯ ВЕКТОРОВ ЭЛЕКТРОМАГНИТНОГО ПОЛЯ НА ПОВЕРХНОСТИ ЭКРАНА НА ОСНОВЕ ПРОВОЛОЧНОЙ СЕТКИ

Рассмотрены особенности оценки эффективности электромагнитного экранирования альтернативных измерительных площадок. Представлены факторы, влияющие на эффективность применения сетчатых экранов. Поставлена задача адаптации метода усредненных граничных условий к расчету параметров экранов с учетом поперечных токов в проводниках.

Ключевые слова: *технический канал утечки информации, электромагнитное поле, экранирование, радиопоглощение, сетчатые структуры, коэффициент поглощения, коэффициент отражения.*

Antyasov I. S., Sokolov A. N.

BOUNDARY CONDITIONS FOR ELECTROMAGNETIC FIELD VECTORS ON THE SCREEN SURFACE BASED WIRE MESH

The specific features of evaluating the effectiveness of electromagnetic shielding of alternative test sites. Presents the factors affecting the effectiveness of mesh screens. The aim is to adapt the averaging method of boundary conditions for the calculation of the parameters screens with the cross-currents in conductors.

Keywords: *technical channel information leakage electromagnetic field shielding radiopogloschenie, mesh structure, the absorption coefficient, the reflection coefficient.*

Электромагнитное экранирование играет существенную роль при построении альтернативных измерительных площадок (АИП) [1]. С этой целью возможно применение листового металла, фольги или металлических сеток [2]. Однако применение сплошного листового металла или фольги затрудняет решение задачи эффективного поглощения внутренних электромагнитных волн, вследствие чего становится проблематичным вы-

полнение требований нормативно-методической документации по затуханиям.

В настоящее время с целью электромагнитного экранирования широко применяются сетчатые структуры. Данный выбор обусловлен не только конструктивно-технологическими достоинствами, но и более лучшими характеристиками требуемых климатических условий внутри АИП. Все сетчатые структуры можно разделить на две группы: перфорированные металлические поверхности и проволочные сетки. Проволочные сетчатые структуры получили более широкое распространение. Эффективность электромагнитной защиты при произвольной поляризации источника излучения прежде всего зависит от густоты сетки и формы ячейки, а также от характера контакта между проводниками в их перекрестиях, формы сечения проводников. Поэтому, как правило, применяются двумерно-периодические структуры с размерами ячеек, много меньшими длины волны [3].

Стоит отметить, что эффективность экранирования в ближней зоне (зоне индукции) будет неодинакова для электрической и магнитной составляющих поля. Учитывая рассматриваемый диапазон частот (от десятков кГц до одного-двух ГГц) и небольшие размеры АИП (в среднем 5×3×3 метра), данное замечание будет актуальным на частотах менее 10 МГц. Поэтому в ближней зоне эффективность экранирования должна вычисляться отдельно для каждой компоненты поля, при этом в дальней зоне (зоне излучения) она будет одинаковой для обеих компонент [4].

Физическая сущность экранирования первичного электромагнитного поля (см. рис. 1а) заключается в том, что электрические заряды и токи, возникающие на поверхности экрана S, обращенной к источнику (рис. 1б, область 1), создают вторичное электромагнитное поле, которое во внешнем пространстве (рис. 1б, область 2) по интенсивности близко к полю источника, а по направлению противоположно ему. Это приводит к взаимной компенсации поля источника и вторичного поля эквивалентных поверхностных электрических зарядов и токов во внешнем пространстве [5].

Для решения внутренней задачи по исследованию эффективности экранирования в требуемом диапазоне частот с целью достижения безэховости АИП необходимо наличие коэффициентов прохождения (отражения) в комплексном виде для учета интерференции переотраженных электромагнитных волн. Указанные коэффициенты были рассчитаны в [6] при решении задачи выбора оптимального экрана с учетом ряда факторов (широко распространенные, недорогие, эффективные при минимальной плотности заполнения металлом) в отдельности для сеток с размером ячейки 0,8 мм и диаметром проволоки 0,32 мм и с размером ячейки 0,9 мм и диаметром проволоки 0,36 мм.

При расчете коэффициентов прохождения (отражения) в [6] использовалась приближенная формула для структур с перфорацией квадратными отверстиями. Однако применимость этой формулы к сетчатым экранам весьма ограничена. Поэтому с целью повышения точности модели ставится задача провести исследование коэффициентов прохождения (отражения) двух систем параллельных проводников, расположенных на некотором расстоянии друг от друга.

Существует метод исследования, заключающийся в замене сетчатой структуры с реальными токами и зарядами сплошной поверхностью, на которой выполняются неко-

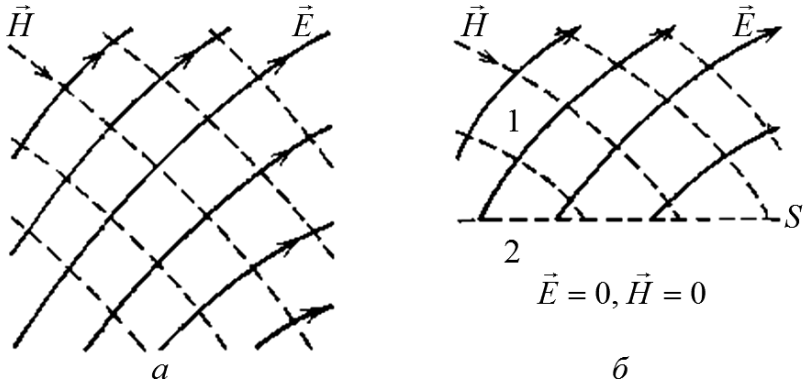

Рис. 1. Электромагнитное поле в пространстве (а) и полупространстве, ограниченном экраном S (б).

торые эквивалентные усредненные граничные условия для сглаженных токов и зарядов так, что на некотором расстоянии от сетки сглаженные и реальные поля равны [3]. Данный метод имеет ограничение по применимости: радиус проводников должен быть много меньшим наибольшего размера ячейки. Это позволяет не учитывать поперечные токи в проводниках (в сравнении с продольными) и облегчает учет неравномерности продольных токов. С целью преодоления этого ограничения ставится задача разработать метод, позволяющий оценивать коэффициенты прохождения (отражения) проволочных сеток с радиусом проводников, близким по значению к размеру ячеек.

Примечания

1. Антясов И. С., Войтович Н. И., Соколов А. Н. Особенности валидации альтернативной измерительной площадки для проведения специальных исследований технических средств // Вестник УрФО. Безопасность в информационной сфере. — Челябинск : Изд. центр ЮУрГУ, 2014. — № 1(11). — С. 10 – 14.

2. Безэховые камеры СВЧ / Мицмахер М. Ю., Торгованов В. А.. – М. : Радио и связь, 1982. – 128 с.

3. Электродинамика сетчатых структур /М. И. Конторович, М. И. Астрахан, В. П. Акимов и др. ; под ред. М. И. Конторовича. – М. : Радио и связь, 1987. – 136 с.

4. Полонский Н. Б. Конструирование электромагнитных экранов для радиоэлектронной аппаратуры. — М. : Сов. радио, 1979. — 216 с.

5. Антясов И. С., Войтович Н. И., Соколов А. Н. Комплексное экранирование альтернативной измерительной площадки для проведения специальных исследований технических средств. // Вестник ЮУрГУ. Компьютерные технологии, управление, радиоэлектроника. — Челябинск : Изд. центр ЮУрГУ, 2014. — № 2 (14).

6. Антясов И. С., Соколов А. Н. Выбор оптимального экрана при построении альтернативной измерительной площадки // 7-я научная конференция аспирантов и докторантов Южно-Уральского государственного университета (национальный исследовательский университет), посвященная Дню Российской науки. — Челябинск, 2015.

Соколов Александр Николаевич, к. т. н., доцент, зав. кафедрой безопасности информационных систем ФГБОУ ВПО «Южно-Уральский государственный университет», г. Челябинск. E-mail: ANSokolov@inbox.ru

Антясов Иван Сергеевич, студент кафедры безопасности информационных систем ФГБОУ ВПО «Южно-Уральский государственный университет», г. Челябинск. E-mail: antyasov@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

Antyasov Ivan, student of Information Systems Security "South Ural State University", Chelyabinsk. E-mail: antyasov@gmail.com

УДК 004.4.056.5

Никольская К. Ю., Хлестов А. Д.

ОБФУСКАЦИЯ И МЕТОДЫ ЗАЩИТЫ ПРОГРАММНЫХ ПРОДУКТОВ

Данная статья нацелена на рассмотрение основных технических методов защиты программных продуктов. Процесс обфускации на сегодняшний день один из самых популярных и часто используемых методов защиты, поэтому он выделен в отдельный блок для более детального изучения.

Ключевые слова: *обфускация, защита программных продуктов, программных продукт.*

Hlestov A. D., Nikolskaya K. U.

OBFUSCATION AND METHODS OF PROTECTION SOFTWARE

This article focuses on the technical review of the main methods of protection software. The process of obfuscation to date one of the most popular and commonly used methods of protection, so it is in a separate block for a more detailed study.

Keywords: *obfuscation, protection of software products, software products.*

Технологии программирования прогрессируют очень быстро. Сейчас исходный код незащищённой программы можно вскрыть без особых усилий, имея некоторую подготовку. Приведу пример технологии .NET, созданной компанией Microsoft. Платформа .NET решает многие проблемы, которые в прошлом омрачали процесс разработки Windows-приложений. Теперь существует одна для всех поддерживаемых платформой языков программирования парадигма разработки приложений. Платформа .NET позволяет разрабатывать мощные, независимые от языка программирования, настольные приложения и масштабируемые (расширяемые) Web-службы, построенные на базе новой мощной полнофункциональной библиотеки классов. Однако защита .NET программ представляет значительную трудность из-за их большой открытости. Приложения для .NET не представляют сложностей для декомпиляции. Однако существует множество методов защиты программных продуктов, которые мы рассмотрим в данной статье.

Основные способы защиты. Не секрет, что любой программный продукт представляет собой некую интеллектуальную собственность. Существует два основных спосо-

ба защиты интеллектуальной собственности (программных продуктов в частности):

1) Юридический. Заключается в создании локальных правовых актов в соответствии с законодательством, которые будут регламентировать использование и защиту интеллектуальной собственности от нелегального использования.

2) Технический. Мы рассматриваем защиту программных продуктов (ПП), поэтому в данном случае технический способ реализуется путём включения в ПП определённых методов защиты, которые будут предотвращать нелегальное использование продукта.

Методы защиты программных продуктов. Опишем наиболее распространённые методы защиты, известные на данный момент.

Выполнение на сервере. Как можно заметить из названия, программа действует по принципу «клиент – сервер». Основной код программы находится на сервере, и её код выполняется на серверной стороне, однако аргументы для работы передаются программой-клиентом. Является одним из самых эффективных методов, но:

1) требует взаимодействия клиента и сервера, что подразумевает наличие сети;

2) скорость работы программы зависит от пропускной способности сети клиента и сервера.

Исходя из этого, данный метод лучше всего использовать для простых программ (сценариев).

Водяной знак (software watermark). Водяной знак – некоторый скрытый код в программном продукте, содержащий информацию о разработчике программы. Водяной знак должен соответствовать следующим требованиям:

• водяной знак должен быть хорошо скрыт в программе и разработчик должен иметь возможность извлечь скрытый код без каких-либо повреждений;

• водяной знак не должен влиять на работу программы;

• водяной знак должен нести определённую информацию о разработчике, которая позволит доказать, что её присутствие в программе неслучайное и является результатом преднамеренных действий.

Для лучшей защиты рекомендуется вставлять в программный продукт несколько водяных знаков. Недостатком такого метода является то, что злоумышленник может обнаружить в программном коде эту информацию и подвергнуть изменению.

Установка подлинности кода (tamper-proofing). Данный метод реализуется путём внедрения в программный продукт процедуры проверки целостности программы. При попытке изменения программы данная процедура делает её неработоспособной. Процедура не должна быть слишком простой, так как для взлома программы достаточно будет определить место, откуда эта процедура вызывается.

Шифрование программного кода. Данный метод защиты предусматривает зашифровывание кода программы, после чего она в зашифрованном виде поставляется конечным пользователям. Когда пользователь запускает такую программу, вначале будет запущена процедура расшифровки программы, которой потребуется ключ, с помощью которого будет расшифрована запускаемая программа.

Ключ представляет из себя последовательность символов, генерируемых в результате некоторых математических операций. К примеру, ключ может быть привязан к характеристикам компьютера пользователя. Однако это может усложнить работу с программой в случае запуска на другом компьютере.

В последнее время становится актуально использование электронных ключей. Электронный ключ представляет из себя небольшое устройство, подключаемое к одному из портов компьютера (COM, USB и т. д.). Такой метод лучше всего подходит для защиты дорогостоящих ПП. Также он не ограничивает работу на определённом компьютере, как в случае, описанном выше.

Обфускация. Для обхода защиты программы в большинстве случаев требуется изучение программного кода. Этот процесс называется «реверсивная (обратная) инженерия». Что же из себя представляет обфускация? Обфускация (от лат. obfuscare — затенять, затемнять; и англ. obfuscate — делать неочевидным, запутанным, сбивать с толку) — приведение исходного текста программы к виду, сохраняющему его функциональность, но затрудняющему его анализ, понимание алгоритмов работы. То есть, обфускация усложняет процесс реверсивной инженерии. Данный метод не является идеальным и его рекомендуется использовать вместе с другими методами защиты. Это очень сильно повысит общий уровень защищённости программного продукта.

Некоторый процесс трансформации программного кода будет считаться процессом обфускации, если он удовлетворяет следующим требованиям:

• код программы будет существенно отличаться от оригинала, но при этом функционирование программы не изменится;

• изучение трансформированного кода (реверсивная инженерия) будет более сложным и трудоёмким, чем изучение исходного кода;

• при каждом процессе трансформации результирующий код будет различным;

• создание программы обратной трансформации кода будет неэффективно.

Принято выделять следующие уровни процесса обфускации:

• низший уровень, когда процесс обфускации осуществляется над ассемблерным кодом программы или непосредственно над двоичным файлом программы, хранящим машинный код;

• высший уровень, когда процесс обфускации осуществляется над исходным кодом программы, написанном на языке высокого уровня.

Наиболее популярным на данный момент является высший уровень процесса обфускации. На низком уровне должны быть учтены особенности работы процессоров, так как программа после обфускации будет корректно работать на одной архитектуре и некорректно на другой.

Оценка процесса обфускации:

• устойчивость – показывает уровень сложности изучения кода программы, прошедшей процесс обфускации;

• эластичность – показывает защищённость программного кода от применения деобфускаторов (программ для обратного преобразования кода);

• стоимость преобразования – показывает, насколько больше системных ресурсов требует преобразованная программа в сравнении с оригиналом.

Виды обфускации. Существуют различные способы преобразования программ, следовательно, данный процесс подразделяется по видам (способам) такого преобразования. Ниже рассмотрим некоторые из них.

Лексическая обфускация. Наиболее простая, заключается в изменении исходного кода программы для приведения его к нечитабельному виду. Включает в себя: удаление комментариев или изменение их на дезинформирующие; удаление отступов и пробелов; замена имён идентификаторов (имён переменных, функций, процедур и т. д.) на длинные наборы символов, сложных для визуального восприятия; изменение расположения блоков программы.

Обфускация данных. Данный тип обфускации связан с изменением структур данных. Является более сложной, чем лексическая, однако наиболее используемой. Этот вид обфускации делится на 3 группы:

1) Обфускация хранения. Заключается в трансформации хранилищ данных, а также самих типов данных (например, создание и использование необычных типов данных, изменение представления существующих и т. д.);

2) Обфускация соединения. Один из важных этапов в процессе реверсивной инженерии программ, основан на изучении структур данных. Поэтому важно постараться в процессе обфускации усложнить представление используемых программой структур данных. Например, при использовании обфускации соединения это достигается благодаря соединению независимых данных или разделению зависимых;

3) Обфускация переупорядочивания. Заключается в изменении последовательности объявления переменных, внутреннего расположения хранилищ данных, а также переупорядочивании методов, массивов, определенных полей в структурах и т. д.

Превентивная обфускация. Данный вид обфускации предназначен для предотвращения успешного применения деобфускаторов к коду программного продукта. Нацелен на использование недостатков часто используемых программных средств деобфускации.

Никольская Ксения Юрьевна, преподаватель кафедры «Безопасность информационных систем» ЮУрГУ, г. Челябинск. E-mail: bambucha13@mail.ru

Хлестов А. Д., студент ЮУрГУ, г. Челябинск

Nikolskaya Ksenia, Lecturer, Department of Information Systems Security SUSU, Chelyabinsk. E-mail: bambucha13@mail.ru

Hlestov A. D., student SUSU, Chelyabinsk

УДК 342.5 : 004.056

Пономарева Ю. В.

ИСТОРИЯ ОГРАНИЧЕНИЯ ДОСТУПА К ИНФОРМАЦИИ О ДЕЯТЕЛЬНОСТИ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ (ГОСУДАРСТВЕННАЯ И СЛУЖЕБНАЯ ТАЙНА)

Статья посвящена истории возникновения и развития охраны информации в сфере государственного управления. В статье подробно рассмотрены различные нормативные источники, начиная с XV века. Дается подробная характеристика возникающих на разных этапах институтов ограничения доступа к информации. Особый интерес представляет в статье анализ законодательства, действовавшего в отношении государственных и «партийных» секретов, начиная с 1917 года. Автор приходит к выводу о том, что даже в период существования Советского Союза положение такой категории информации ограниченного доступа, как «служебная тайна», в системе охраняемой информации не было четко нормативно закреплено и под гриф «ДСП» попадали многие сведения, которые мало общего имели с системой государственного управления.

Ключевые слова: *информация ограниченного доступа, секретная информация, конфиденциальность, тайна.*

Ponomareva J. V.

HISTORY LIMITED ACCESS TO INFORMATION ABOUT THE ACTIVITIES OF GOVERNMENT (STATE AND OFFICIAL SECRETS)

The article is devoted to the history and development of data protection in the field of public administration. Detailed legal institutions of restricted information in different historical periods. Of particular interest is the article analysis of the legislation in force in relation to the state and «party» secret since 1917. The author concludes that even in the period of the Soviet Union,

the situation of such a category of restricted information as «official secret» in the protected information was not clearly legal fixed and classified as «Confidential» got many details that had nothing to do with system of government

Keywords: *to information of a limit access, secretinformation, confidentiality, secret.*

С момента возникновения древних государств люди осознавали значение и важность различной информации, а также нежелательность её распространения в той или иной степени. Охрана «государственных секретов» всегда была одной из важнейших задач, которая стояла перед аппаратом государственного управления. Пожалуй, одной из самых древних тайн государственного управления можно назвать военную тайну, когда ограничение доступа к информации о стратегии, тактике ведения боя, а также место дислокации воинских подразделений играло жизненно важную роль для всего государства. Однако особую роль в функционировании государственного аппарата и в управлении государством всегда играли государственные секреты.

Вплоть до XVII века отношения между правителем и подчиненными регулировались широким и всеобъемлющим понятием «верность» [7]. Сложно сказать, было ли возникновение этого понятия связано с нравственными основами служения правителю или же оно основывалось на имущественной зависимости подчиненных. Чаще всего произносилась устная клятва правителю, которая и была определенной гарантией верности. [8]. В понятие верности входила, как правило, готовность «сложить голову» за князя, которому служил дружинник. Поэтому связывать понятие «верности» с обязанностью хранить в тайне определенную информацию было бы ошибочным. В дальнейшем же понятие «верности» приобрело более широкое и даже всеобъемлющее значение в отношении службы государю.

Одним из первых упоминаний о секретности считается упоминание об особом порядке рассмотрения секретных дел в Указе Петра I от 4 апреля 1714 года № 2791 «О заведении в Сенатах, в Советах Военных и Губернских протоколов для внесения в оные определения по всем делам, о недачи голосов при совещании, о подписании членами собрания протоколов, о составлении решительного определения по большинству голосов и о записи в протокол особенных мнений, несогласных с общим решением» [13, ст. 2791]. В этом указе прописан особый порядок рассмотрения секретных дел, а также особый порядок допроса свидетелей. Из данного Указа не явствует, что эти секретные дела носили исключительно государственный характер. Секретность понимается здесь в широком смысле.

Однако вопреки распространенному мнению это упоминание не является первым упоминанием о соблюдении тайны в отношении дел государевых.

Интересно изучить некоторые формы присяги разных чиновников и проследить определенное развитие «тайности» деятельности государственного аппарата.

В форме присяги разных чиновников [13, Т. 1. С. 255] от 31 августа 1651 года упор делается на верность государю и несение государевой службы «без хитрости», указания на обязательность сохранения в тайне той или иной информации отсутствуют. Однако уже буквально через два года была утверждена иная форма присяги разных чиновников, в которой чиновникам некоторых должностей предписывалось «государская думы и Боярского приговору никому до Государева указа не сказывати», а дьяк должен был «тайные государевы и всякие дела хранить в секрете» [13, Т. 1, С. 311, 314]. То есть начинает наблюдаться тенденция постепенного засекречивания государственных дел и государственной службы. При этом отсутствует выделение государственной тайны как сведений определенного свойства. Отмечается лишь необходимость неразглашения тайных государевых дел. Безусловно, следует помнить о том, что ещё в 1653 году Царем Алексеем Михайловичем был учрежден Приказ тайных дел. В этом приказе заседали дьяк и 10 подьячих. Именно с введением тайного приказа можно связывать возникновение государственной тайны как политико-правового явления и, соответственно, такое закрепление формы присяги с включением соответствующих обязательств.

Одним из первых «секретных» документов (дошедших до наших дней и имеющихся в свободном доступе) можно назвать царский указ именной, **объявленный в разряд тайных дел** подьячим «О наказании кнутом по-

дьячего за прописку государева наименования» (1658 г.) [13, Т. 1. С. 459]. Для исследования он ценен не своим содержанием, а своей формой: указ объявлен в разряд тайных дел. Эта маленькая деталь свидетельствует о том, что началось использование особого оформления и обозначения документов, содержащих информацию, относимую к государственной тайне.

Следующее упоминание о секретах в сфере государственного управления встречается в Генеральном регламенте 1720 года. В этом нормативном акте устанавливается впервые секретный характер ведения государственных дел: «...повелевает его величество накрепко, чтоб все, что при коллегиях чинится, а наипаче ежели такие дела, которые его царского величества высокой службе и интереса касаются, тайно содержаны и весьма прежде времени явны не были» [14. С.127] . Кроме того, обязательство неразглашения государственных тайн есть и в клятве, которую должны были давать присяжные: «Когда же к службе и пользе его величества, какое тайное дело, или какое б оно ни было, которое приказано мне будет тайно содержать<...>по совести своей исправлять» [14. С. 110]. Также в этом регламенте предусматривались наказания для тех, «кто злым образом на время, или вовсе, тайно из коллегийных писем и документов что унесет». Стоит отметить, что конкретное наказание не предусматривалось, а лишь предполагалось соответствующим «важности дела». Если мы проанализируем данные положения, то обнаружим, что понятие «тайна государственного управления» не было определено, не были определены критерии и порядок отнесения информации к тайной. Несмотря на это, в нормативном акте прописаны три наиболее важных аспекта правового регулирования:

1) обязанность государственных служащих хранить тайну (субъекты правоотношений) и своеобразная «процедура допуска к тайне» в форме клятвы;

2) необходимость ведения в коллегиях и канцеляриях дел тайно (гипотеза и диспозиция);

3) предусмотрено наказание за разглашение тайны (санкция).

Таким образом, можно говорить о зарождении института тайны государственного управления. Следует отметить, что в данном случае речь не идет о зарождении института государственной тайны в современном его понимании, так как нет предписания сохранения информации в тайне в зависимости от содержания. Так, в Генеральном регламенте предписывалось: «повелевает его величество накрепко, чтоб все, что при коллегиях чинится <...> тайно». В данном случае речь можно вести не только о сохранении в тайне информации о делах государственной важности, но и о сохранении в тайне внутренней информации коллегии. Если в данном случае проводить аналогию с современностью, то такую внутреннюю информацию коллегий можно отнести к тайне служебной.

В дальнейшем развитие нормативной базы можно проследить в Указах Петра I от 13 января 1724 г. «О неписании секретных дел в партикулярных письмах», от 16 января 1724 г. «О поручении секретных дел в Сенате благонадежным людям» и в Приказе Правительствующего Сената от 5 марта 1724 г. «О надписях на пакетах, в которых секретные дела» [13, Т. 7. Сс. 4409, 4418, 4481].

В Указе от 13 января 1724 г. «О неписании секретных дел в партикулярных письмах» встречаем следующее указание: «О делах, которые тайности подлежат в государственных делах, оного отнюдь в партикулярных письмах ни к кому не писать». В этом указании можно отметить выделение круга тайной информации в зависимости от её содержания и от её государственного значения. Такое выделение очень важно, так как в данном документе уже запрещается разглашать не вообще всю информацию, которая есть в органах аппарата управления, а лишь ту, которая «полежит тайности в государственных делах». Таким образом, буквально начинает выделяться тот объект (информация), который и должен подлежать правовой защите.

В Указе от 16 января 1724 г. «О поручении секретных дел в Сенате благонадежным людям» предписывалось следующее: «учините <...>, чтобы секретные дела были особливо у надежных людей». В этом Указе впервые начали устанавливаться определенные требования к людям, которые получали доступ к секретам государственной службы.

В Приказе Правительствующего Сената от 5 марта 1724 г. «О надписях на пакетах, в которых секретные дела» предусматривался уже особый порядок доставки секретных документов, порядок их оформления: «доношения и прочия письма, в которых писать случится о каких секретных делах, посылать за печатьми в пакетах, на которых подписывать

именно, что оные о секретных делах, а в сенатах таких пакетов секретарям не распечатывать».

Петровская эпоха ознаменовала появления такого правового явления, как секрет (тайна) государственной службы. Несмотря на то, что не было ещё деления информации на различные виды тайны, однако основные положения, регулирующие порядок допуска, сохранения, обращения с информацией такого рода, а также наказания за разглашение тайны были уже прописаны в законодательстве.

В эпоху правления императрицы Екатерины II намеченные тенденции к повышению степени охраны и развития организационно-правовых мер получили своё развитие. Так, в 1765 году был издан Сенатский приказ «Об обозначении на бумагах и конвертах по делам секретным как прежними указами о том предписано». В этом указе предписывалось помечать не только документы, но и конверты пометкой «секретно». Делалось это с целью сохранения тайны и вскрытия конверта только указанным адресатом.

С целью дальнейшего совершенствования делопроизводства был издан Сенатский приказ от 7 января 1768 г. «О подписывании представлений, доношений и рапортов по секретным делам». В указанном документе обращается внимание на нарушение действующего порядка обращения с секретными документами, определены конкретные лица, которые должны подписывать секретные документы. Приказом устанавливается штраф, который взимается в случае нарушения предписанного порядка обращения с секретными документами. Размер штрафа составлял 10 рублей. Это, пожалуй, первая четко установленная санкция за нарушение секретности государственных дел.

В дальнейшем в Уложении о наказаниях уголовных и исправительных 1845 года государственным преступлениям был посвящен целый раздел.

В этом разделе было подробно прописано, что понимается под государственной изменой. Такое детальное регулирование понятия «государственная измена» встречается в законодательстве впервые. В понятие государственной измены включалось также разглашение государственной тайны. Следует отметить, что государственной изменой могло стать разглашение не только государственной тайны, но и иной информации, которая не была секретной: план крепости, порта, гавани, арсенала, укрепленного или иного стана, тех мест, где происходят военные действия, известия о расположении и движении войск, о состоянии армии или других средствах нападения, обороны. Уложение также предусматривало наказание за опубликование планов российских крепостей, иных укрепленных мест, гаваней, портов, арсеналов без дозволения правительства.

Указанное нормативное регулирование представляет немалый интерес, так как в нем устанавливается запрет на разглашение не только государственной тайны, но и иной информации, имеющей стратегическую ценность в случае военных действий. Это свидетельствует о том, что массив информации, имеющей ограниченное распространение, перестает быть однородным и постепенно получает различия в правовом регулировании в зависимости от степени значимости сведений и порядка их обращения.

В Уголовном уложении 1903 года меры ответственности за разглашения различных видов тайн получили свое активное развитие. Во многом это было связано не только с развитием общественных отношений, но и с политической обстановкой того времени. Можно сказать, что в трех главах уложения была предусмотрена ответственность за разглашение тайн: в VI главе предусмотрена ответственность за государственную измену, под которой понимается кроме прочего опубликование или сообщение агенту иностранного государства плана, рисунка, документа, находящегося в тайне в целях охраны государственной безопасности России, кроме того в XXIX главе предусматривалась впервые уголовная ответственность за разглашение тайн. Целая глава была посвящена преступлениям, связанным с разглашением той или иной информации. Важно отметить, что тайной в данном случае понималась не только информация, являющаяся государственной тайной, но также и тайна «другого лица», которая была доверена огласившему, оглашение которой могло повлечь имущественный вред или опозорить лицо, к коему относились такие сведения. Новое Уголовное уложение впервые устанавливало ответственность за разглашение тайны переписки (ст. 542), секрета производства (ст. 543), банковской тайны (ст. 544), коммерческой тайны (ст. 545), налоговой тайны (ст. 546). Таким образом, впервые в уголовном законодатель-

стве России речь шла об ответственности не только за разглашение тайны государства, но и частной тайны, кроме того, достаточно подробно были разграничена ответственность в зависимости от вида разглашаемой тайны.

Кроме того, необходимо особое внимание уделить также XXXVII главе «О преступных деяниях на службе государственной и общественной» Уголовного уложения, в которой была предусмотрена достаточно развернутая система уголовных наказаний за преступления в сфере государственной службы, среди которых было оглашение сведений, которые должны храниться в тайне (правительственные распоряжения, сведения и документы), в том числе телеграмм или почтовых сообщений, а также сведений, касающихся внешней безопасности России. Впервые в Уложении в статье 655 предусматривалась ответственность за разглашения «частной тайны», ставшей известной служащему в силу должностных обязанностей (тайна частной жизни, секрет производства, нотариальная тайна). Кроме того, была введена также ответственность за разглашение такой специфической информации в сфере государственного управления, как информация о способах изготовления государственных кредитных бумаг и их секретных признаках, а также тайны торгов по казенным или общественным подрядам или поставкам, когда торги производятся через запечатанные объявления. То есть можно в этом случае констатировать начало формирования как таковой служебной тайны, которая выделяется из общего массива информациии о государтвенном управлении и перестает быть связанной исключительно с тайной государственной. Стоит особо отметить, что в Уложении 1845 года ответственность за разглашение государственной тайны и другой информации управленческого и военного характера предусматривалась только в разделе, посвященном государственным преступлениям. В разделе «О проступках и преступлениях по службе государственной и общественной» ответственности за разглашение информации, ставшей известной служащему в силу его служебного положения, либо за разглашение иной информации в сфере порядка управления в Уложении 1845 года не предусмотрено. Таким образом, Уложение 1903 года впервые разграничило различные виды информации ограниченного доступа и предоставило защиту не только сведениям в сфере государственной службы, управления и внешней безопасности страны, но и сведениям, составляющим частную тайну как физических, так и юридических лиц.

И все же одной из проблем уголовного законодательства того времени, как отмечают исследователи, являлось «отсутствие подробного «Перечня сведений, составляющих государственную тайну». На основании законодательства можно было лишь выделить отдельные группы сведений, имеющих гриф «долженствующие сохраняться в тайне»:

- планы, чертежи, рисунки или макеты российских укрепрайонов, крепостей и других фортификационных сооружений;
- технические данные о военных кораблях;
- сведения о содержании мобилизационных планов и расположении войск на случай войны [4, стр. 411].

Так, к примеру, «из-за «особенностей» законодательства из 150 установленных правоохранительными органами Варшавского военного округа австрийских и германских шпионов (от мелких контрабандистов до офицеров Штаба военного округа) к уголовной ответственности было привлечено 33 человека [6].

В начале XX века во многом из-за происходящих внешнеполитических и внутриполитических процессов (Русско-японская война, первая революция, Первая мировая война...) охрана секретов в сфере государственного управления и их регулирование сводилась к охране государственной тайны и борьбе со шпионажем. Именно поэтому нормативные акты, издаваемые в то время, были во многом направлены именно на регулирование информации в сфере военной тайны и информации, связанной с дипломатическими отношениями и имеющей отношение к внешней безопасности России.

До начала XX века не существовало единой системы охраны государственных секретов. По словам исследователей, «руководство МИДа не предпринимало почти никаких попыток создать комплексную систему защиты информации. И более того, многие чиновники просто не понимали необходимость соблюдать элементарные правила по обеспечению сохранности сведений, содержащих информацию о планах и особенностях проведения внешнеполитического курса Российской империи».

В качестве примера можно привести отрывок из воспоминаний министра иностранных дел В. Н. Ландздорфа (1900–1906). Всю жизнь он был связан с центральным аппаратом МИДа. <...> Как писал сам Ландздорф в своем «Дневнике», «странным является мое положение в данный момент, мои секретные архивы содержат все тонкости политики последнего царствования. Ни молодой государь (Николай II), ни почтеннейший Шишкин, назначенный временно управляющим Министерством иностранных дел, не имеют не малейшего представления о документах, доверенных в последние годы исключительно и совершенно бесконтрольно мне... Я оказался исключительным обладателем государственных тайн, являющихся основой наших взаимоотношений с другими странами» [11]. Исследователи отмечают, что на законодательном уровне понятие «шпионаж» было достаточно узким. Однако в «Инструкции начальникам контрразведывательных отделений», которая была утверждена 8 июня 1911 г. [15], был приведен расширенный перечень сведений, разглашение которых подпадало под понятие «шпионаж». Сведения относились к военной сфере. Уже в 1912 году появился новый закон, который многие правоведы того времени называли одним из самых прогрессивных в Европе. Закон [9] предусматривал расширение и уточнение понятия «государственная измена», а также вводил новое определение сведений, являющихся государственной тайной в военной сфере: «это сведения или предметы, касающиеся внешней безопасности России или ее вооруженных сил, предназначенных для военной обороны страны».

С началом Первой мировой войны пришлось усилить меры по защите информации, относящейся к военным действиям и военным планам, в том числе путем введения цензуры печати [16], которая подразумевала запрет на публикацию в средствах массовой информации большинства информации, относящейся к развитию событий, техническом и ресурсном оснащении войск на театре военных действий. Кроме того, был также утвержден «Перечень сведений и изображений, касающихся внешней безопасности России и ее военно-морской и сухопутной обороны, оглашение и распространение коих в печати или в речах или докладах, произносимых в публичных собраниях, воспрещается на основании статьи I отдела II закона 5 июля 1912 года, об изменении действующих законов о государственной измене путем шпионства, и статьи II Высочайшего Указа Правительствующему Сенату от 20 июля 1914 года», который включал в себя 25 видов сведений, публикация которых в печати была запрещена. Сведения относились к сведениям в области ведения военных действий, планирования военных операций и состояния дел на театре военных действий (здесь стоит отметить, что в 1917 году в основу Декларации правительства от 2 марта 1917 года лег принцип, который отменял данный Указ. В пункте 2 была провозглашена свобода слова, печати, союзов, собраний и стачек с распространением политических свобод на военнослужащих в пределах, допускаемых военно-техническими условиями. Таким образом, фактически во многом данный Указ играл и политическую роль при смене режима).

В дальнейшем перечень с изменением военно-политической обстановки был изменен в 1915 году. «В 1915 г. были добавлены пункты военно- и социально-экономического характера (союзническое снабжение, заготовки для военной промышленности, перебои в ее работе; вместо беспорядков на занятых войсками территориях – «о всякого рода нарушениях обычного течения жизни» в местностях на положении чрезвычайной охраны и военном), а также добавления делового военного характера, видимо, по опыту применения перечня – о результатах неприятельской бомбардировки и о крушении неприятельских кораблей и др.; Перечень 1916 г. повторял его 30 пунктов без изменений» [1]. В дальнейшем вплоть до 1917 г. Перечни не издавались.

Несмотря на то что стала формироваться система обозначения информации, относящейся к государственной тайне и вводиться определенные меры для ее охраны, нельзя не признать, что в России по-прежнему отсутствовала единая система защиты информации. Кроме того, к государственной тайне в основном относили сведения в сфере военного управления. Как отмечают исследователи, «МИД, Военное ведомство и Департамент полиции самостоятельно прилагали усилия по обеспечению сохранности государственной тайны. При этом Департамент полиции славился своей системой конфиденциального делопроизводства, а МИД и Военное ведомство имели достижения в области криптографии. В то же время предпринимаемые

мероприятия носили хаотичный характер и не могли обеспечить эффективной защиты государственных секретов. Молодой Советской республике пришлось разработать и создать эффективную систему защиты государственной тайны» [12].

В рамках разработки системы защиты государственной тайны было предпринято множество организационных мероприятий, создано, а в дальнейшем реорганизовано множество различных государственных органов. Историю их создания и реорганизации в рамках настоящего исследования мы не будем рассматривать подробно, так как нас интересует по большей части именно правовое регулирование и природа государственных секретов.

Вплоть до 1921 года не предпринималось никаких попыток для упорядочения порядка обработки, хранения документов, содержащих служебную тайну. Отчасти, полагаем, это было связано с политической неопределенностью и становлением правовой системы и всего государства в целом. Вплоть до 1921 года в основном постановления и иные нормативные акты касались введения военной цензуры. При этом стоит отметить, что в дальнейшем вопросы цензуры и охраны информации, составляющей государственную тайну/тайну управления, будут тесно взаимосвязаны.

Только 13 октября 1921 года был издан Декрет СНК «Перечень сведений, составляющих тайну и не подлежащих распространению», который подразделял сведения на военные и экономические. Перечень состоял из трех глав, в первой из которых были сведения военного характера (отдельно для военного и мирного времени), вторая глава содержала сведения экономического характера о денежном обращении и производстве денег, денежной реформе, валютах, ценных бумагах, импортном и экспортном плане, экспортном фонде, продмаршрутах, обеспеченности топливом и подвижным составом отдельных железных дорог, состоянии милиции, преступности и беспорядках, режиме в местах заключения и т. д. Третья глава была посвящена порядку публикации сведений, запрещенных второй главой (с разрешения наркоматов) [1].

Действующая система все же не позволяла должным образом избежать утечек информации, и 30 августа 1922 года Секретариат ЦК РКП(б) принял постановление «О порядке хранения и движения секретных документов», которое и положило начало упорядочению секретного делопроизводства [5].

В дальнейшем развитие регулирования охраняемых сведений в сфере государственного управления, в сфере экономического, политического, общественного и социального развития шло двумя путями:

1) регулирование порядка обращения со сведениями, составляющими государственную тайну, и сведениями, не подлежащими опубликованию, помеченными грифом «не для печати», «сведения, не подлежащие оглашению»;

2) введение цензуры, которая подразумевала ограничение доступа к ряду периодических изданий, произведений науки, литературы, искусства.

В целях контроля за издаваемой и распространяемой литературой в 1922 году было создано Главное управление по делам литературы и издательства (Главлит), на которое возлагались функции контроля за содержание издаваемой литературы, а также контроля за тем, чтобы сведения, относящиеся к государственной тайне, не были распространены в открытой печати.

Следует отметить, что в дальнейшем полномочия Главлита существенно расширялись. [23]. Главлит в дальнейшем не только проверял издания на допустимость их содержания, но и издавал Перечни сведений, запрещенных к опубликованию в открытой печати. Данные Перечни до сих пор отсутствуют в широком доступе: их нет в библиотеках, в интернете и правовых базах.

Вместе с тем вопросам цензуры посвящены многие научные исследования [2].

К печати были запрещены сведения, большинство из которых не относилось к государственной тайне. Так, в одном из перечней 1976 года был предусмотрен запрет опубликовывать сведения о покупательной способности рубля и иностранных валют, сравнении зарплат советских рабочих с зарплатами рабочих за рубежом, данные о размере и распределении зарплат в СССР, сведения о беспорядках и конфликтах в армии на уровне роты и выше, сведения о крупных авариях на производстве и так далее.

В 1981 году вышел Приказ Главархива СССР от 23.04.1981 № 77-ДСП, в котором подробно описывались те категории сведений, публикование которых в открытой печати

было запрещено. Помимо прочих, в п. 1.5 включались несекретные сведения ограниченного распространения, относящиеся к деятельности других министерств (ведомств), публикация которых могла осуществляться только с разрешения этих государственных органов. По своей сути такие сведения являлись не чем иным, как служебной тайной в современном ее понимании.

Стоит отметить, что до сих пор не утратил силу документ, изданный в 1971 году: Перечень сведений органов прокуратуры, не подлежащих опубликованию в открытой печати, передачах по радио и телевидению [25]. Некоторые из указанных сведений составляют профессиональную тайну (тайну следствия, тайну судебного разбирательства), другие же из них являются «внутренней информацией». При этом следует отметить, что указанный перечень содержит также и запрет на распространение статистической информации, что на данном этапе противоречит концепции открытости органов государственной власти и праву на доступ к информации. Вместе с тем в этом документе встречаются упоминания о грифах, использующихся во внутреннем документообороте государственных органов: грифы «секретно», «не подлежит опубликованию», «не для печати». Здесь стоит отметить, что уже само такое упоминание говорит об обособлении от государственной тайны целого пласта управленческой информации, доступ к которой был существенно ограничен и регламентирован лишь ведомственными актами, которые чаще всего не были официально опубликованы.

Если же говорить о правовой регламентации государственной и служебной тайны как таковой, то здесь приходится в основном исходить из положений уголовного кодекса и перечней сведений, являющихся по своему содержанию специально охраняемой государственной тайной [20, 24]. Отдельного нормативного акта, в котором бы содержался перечень информации, относящейся к государственной тайне и порядке ее защиты, не существовало.

Интересно обратить внимание на используемые формулировки при определении государственной тайны и определении мер «социальной защиты» за шпионаж. Так, еще в 1925 году под понятие «шпионаж» подпадало разглашение не только информации, являющейся специально охраняемой законом тайной, но и информации, не подлежащей оглашению по прямому запрещению закона или по распоряжению руководителей ведомств, учреждений и предприятий [18, 19, 21]. В то же время в 1926 году в Постановлении СНК [20] указывалось на то, что к специально охраняемой государственной тайне относятся объявленные секретными или не подлежащими оглашению издания и документы. Таким образом, была заложена уже в 1926 году определенная терминологическая неопределенность, которая позволяла в дальнейшем расширять границы сведений, относимых к государственной тайне.

В 1947 году перечень сведений, относящихся к государственной тайне, стал уже практически открытым. Принятое Постановление [24] в п. 14 предусматривало включение в состав государственных сведений «других сведений, которые будут признаны Советом Министров СССР не подлежащими разглашению». Постепенно повышалось засекречивание управленческой информации в экономической, политической, социальной и военной сферах.

В 1958 году был принят закон «Об уголовной ответственности за воинские преступления», который вводил новый состав преступления: «Разглашение военной тайны или утрата документов, содержащих военную тайну», при этом в военную тайну в этом случае уже входили не только сведения, относящиеся к государственной тайне, но и военные сведения, не подлежащие разглашению.

Только в 1984 году было впервые упомянуто в Уголовном кодексе понятие «Служебная тайна», при этом вводился отдельный состав преступления, предусматривавший ее разглашение иностранной организации (Статья 76.1. Передача иностранным организациям сведений, составляющих служебную тайну). Под служебной тайной понимались экономические, научно-технические или иные сведения, полученные лицом, которому эти сведения были доверены по службе или работе или стали известны иным путем и отнесенные к служебной тайне.

Таким образом, на наш взгляд, ошибочно говорить о том, что во времена Советского Союза служебная тайна стройно вписывалась в систему тайны государственной. Можно сделать вывод из информации, содержащейся в документах, о том, что сама по себе служебная тайна была механизмом обеспечения нужд государственного управления, которая, с одной стороны, позволяла охранять сведе-

ния, распространение которых могло бы повредить системе государственного управления, а с другой стороны, попросту позволяла скрыть огрехи и ошибки политического управления в стране. Кроме того, нанесение различных грифов в министерствах, ведомствах и на предприятиях, таких как «Для служебного пользования», «Не для печати», «Не подлежит опубликованию», давало неограниченные возможности для сокрытия той или иной информации. При этом статус таких документов был определен слабо. А под служебной тайной в 1984 году понимались по большей части сведения, аналогом которых в настоящее время является «секрет производства» и «коммерческая тайна».

После образования Российской Федерации и начала формирования системы законодательства, статус служебной тайны стал еще более размытым и неопределенным. Несмотря на необходимость принятия закона «О служебной тайне», такой закон до сих пор не принят. Как видим, институт служебной тайны и во времена Советского Союза не имел четкой юридической базы и какого-либо глубокого теоретического осмысления. По большому счету, в связи с отсутствием требований открытости власти и права на информацию такое теоретическое осмысление, возможно, было и не нужно, так как институт «служебной тайны» имел по большей части строго прикладной характер и решал практические задачи.

Как отмечал А. А. Фатьянов, служебную информацию составляли те сведения, которые были в так называемой «буферной зоне». В этом случае сведения сами по себе не могли являться государственной тайной, однако при их интеграции становились государственной тайной, либо являлись производными от нее сведениями [10].

Примечания

1. Батулин П. В. Перечни военной цензуры 1912–1923 гг. // Киберленинка. URL:[http://CyberLeninka.ru/article/n/perechni-voennoy-tsenzury-1912-1923-gg.pdf]

2. Горяева, Т. М. История советской политической цензуры, 1917-1991 гг.. Автореф. дис. на соиск. учен. степ. д.ист.н. Спец. 07.00.02 /Горяева Т.М.; [Рос. гос. гуманитар. ун-т]. - М., 2000. - 40 с.

3. Клепиков Н. Н. Политическая цензура на Европейском Севере РСФСР/СССР в 1920–1930-е гг.: автореф. дис. на соиск. учен. степ. к.ист.н. /Клепиков Николай Николаевич; [Помор. гос. ун-т им. М. В. Ломоносова].

4. Колпакиди А. А., Север А. Спецслужбы Российской империи. Уникальная энциклопедия. - М.: Эксмо, 2010. – 781 с.

5. Куренков Г. А. Секретное делопроизводство ЦК (до Великой Отечественной войны) http://www.opentextnn.ru/history/deloproizvodstvo/?id=4897

6. Зданович А. А. Забытое дело подполковника Гримма //Независимое военное обозрение. 1998.– № 6.

7. Стефанович П. С. Понятие верности в отношениях князя и дружины на Руси в XII–XIII вв. // Древняя Русь. Вопросы медиевистики. — 2008.— № 1 (32). — С. 72–82.

8. Стефанович П. С. Дружинный строй в Древней Руси и у древних германцев: существовала ли клятва верности вождю (правителю)? // Древняя Русь. Вопросы медиевистики. — 2008.— № 2 (32). — С. 33—40.

9. Резанов А. С. Закон 5 июля 1912 г. «О государственной измене путем шпионства в мирное время».

10. Фатьянов А. А. Тайна и право (Основные системы ограничений на доступ к информации в российском праве) : Моногр. / А. А. Фатьянов. - М. : Изд-во МИФИ, 1998. – С. 138.

11. Чертопруд С. Организация защиты государственных секретов в МИДе Российской империи в период с 1903 по 1917 год. http://www.agentura.ru/press/cenzura/secret-russia/

12. Чертопруд С. Зарождение и становление системы защиты государственной тайны в Советском Союзе с 1918 по 1930 год. URL: [http://www.agentura.ru/press/cenzura/secret-ussr/]

13. Полное собрание законов Российской империи в 46 томах. Печат. в Типографии 2-го отд. Собственной Его Импера-торского Величества Канцелярии. 1830. Ст. 2791.

14. Реформы Петра I. Сборник документов. Сост. В. И. Лебедев. М., Гос.соц.-эк.изд-во. – 371 с.

15. Инструкция начальникам контрразведывательных отделений от 8 июня 1911 г. URL: [http://www.e-reading.by/chapter.php/1004112/36/Linder_Iosif_-_Specsluzhby_Rossii_za_1000_let.html]

16. Именной высочайший указ 20.7.1914 г. Об утверждении временного Положения о военной цензуре. URL: [http://xn--e1aaejmenocxq.xn--p1ai/content/ustanovlenie-voennoi-cenzury]

17. Постановление СНК СССР от 27_04_1926 «Об утверждении перечня сведений, являющихся по своему содержанию специально охраняемой государственной тайной».

18. Постановление от 14 августа 1925 года «О шпионаже, а равно о собирании и передаче экономических сведений, не подлежащих оглашению» // СПС «КонсультантПлюс».

19. Постановление ВЦИК от 22 ноября 1926 года «О введении в действие уголовного кодекса Р.С.Ф.С.Р.» // СПС «КонсультантПлюс».

20. Постановление СНК СССР от 27.04.1926 «Об утверждении перечня сведений, являющихся по своему содержанию специально охраняемой государственной тайной» // СПС «КонсультантПлюс».

Постановление ЦИК СССР от 25.02.1927 «Положение о преступлениях государственных (контрреволюционных и особо для Союза ССР опасных преступлениях против порядка управления)» // СПС «КонсультантПлюс».

21. Постановление ВЦИК, СНК РСФСР от 06.06.1927 «Об изменении Уголовного Кодекса Р.С.Ф.С.Р. редакции 1926 г.» // СПС «КонсультантПлюс».

22. Постановление СНК РСФСР от 06.06.1931 «Об утверждении Положения о Главном управлении по делам литературы и издательств и его местных органах» // СПС «КонсультантПлюс».

23. Постановление Совмина СССР от 08.06.1947 № 2009 «Об установлении перечня сведений, составляющих государственную тайну, разглашение которых карается по закону» // СПС «КонсультантПлюс».

24. Приказ Генпрокуратуры СССР от 22.11.1971 № 45 «О Перечне сведений органов прокуратуры, не подлежащих опубликованию в открытой печати, передачах по радио и телевидению» // СПС «КонсультантПлюс».

Пономарева Юлия Владимировна, аспирант кафедры конституционного и административного права ЮУрГУ. E-mail: julia.ponomareva17@mail.ru

Ponomareva Julia, postgraduate Department of Constitutional and Administrative Law SUSU. -mail: julia.ponomareva17@mail.ru

УДК 004.056.53 + 005.992.1 : 34.03

Паршин К. А, Басыров Р. Р.

НОРМАТИВНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ РОССИЙСКОЙ ФЕДЕРАЦИИ В ОБЛАСТИ СИСТЕМ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

На сегодняшний день системы электронного документооборота занимают одну из важнейших ролей в делопроизводстве предприятия, позволяя разгрузить бюрократическую машину за счет автоматизации процесса создания, хранения и прохождения всей стадий жизненного цикла документа. Вместе с тем, электронный документооборот порождает новые риски, связанные с конфиденциальностью циркулирующей информации, и пренебрежение защитой обязательно приведет к новым угрозам.

В последние годы спрос на системы электронного документооборота существенно возрос, связано это в первую очередь с законодательством Российской Федерации, регламентирующим переход на системы электронного документооборота для государственных структур, а также положительным опытом их использования в частном коммерческом секторе. Но, внедряя системы электронного документооборота, необходимо уделить существенное внимание безопасности системы. На протяжении многих лет публикуются целые книги о промышленном шпионаже, преступлениях в компьютерной сфере, а наиболее практичные организации уже не один год реализуют написанное на практике.

Ключевые слова: *информация, безопасность, система электронного документооборота, защита информации, данные, информационная система, автоматизированная система, персональные данные, конфиденциальная информация.*

Parshin K. A., Basyrov R. R.

REGULATORY LANDSCAPE RUSSIAN FEDERATION IN ELECTRONIC DOCUMENT MANAGEMENT SYSTEMS

Today, electronic document management system took a major role in proceedings before the enterprise, will relieve the bureaucracy by automating the process of creating, storing and passing all stages of the life cycle of the document. At the same time, electronic documents gives rise to new risks related to the confidentiality of information circulating and neglect of protection will necessarily lead to new threats.

In recent years, demand for electronic document management system has increased significantly, this is due primarily to the Russian Federation laws regulating the transition to electronic document management systems for government agencies, as well as the positive experience of their use in the private commercial sector. But by implementing an electronic document should be given considerable attention to the security of the system. For many years, published a book about the whole industrial espionage, cyber crime, and the most practical organization for more than a year writing implement in practice

Keywords: *information security, electronic document management system, information security, data, information systems, automated system, personal information, confidential information.*

При внедрении и использовании систем электронного документооборота на первое место встаёт задача защиты информации, обрабатываемой и хранящейся в системе. Для её решения используется комплекс организационных и программно-технических мер, регламентированных нормативно-правовой базой.

В западных странах уже давно созданы и действуют стандарты, определяющие требования к СЭД: в США – DoD 5015.2-STD (Design Criteria Standard for Electronic Records Management Software Applications); в Евросоюзе – MoReq (Model requirements for the management of electronic records) [3]. Однако в российском законодательстве отсутствуют единые стандарты, требования к системам электронного документооборота, которыми можно было бы руководствоваться при проектировании и/или выборе системы.

Говоря о защищенном электронном документообороте, зачастую подразумевают защиту информации, содержащейся в электронном документе. В этом случае все сводится к защите информации от утечки, несанкционированных и непреднамеренных воздействий на защищаемую информацию. Комплекс мер по организации защиты информации в электронном документообороте включает в себя: защиту рабочих мест пользователей, защиту сети передачи данных, использование специализированных физических носителей информации и защиту данных на них; а также комплекс организационных мер, определяющих порядок работы с СЭД и циркулирующей в ней информацией ограниченного доступа [4]. На рис. 1 представлены структурные уровни системы электронного документооборота.

К основной базе нормативно-правовых документов, регламентирующих способы и методы защиты информации, можно отнести: Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», данный документ:

1) устанавливает основные термины и определения, используемые в информационных технологиях, а также область их применения;

2) регламентирует отношения, возникающие в сфере информации, информационных технологий и защиты информации;

3) устанавливает правовое регулирование отношений, связанных с использованием информации ограниченного доступа.

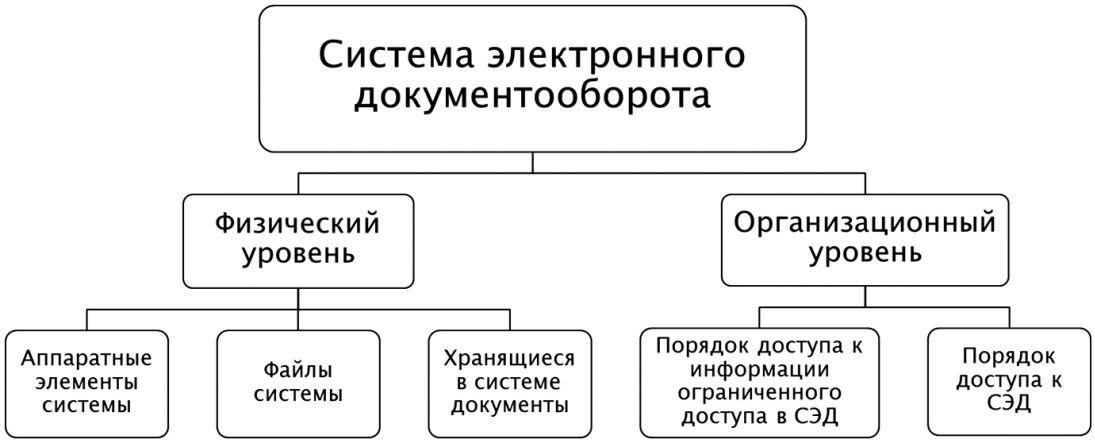

Рис. 1. Структурные уровни системы электронного документооборота

Доктрина информационной безопасности Российской Федерации устанавливает виды угроз безопасности информационных и телекоммуникационных средств и систем. Федеральный закон № 63-ФЗ «Об электронной подписи», регулирующий отношения в области использования электронных подписей:

1) определяет понятие ЭП, сертификат ключа проверки электронной подписи, ключ электронной подписи и др.;

2) определяет право использования ЭП и принципы её использования;

3) определяет виды ЭП и области их применения.

Так как в системе электронного документооборота может обрабатываться информация, содержащая персональные данные, следует также отметить Федеральный закон № 152-ФЗ «О персональных данных», регулирующий отношения, связанные:

1) с обработкой персональных данных в системах электронного документооборота;

2) организацией хранения, комплектования, учета и использования содержащих персональные данные документов;

3) предоставлением доступа к сведениям, содержащим персональные данные.

Также необходимо отметить Приказ ФСТЭК России № 21 от 18 февраля 2013 г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», определяющий состав мер по обеспечению безопасности персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

Помимо информации ограниченного доступа, содержащей персональные данные, с СЭД может обрабатываться информация, отнесённая к сведениям, содержащим служебную тайну, в этом случае стоит отметить разработанный проект федерального закона «О служебной тайне», в котором определяются:

1) принцип отнесения сведений к служебной тайне;

2) порядок отнесения сведений к служебной тайне применительно к системам электронного документооборота;

3) порядок снятия ограничений на распространение сведений, составляющих служебную тайну, применительно к системам электронного документооборота.

Помимо законодательных, существует ряд руководящих документов и ГОСТов, определяющих состав и содержание методик, технических средств и методов реализации защиты информации в СЭД:

• ГОСТ Р 53898-2013 «Системы электронного документооборота. Взаимодействие систем электронного документооборота. Технические требования к электронному сообщению» устанавливает формат, состав и содержание электронного сообщения, обеспечивающего информационное взаимодействие систем управления документами;

• ГОСТ 6.10.4-84 «Унифицированные системы документации. Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники» устанавливает требования к составу и содержанию реквизитов, придающих юридическую силу документам, создаваемым средствами вычислительной техники, а также порядок внесения изменений в эти документы;

• РД «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации», описывающий основные принципы защиты информации от несанкционированного доступа;

• РД «Защита от несанкционированного доступа к информации. Термины и определения» устанавливает термины и определения в области защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации;

• РД «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» устанавливает классификацию средств вычислительной техники по уровню защищенности от несанкционированного доступа к информации;

• РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» устанавливает классификацию автоматизированных систем, подлежащих защите от несанкционированного доступа к информации, и требования по защите информации в АС различных классов;

• РД «Средства вычислительной техники. Межсетевые экраны. Защита от несанкциони-

рованного доступа. Показатели защищенности от несанкционированного доступа к информации» устанавливает классификацию межсетевых экранов по уровню защищенности от несанкционированного доступа к информации;

• РД «Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности» определяет порядок разработки, оценки, регистрации и публикации профилей защиты и заданий по безопасности информационных систем, предназначенных для обработки информации ограниченного доступа.

Также нужно отметить утверждённую Заместителем директора ФСТЭК России 14 февраля 2008 г. «Методику определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», предназначенную для использования при проведении работ по обеспечению безопасности персональных данных при их обработке в автоматизированных информационных системах персональных данных.

Делая выводы, можно говорить о том, что нормативная правовая база Российской Федерации в области информационных систем постоянно дополняется и редактируется в соответствии с требованиями информационной безопасности: конкретизируются требования, предъявляемые к ИС в её технической и организационной части, устанавливается порядок лицензирования и сертификации систем, пополняется классификация возможных угроз и методов их предотвращения. Однако данные нормативно-правовые акты предъявляют требования к информационным системам в целом, и лишь малая их часть относится непосредственно к электронному документообороту, таким образом, в развивающемся информационном обществе встаёт актуальным вопрос создания нормативного акта, регулирующего отношения в области проектирования, разработки и внедрения информационных систем электронного документооборота, учитывающих всю специфику данных систем: хранение и обработка информации ограниченного доступа в совокупности с общедоступной информацией, придание электронным документам юридической силы, условия хранения электронных документов и содержащейся в них информации, взаимодействие разнородных систем при электронном документообмене.

Примечания

1. Стратегия развития информационного общества в Российской Федерации от 7 февраля 2008 г. № Пр-212.

2. Постановление Правительства Российской Федерации от 6 сентября 2012 г. № 890, г. Москва «О мерах по совершенствованию электронного документооборота в органах государственной власти».

3. Жвакина Е. Текущее законодательство в сфере электронного документооборота и СЭД/ECM // ECM-Journal.ru – http://ecm-journal.ru/docs/Chast-2-Tekushhee-zakonodatelstvo-v-sfere-ehlektronnogo-dokumentooborota-i-SEhDECM.aspx

4. Электронный документ и документооборот: правовые аспекты. М.: ИНИОН РАН, 2003.

5. Самодуров А. Особенности защиты электронного документооборота // CNews.ru – http://www.cnews.ru/reviews/free/security2006/articles/e-docs/

Паршин Константин Анатольевич, к. т. н, доцент кафедры «Информационные технологии и защита информации», «Уральский государственный университет путей сообщения», Екатеринбург. E-mail: KParshin@usurt.ru

Басыров Руслан Равильевич, Программист 2 категории Управления информатизации, отдел АСУФР, «Уральский государственный университет путей сообщения», 620034, Свердловская обл, Екатеринбург г. Колмогорова ул. 66.

Konstantin Parshin, associate professor of "Information technologies and protection of information" Ural State University of Railway Transport , Ekaterinburg. E-mail: KParshin@usurt.ru

Ruslan Basyrov, Programmer 2 categories of Informatization, Department ASUFR, «Ural State University of Railway Transport», 620034, Sverdlovsk region, Ekaterinburg g, Kolmogorov street, 66. E-mail: rrbasyirov@usurt.ru

УДК 004.056.53 + 347.731

Вожакин Т. А.

ОПЫТ ПРАВОВОГО РЕГУЛИРОВАНИЯ ИНСАЙДЕРСКОЙ ИНФОРМАЦИИ

В статье анализируется опыт правового регулирования инсайдерской информации за рубежом. Дается сравнение регулирования отдельных положений института инсайдерской информации в России и за рубежом. Делается вывод, что широко представленный в зарубежном законодательстве дифференцированный подход к ответственности за инсайд, учитывающий особенности субъекта правонарушения, является более предпочтительным. На лиц, не относящихся к инсайдерам, не должна распространяться ответственность за передачу полученной ими инсайдерской информации другим субъектам, а также за дачу рекомендаций третьим лицам по совершению операций на организованных рынках, если в основе этих рекомендаций лежит инсайдерская информация.

Ключевые слова: *инсайдерская информация, правовой режим, зарубежный опыт, конфиденциальность.*

Vozhakin T. A.

EXPERIENCE OF LEGAL REGULATION INSIDER INFORMATION

The article analyzes the experience of legal regulation of insider information abroad. Compares the regulation of certain provisions of the Institute of insider information in Russia and abroad. It is concluded that the widely represented in foreign legislation differentiated approach to liability for insider taking into account the peculiarities of the subject of the offense, it is more preferable. Persons who do not belong to insiders should not apply for the transfer of responsibility they receive insider information to other entities, as well as for giving recommendations to third parties to perform operations on organized markets, if the basis of these recommendations is insider information.

Keywords: *insider information, the legal regime, foreign experience, privacy.*

Инсайдерское законодательство передовых стран имеет продолжительную историю и во многом по этой причине, характеризуется высокой степенью развитости и проработанности. В силу этого зарубежный опыт представляет значительный интерес для оценки отечественных законодательных конструкций в области запрета инсайдерской торговли.

США. Понятие инсайдера в американском законодательстве строго не определено, решающее значение имеют судебные прецеденты [3, с. 72]. Фактически инсайдером может признано любое лицо, имеющее доступ к внутренней информации [6, с. 38]. Для американского антиинсайдерского законодательства характерно разделение на инсайдеров и квазиинсайдеров [6, с. 41].

Великобритания. Инсайдерами признаются любые лица, владеющие инсайдерской информацией и обладающие правом доступа

к этой информации. К таковым относятся директора, иные должностные лица или сотрудники компании-эмитента, а также иные лица, имеющие доступ к инсайдерской информации в силу служебных или профессиональных обязанностей. Все перечисленные выше лица – первичные инсайдеры. Ко вторичным инсайдерам законодатель относит лиц, получивших внутреннюю информацию от первичных инсайдеров. Так, водитель такси или бармен, подслушавшие беседу инсайдеров первого уровня, являются инсайдерами второй категории. В законе не дано четкого определения инсайдеров второй категории [6, с. 73–74].

Франция. Денежным и финансовым кодексом предусмотрены три категории инсайдеров: 1) прямые инсайдеры – это «руководители» общества-эмитента (к их числу закон относит президента общества-эмитента, генеральных директоров, членов совета директоров, физических или юридических лиц, осуществляющих в этом обществе функции управляющего или члена наблюдательного совета, постоянных представителей юридических лиц, а также супругов указанных лиц (за исключением раздельно проживающих на основании судебного решения)); 2) косвенные инсайдеры – это лица, располагающие служебной информацией в связи с их профессиональной деятельностью или выполнением ими иных функций (чиновники, ликвидаторы, работники бирж и банков, контрагенты по договорам, адвокаты, консультанты, архитекторы, журналисты, работники организаций страхования и т. п., вплоть до водителя такси и парикмахера, которым служебная информация стала известна в связи с осуществлением ими профессиональных функций); 3) иные лица, располагающие привилегированной информацией «со знанием дела», к числу которых можно отнести любое получившее доступ к такой информации лицо, в том числе в результате ее противоправного или случайного разглашения [3, с. 73].

Германия. Действующий закон не определяет понятие инсайдера, предусматривая ответственность за совершение сделок с использованием инсайдерской информации любыми лицами, этой информацией располагающими [6, с. 76–77]. В немецком законодательстве также присутствует разделение на так называемых «первичных» и «вторичных» инсайдеров. Закон не дает четкого определения того, кто относится к «вторичным» инсайдерам, а лишь признает сделку противоправной, если в ее основе лежит использование инсайдерской информации и лицо знает, что информация, которую он использовал, инсайдерская [4, с. 292–293].

Австралия. Законодательство Австралии признает инсайдером любое лицо независимо от того, является ли оно сотрудником компании, акции которой торгуются на бирже, или имеет иной характер отношений с компанией [5]. Важным является то, что лицо владеет информацией и осознает, что информация содержит нераскрытые сведения о ценных бумагах, которые могут оказать существенное влияние на их рыночную цену [6, с. 53].

Япония. Запрет на инсайдерскую деятельность распространяется на инсайдеров и квазиинсайдеров. Инсайдерами признаются акционеры, владеющие более 10% акций компании, а также директора и сотрудники компании, квазиинсайдерами – государственные чиновники, а также все те, кто имеет официальные отношения с компанией, в частности юристы, служащие банков, консультанты, переводчики, журналисты. Вторичные инсайдеры (квазиинсайдеры) также могут быть привлечены к ответственности, если они осведомлены о том, что источник информации – инсайдер [6, с. 52].

Таким образом, для зарубежного законодательства в целом характерно неопределенное понимание инсайдера как любого лица, располагающего инсайдерской информацией; при этом инсайдеров делят на первичных (лиц, имеющих доступ к инсайдерской информации в силу служебных или профессиональных обязанностей) и вторичных (или квазиинсайдеров). В России реализован несколько иной подход: в отечественном законодательстве однозначно определена категория «инсайдер» (как некий исчерпывающий перечень субъектов, имеющих на легальной основе доступ к инсайдерской информации), но к административной ответственности могут быть привлечены не только инсайдеры, но и любые лица, в силу тех или иных причин располагающие инсайдерской информацией. Для российского законодательства нехарактерно разделение инсайдеров на первичных и вторичных (закон просто выделяет инсайдеров из всего круга лиц, обладающих инсайдерской информацией). Следовательно, можно говорить о разграничении субъектов административного правонарушения, предусмотренного статьей 15.21

КоАП РФ, на инсайдеров и прочих лиц, владеющих инсайдерской информацией.

Подобные расхождения между российским законодательством и законодательством ряда зарубежных государств являются весьма допустимыми, а позиция отечественного законодателя представляется вполне оправданной. Сама же необходимость выделения группы инсайдеров в России связана с возложением на этот круг субъектов ряда специфических обязанностей (по распространению и передаче инсайдерской информации, по ведению и передаче списка инсайдеров и прочее).

В связи с этим непонятны опасения С. Гришаева, что указанный в статье 4 Федерального закона «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком» перечень инсайдеров не распространяется на тех, кому инсайдерская информация может быть передана лицами, имеющими к ней непосредственный доступ (например, родственники инсайдеров) [2, с. 9]. Да, родственники инсайдеров не являются инсайдерами, но это вовсе не означает, что если эти субъекты неправомерно используют переданную им инсайдерскую информацию, они останутся безнаказанными. Их привлекут к административной ответственности не как инсайдеров, а как лиц, располагавших инсайдерской информацией и неправомерным образом использовавших ее (что не повлияет ни на квалификацию, ни на размер назначенного наказания).

В п. 1 ст. 6 ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком» пояснено, что понимается под неправомерным использованием инсайдерской информации – использование инсайдерской информации:

1) для осуществления операций с финансовыми инструментами, иностранной валютой и (или) товарами, которых касается инсайдерская информация, за свой счет или за счет третьего лица, за исключением совершения операций в рамках исполнения обязательства по покупке или продаже финансовых инструментов, иностранной валюты и (или) товаров, срок исполнения которого наступил, если такое обязательство возникло в результате операции, совершенной до того, как лицу стала известна инсайдерская информация;

2) путем передачи ее другому лицу, за исключением случаев передачи этой информации лицу, включенному в список инсайдеров, в связи с исполнением обязанностей, установленных федеральными законами, либо в связи с исполнением трудовых обязанностей или исполнением договора;

3) путем дачи рекомендаций третьим лицам, обязывания или побуждения их иным образом к приобретению или продаже финансовых инструментов, иностранной валюты и (или) товаров.

В п. 3 ст. 6 ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком» сделано уточнение, что к нарушению запрета на передачу инсайдерской информации другому лицу не относится передача инсайдерской информации для ее опубликования редакции средства массовой информации, ее главному редактору, журналисту и иному ее работнику, а также ее опубликование в средстве массовой информации. При этом передача такой информации для ее опубликования или ее опубликование не освобождают от ответственности за незаконное получение, использование, разглашение сведений, составляющих государственную, налоговую, коммерческую, служебную, банковскую тайну, тайну связи (в части информации о почтовых переводах денежных средств) и иную охраняемую законом тайну, и от соблюдения обязанности по раскрытию или предоставлению инсайдерской информации.

Таким образом, по российскому законодательству к неправомерному использованию инсайдерской информации относится 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.

Для полноты характеристики обратимся к зарубежному опыту в правовом установлении запрещенных форм инсайдерской торговли. Это позволит определить особенности отечественного подхода к решению проблемы неправомерного использования инсайдерской информации и выявить его возможные недостатки.

Европейский союз. Применительно к инсайдерской информации установлены следующие запреты: 1) лица, располагающие инсайдерской информацией, не вправе использовать ее для покупки или продажи финансовых инструментов; 2) лица, располагающие инсайдерской информацией, не вправе: а) передавать ее третьим лицам, за исключением случаев, когда такая передача является частью обычного процесса исполнения должностных обязанностей; б) давать третьим лицам основанные на инсайдерской информации рекомендации о покупке или продаже финансовых инструментов; 3) лица, являющиеся профессиональными участниками рынка ценных бумаг, не вправе выполнять поручения своих клиентов, если имеется обоснованное подозрение, что подобные поручения базируются на инсайдерской информации [1]. При этом запрет на совершение сделок с использованием инсайдерской информации распространяется как на инсайдеров, так и на вторичных инсайдеров (любое лицо, получившее информацию от инсайдера, автоматически принимает на себя обязательство инсайдера не совершать сделки) [6, с. 67]. Ответственность же за передачу инсайдерской информации третьим лицам предусмотрена только для инсайдеров [6, с. 67].

Великобритания. Ограничения на использование инсайдерской информации: лицо, располагающее внутренней информацией о ценных бумагах, не вправе совершать от себя лично или через третьих лиц операции с инсайдерскими ценными бумагами, давать рекомендации третьим лицам при совершении операций с бумагами, даже если отсутствует личный интерес и третье лицо не осознает, что в основе содействия лежит инсайдерская информация; инсайдеры и лица, располагающие инсайдерской информацией, не вправе передавать иным лицам или делать доступной для третьих лиц инсайдерскую информацию или основанные на ней сведения, за исключением случаев, когда этого потребуют служебные обязанности [6, с. 73–74]. Таким образом, по британскому праву за неправомерную передачу инсайдерской информации третьим лицам юридической ответственности подлежат не только инсайдеры, но и все лица, располагающие инсайдерской информацией.

Франция. Запрещенное законом деяние – это осуществление инсайдером лично или через подставных лиц операций с ценными бумагами и финансовыми инструментами либо попущение совершать такие операции (например, в результате разглашения служебной информации), если это деяние совершено до ознакомления публики со служебной информацией. В случае попущения совершению операции третьими лицами необходимо осознание того факта, что разглашенная служебная информация будет использована третьими лицами при совершении сделок на рынке ценных бумаг. При этом «осознание» понимается широко, не требуется знания ни о личности третьих лиц, ни о деталях операций [3, с. 73]. При осуществлении операций с ценными бумагами и финансовыми инструментами не требуется, чтобы лицо, осознанно использующее конфиденциальную информацию, заранее имело намерение получить прибыль, либо получило ее в действительности. Ответственность наступает даже в том случае, если виновный вообще не имел намерения спекулировать или получить прибыль от совершенной операции [6, с. 74–75].

Германия. Ответственность предусмотрена за: 1) покупку или продажу ценных бумаг с использованием инсайдерской информации; 2) сообщение об этой информации либо открытие к ней доступа; 3) рекомендации совершить сделку с ценными бумагами или склонение к этому любым иным способом [3]. В то же время законодатель не запрещает вторичному инсайдеру передавать информацию третьим лицам (запрещено лишь использовать инсайдерскую информацию при совершении сделок) [3, с. 292–293].

Австралия. Инсайдеру запрещено осуществлять какие-либо сделки с ценными бумагами, если он знает или должен знать, что данная информация публично недоступна заинтересованным инвесторам и может оказать существенное влияние на рыночную цену этих акций [6, с. 52–53]. За передачу инсайдерской информации любому третьему лицу инсайдер может быть привлечен к ответственности, если при этом он знал или должен был знать, что то лицо с большой вероятностью будет совершать сделки с акциями [6, с. 68].

Япония. Ответственность за передачу инсайдерской информации третьим лицам предусмотрена только для инсайдеров [6, с. 68]. Вторичные инсайдеры могут быть привлечены к ответственности за использование инсайдерской информации при осуществлении операций с ценными бумагами, если они

осведомлены о том, что источник информации – инсайдер [6, с. 52].

В США в отличие от всех рассмотренных выше стран юридическая ответственность за неправомерную передачу информации третьим лицам предусмотрена для инсайдеров и квазиинсайдеров только в том случае, если эта передача информации носила возмездный характер (то есть осуществлялась за вознаграждение; при этом вид вознаграждения не имеет значения). Ответственность же лица, воспользовавшегося полученной информацией, зависит от того, знало ли оно, что источник информации поступил противоправно, передавая внутреннюю информацию компании [6, с. 41].

Очевидно сходство положений отечественного законодательства с законодательством ряда иностранных государств по вопросу определения категории «неправомерное использование инсайдерской информации». В пункте 1 статьи 6 Федерального закона «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком» отражены все три способа неправомерного использования инсайдерской информации, которые запрещены законодательствами государств с развитым финансовыми рынками. Однако есть и определенные расхождения.

В ряде зарубежных правопорядков юридическая ответственность за незаконное использование инсайдерской информации устанавливается не только для инсайдеров, но и для вторичных инсайдеров (или квазиинсайдеров, то есть лиц, располагающих инсайдерской информацией). При этом в законах этих стран делается разграничение относительно способов осуществления неправомерного использования инсайдерской информации в зависимости от субъекта правонарушения. Как правило, вторичные инсайдеры (квазиинсайдеры) не подлежат ответственности за передачу инсайдерской информации или за дачу рекомендаций третьим лицам; для них установлен запрет лишь на использование инсайдерской информации при совершении операций с финансовыми инструментами. Для российского законодательства подобное разделение нехарактерно: запрет на неправомерное использование инсайдерской информации (независимо от способа его совершения) является универсальным и распространяется абсолютно на всех лиц, располагающих инсайдерской информацией (безотносительно к тому, является ли это лицо инсайдером или нет). Единственное, в пункте 2 статьи 7 Федерального закона «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком» сделано уточнение, что использование инсайдерской информации считается неправомерным, а лицо, ее использовавшее, подлежит юридической ответственности только в том случае, если это лицо осознавало, что информация является инсайдерской.

Полагаем, широко представленный в зарубежном законодательстве дифференцированный подход к ответственности за инсайд, учитывающий особенности субъекта правонарушения, является более предпочтительным. На лиц, не относящихся к инсайдерам, не должна распространяться ответственность за передачу полученной ими инсайдерской информации другим субъектам, а также за дачу рекомендаций третьим лицам по совершению операций на организованных рынках, если в основе этих рекомендаций лежит инсайдерская информация. Связано это с тем, что у не являющего инсайдером субъекта ввиду отсутствия у него должностных, трудовых, договорных отношений (то есть каких-либо правовых связей) с организацией никаких юридических обязательств перед этой компанией относительно использования ее внутренних сведений (инсайдерской информации) нет и не может быть. Негативные юридические последствия за нарушение режима конфиденциальности инсайдерской информации должны наступать лишь для тех, кто этот режим обязан был соблюдать, то есть для тех, кому эта информация была на легальных основаниях вверена – для инсайдеров. Для всех же прочих правовой запрет на инсайдерскую торговлю может распространяться лишь на случаи непосредственного использования полученной инсайдерской информации в целях совершения операций на организованных рынках.

Примечания

1. Гетьман-Павлова, И. В. Регулирование инсайдерской торговли на мировых рынках ценных бумаг / И. В. Гетьман-Павлова // Банковское право. – 2007. – № 1.

2. Гришаев, С. Инсайдерская информация и манипулирование рынком: новое в законодательстве / С. Гришаев // Хозяйство и право. – 2010. – № 11.

3. Клепицкий, И. А. Инсайдерская информация и уголовный закон / И. А. Клепицкий // Закон. – № 9.

4. Костерина, О. Е. Анализ законодательства России и Германии об использовании служебной (инсайдерской) информации на рынке ценных бумаг / О. Е. Костерина // Вестник Костромского государственного университета им. Н. А. Некрасова. – 2007; Погосова, А. С. Особенности правового режима инсайдерской информации на рынке ценных бумаг / А. С. Погосова // Современное право – 2011. – № 1.

5. Ширинян, И. Мировой опыт использования инсайдерской информации на рынке ценных бумаг / И. Ширинян // Рынок ценных бумаг. – 2004. – № 13.

Вожакин Тимофей Александрович, аспирант кафедры конституционного и административного права Южно-Уральского государственного университета. E-mail: fricasoid@mail.ru.

Vozhakin Timothy, graduate student of Constitutional and Administrative Law of the South Ural State University. E-mail: fricasoid@mail.ru.

УДК 004.056.53 + 347.775.03 + 658.5 : 347.775.03

Минбалеев А. В.

ПРАВОВАЯ ОХРАНА КОММЕРЧЕСКОЙ ТАЙНЫ: ОЧЕРЕДНАЯ РЕФОРМА ЗАКОНОДАТЕЛЬСТВА[1]

В статье рассматривается актуальная сегодня проблема защиты коммерческой тайны. В России на протяжении пятнадцати лет произошло несколько изменений режима коммерческой тайны. Автор анализирует современный режим коммерческой тайны, дает рекомендации по ее защите на основе новых норм. В статье разграничиваются секреты производства и информация, составляющая коммерческую тайну. Автор анализирует изменения гражданского и информационного законодательства и делает вывод, что сегодня секреты производства могут охраняться как в режиме коммерческой тайны, так и в режиме профессиональной тайны, служебной тайны и других режимов и конфиденциальности. Исследуются актуальные проблемы применения режима коммерческой тайны к секретам производства.

Ключевые слова: *секреты производства, информационная безопасность, коммерческая тайна, конфиденциальность, защита коммерческой информации.*

Minbaleev A. V.

LEGAL PROTECTION OF COMMERCIAL SECRETS: THE NEXT REFORM LEGISLATION

The today issue of the day of defence of commercial secret is examined in the article. In Russia a few changes of the mode of commercial secret happened during fifteen years. An author analyses the modern mode of commercial secret, gives to recommendation on her defence on the basis of new norms. The secrets of production and information making a commercial secret are differentiated in the article. An author analyses the changes of civil and informative legislation and draws conclusion, that today the secrets of production can be guarded both in the mode of commercial secret and in the mode of professional secret, official secret and other modes and confidentiality. The issues of the day of application of the mode of commercial secret are investigated to the secrets of production.

Keywords: *secrets of production, informative safety, commercial secret, confidentiality, defence of commercial information.*

[1] Статья написана в рамках выполнения НИР по теме: «Разработка научно-методического обеспечения правовой поддержки хозяйствующих субъектов, ориентированная на минимизацию предпринимательского риска» в рамках реализации программы развития Южно-Уральского государственного университета на 2010–2019 гг. по приоритетному направлению развития «Энергосбережение в социальной сфере».

Специалисты в области защиты информации сегодня практически не удивляются, если им говоришь, что режим коммерческой тайны претерпел очередные изменения и появились новые требования. На протяжени последних 15 лет прошло как минимум пять подобных изменений. Поиски законодателем оптимального пути регулирования информации, составляющей комерческую тайну, строятся часто на принципе «практика рассудит». Однако последние изменения законодательства еще даже не успели за попыткой сказать правоприменительной практике своего слова в необходимости тех или иных изменений.

Согласно изменениям, внесенным Федеральным законом от 12 марта 2014 г. № 35-ФЗ «О внесении изменений в части первую, вторую и четвертую Гражданского кодекса Российской Федерации и отдельные законодательные акты Российской Федерации», законодателем сделана попытка развести секреты производства (ноу-хау) и информацию, составляющую коммерческую тайну.

Согласно ФЗ «О коммерческой тайне», информация, составляющая коммерческую тайну, – это «сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны». Соответственно коммерческая тайна – это режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Режим коммерческой тайны в целом не изменяется и так же, как и ранее, связан с рядом обязательных и рекомендуемых мер, которые должен осуществлять обладатель сведений, в отношении которых производится засекречивание. Согласно Федеральному закону «О коммерческой тайне» к числу обязательных мер (количественный показатель защиты конфиденциальности информации в режиме коммерческой тайны), которые должен применять обладатель информации, желающий установить в отношении нее режим коммерческой тайны, относятся:

1) определение перечня информации, составляющей коммерческую тайну;

2) ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

3) учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;

4) регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

5) нанесение на материальные носители, содержащие информацию, составляющую коммерческую тайну, или включение в состав реквизитов документов, содержащих такую информацию, грифа «Коммерческая тайна» с указанием обладателя такой информации (для юридических лиц – полное наименование и место нахождения, для индивидуальных предпринимателей – фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства). Наряду с указанными мерами обладатель информации, составляющей коммерческую тайну, вправе применять при необходимости средства и методы технической защиты конфиденциальности этой информации, другие не противоречащие законодательству Российской Федерации меры.

Меры по охране конфиденциальности информации признаются разумно достаточными (качественный показатель защиты конфиденциальности информации в режиме коммерческой тайны), если:

1) исключается доступ к информации, составляющей коммерческую тайну, любых лиц без согласия ее обладателя;

2) обеспечивается возможность использования информации, составляющей коммерческую тайну, работниками и передачи ее контрагентам без нарушения режима коммерческой тайны.

В новой редакции ФЗ «О коммерческой тайне» законодатель устанавливает ряд положений, касающихся права обладания информацией, составляющей коммерческую тайну.

Таким образом, законодатель подчеркивает, что в отношении информации, составляющей коммерческую тайну, применяется именно право обладания, а в отношении секретов производства (ноу-хау), охраняемых в режиме коммерческой тайны, применяется режим интеллектуальных прав как на объект интеллектуальной собственности. Права обладателя информации, составляющей коммерческую тайну, возникают с момента установления им в отношении этой информации режима коммерческой тайны в соответствии с вышеуказанными обязательными количественными и качественными мерами. Обладатель информации, составляющей коммерческую тайну, имеет право:

1) устанавливать, изменять, отменять в письменной форме режим коммерческой тайны в соответствии с настоящим Федеральным законом и гражданско-правовым договором;

2) использовать информацию, составляющую коммерческую тайну, для собственных нужд в порядке, не противоречащем законодательству Российской Федерации;

3) разрешать или запрещать доступ к информации, составляющей коммерческую тайну, определять порядок и условия доступа к этой информации;

4) требовать от юридических лиц, физических лиц, получивших доступ к информации, составляющей коммерческую тайну, органов государственной власти, иных государственных органов, органов местного самоуправления, которым предоставлена информация, составляющая коммерческую тайну, соблюдения обязанностей по охране ее конфиденциальности;

5) требовать от лиц, получивших доступ к информации, составляющей коммерческую тайну, в результате действий, совершенных случайно или по ошибке, охраны конфиденциальности этой информации;

6) защищать в установленном законом порядке свои права в случае разглашения, незаконного получения или незаконного использования третьими лицами информации, составляющей коммерческую тайну, в том числе требовать возмещения убытков, причиненных в связи с нарушением его прав.

Ряд положений в обновленном законодательстве связан с восстановлением в законодательстве и появлением новых требований по обеспечению режима коммерческой тайны в трудовых отношениях. Так, в целях охраны конфиденциальности информации, составляющей коммерческую тайну, работодатель обязан:

1) ознакомить под расписку работника, доступ которого к этой информации, обладателями которой являются работодатель и его контрагенты, необходим для исполнения данным работником своих трудовых обязанностей, с перечнем информации, составляющей коммерческую тайну;

2) ознакомить под расписку работника с установленным работодателем режимом коммерческой тайны и с мерами ответственности за его нарушение;

3) создать работнику необходимые условия для соблюдения им установленного работодателем режима коммерческой тайны.

Доступ работника к информации, составляющей коммерческую тайну, осуществляется с его согласия, если это не предусмотрено его трудовыми обязанностями. В целях охраны конфиденциальности информации, составляющей коммерческую тайну, работник обязан:

1) выполнять установленный работодателем режим коммерческой тайны;

2) не разглашать эту информацию, обладателями которой являются работодатель и его контрагенты, и без их согласия не использовать эту информацию в личных целях в течение всего срока действия режима коммерческой тайны, в том числе после прекращения действия трудового договора;

3) возместить причиненные работодателю убытки, если работник виновен в разглашении информации, составляющей коммерческую тайну и ставшей ему известной в связи с исполнением им трудовых обязанностей;

4) передать работодателю при прекращении или расторжении трудового договора материальные носители информации, имеющиеся в пользовании работника и содержащие информацию, составляющую коммерческую тайну.

Работодатель вправе потребовать возмещения убытков, причиненных ему разглашением информации, составляющей коммерческую тайну, от лица, получившего доступ к этой информации в связи с исполнением трудовых обязанностей, но прекратившего трудовые отношения с работодателем, если эта информация разглашена в течение срока действия режима коммерческой тайны. Причиненные работником или прекратившим трудовые отношения с работодателем лицом

убытки не возмещаются, если разглашение информации, составляющей коммерческую тайну, произошло вследствие несоблюдения работодателем мер по обеспечению режима коммерческой тайны, действий третьих лиц или непреодолимой силы.

Трудовым договором с руководителем организации должны предусматриваться его обязанности по обеспечению охраны конфиденциальности составляющей коммерческую тайну информации, обладателем которой являются организация и ее контрагенты, и ответственность за обеспечение охраны конфиденциальности этой информации. Руководитель организации возмещает организации убытки, причиненные его виновными действиями в связи с нарушением законодательства Российской Федерации о коммерческой тайне. При этом убытки определяются в соответствии с гражданским законодательством. Работник имеет право обжаловать в судебном порядке незаконное установление режима коммерческой тайны в отношении информации, к которой он получил доступ в связи с исполнением трудовых обязанностей.

Теперь обратимся к положениям о секретах производства (ноу-хау) и соответствующим нормам гражданского законодательства.

Согласно ст. 1465 ГК РФ в новой редакции от 12 марта 2014 г., под секретом производства (ноу-хау) признаются «сведения любого характера (производственные, технические, экономические, организационные и другие) о результатах интеллектуальной деятельности в научно-технической сфере и о способах осуществления профессиональной деятельности, имеющие действительную или потенциальную коммерческую ценность вследствие неизвестности их третьим лицам, если к таким сведениям у третьих лиц нет свободного доступа на законном основании и обладатель таких сведений принимает разумные меры для соблюдения их конфиденциальности, в том числе путем введения режима коммерческой тайны». При этом законодатель указывает, что секретом производства не могут быть признаны сведения, обязательность раскрытия которых либо недопустимость ограничения доступа к которым установлена законом или иным правовым актом. Полагаем, что последнее положение о возможности ограничения доступа к информации ограниченного доступа иным правовым актом является вряд ли допустимым, поскольку противоречит положениям Конституции Российской Федерации. Любой режим конфиденциальности является ограничением конституционного права на информацию, а значит, должен устанавливаться только на уровне федерального закона.

Секреты производства (ноу-хау) по обновленным требованиям ГК РФ могут быть защищены не только в режиме коммерческой тайны, если они являются фактически информацией, составляющей коммерческую тайну, но и в ином режиме информации ограниченного доступа. Например, это может быть режим профессиональной тайны (банковская тайна, аудиторская тайна и др.), служебной тайны (если информация непосредственно связана со служебной деятельностью в государственных предприятиях и учреждениях), за исключением налоговой и военной тайны. Полагаем, что секреты производства однозначно не могут охраняться в режиме государственной тайны.

В качестве секретов производства (ноу-хау), соответственно, может охраняться в режиме коммерческой тайны достаточно большой перечень информации, который формируется исходя из интересов хозяйствующего субъекта. Данный интерес обусловливается рядом факторов: возможность применения хозяйствующим субъектом мер по обеспечению конфиденциальности в режиме коммерческой тайны; эффективность режима коммерческой тайны для данного вида информации; необходимость обеспечения не только режима обладания информацией, но и режима исключительного права на секрет производства как объект интеллектуальной собственности (например, в случаях, когда субъект собирается внести в состав нематериальных активов исключительные права на секреты производства) и др.

В случаях же необходимости или большей эффективности применения иных разумных мер для соблюдения их конфиденциальности секреты производства могут быть защищены в другом режиме.

Обладателю секрета производства принадлежит исключительное право его использования любым не противоречащим закону способом (исключительное право на секрет производства), в том числе при изготовлении изделий и реализации экономических и организационных решений. Таким образом, как и до введения изменений в 2014 г., в качестве секретов производства (ноу-хау) могут выступать практически любые сведения, в том чис-

ле и не имеющие никакого отношения к производству, например, сведения об особенностях управления деятельностью организации или учреждения, об особенностях организации системы охраны и т. п. И все сведения, которые ранее охранялись как сведения, составляющие коммерческую тайну, сегодня могут быть признаны секретами производства и охраняться в качестве объекта интеллектуальной собственности.

При применении режима коммерческой тайны для охраны секретов производства хозяйствующие субъекты сегодня сталкиваются с вопросом о том, как разграничить сегодня информацию, составляющую коммерческую тайну, которые не являются секретами производства, с последними. Полагаем, что выходом из данной ситуации могло бы быть закрепление в приказах по организации режима секретов производства в отношении отдельных сведений, а также указание в перечне сведений, составляющих коммерческую тайну организации, что отдельные из них являются еще и секретами производства.

МИНБАЛЕЕВ Алексей Владимирович, д.ю.н., доцент, заместитель декана юридического факультета, профессор кафедры конституционного и административного права Южно-Уральского государственного университета. E-mail: alexmin@bk.ru.

MINBALEEV Aleksey Vladimirovich, Doctor of Law, professor of department of constitutional and administrative law, associate of faculty of law dean at the South Ural State University. E-mail: alexmin@bk.ru.

УДК 004.056.5 + 004.021

Микова С. Ю., Оладько В. С.

ОЦЕНКА КАЧЕСТВА АЛГОРИТМА ОБНАРУЖЕНИЯ СЕТЕВЫХ АНОМАЛИЙ НА ОСНОВЕ ДИСКРЕТНОГО ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЯ С ПОМОЩЬЮ F-МЕРЫ

В работе рассматривается проблема оценки качества алгоритмов обнаружения сетевых аномалий. В качестве показателя качества используется гармоническая F-мера. Предложена методика исследования качества алгоритма. Приводится количественная оценка показателей полноты, точности F-меры. Проведены экспериментальные исследования качества алгоритма обнаружения сетевых аномалий на основе дискретного вейвлет-преобразования, показывающие зависимость качества алгоритма от размера скользящего окна.

Ключевые слова: *классификация, сетевая атака, точность, полнота*

Mikova S. Yu., Oladko V. S.

ASSESSMENT OF QUALITY OF NETWORK ANOMALIES DETECTION ALGORITHM BASED ON DISCRETE WAVELET TRANSFORMS USING THE F-MEASURE

The paper considers the problem of quality assessment algorithms detect network anomalies The quality of the algorithms proposed to estimate the harmonic F-measure. Method of research quality of the algorithm proposed. Quantitative assessment of the completeness, accuracy, F-measure is provided. Experimental study of the quality of network anomalies detection algorithm based on discrete wavelet transform, showing the dependence of the quality of the algorithm on the size of the sliding window.

Keywords: *classification, network attack, accuracy, completeness.*

Вторжение в систему злоумышленника может привести к утечке, искажению или недоступности данных, обрабатываемых в информационных системах организаций и в технологических сетях предприятия. Часто аномалия в сети – это один из признаков сетевой атаки злоумышленника [1]. Существует много алгоритмов обнаружения сетевых аномалий. Каждый из алгоритмов имеет свои особенности реализации, количество и тип анализируемых параметров сетевого трафика и/или сетевых пакетов. При этом в процессе обнаружения аномалий каждым из существующих алгоритмов решается за-

Таблица 1. Возможные результаты классификации аномалий

Класс A=anomaly		Принадлежность к классу A	
		ДА	НЕТ
Результат Классификации	Правильный	Truepositive (TP) *anomaly* ⟶ *anomaly*	Falsepositive (FP) *normal* ⟶ *anomaly* (Ошибка второго рода)
	Неправильный	Falsenegative (FN) *anomaly* ⟶ *normal* (Ошибка первого рода)	Truenegative (TN) *normal* ⟶ *normal*

Где TP - истино-положительное решение (правильно обнаруженные аномалии); FP - ложно-положительное решение (ошибки второго рода); FN - ложно-отрицательное решение (ошибки первого рода); TN - истино-отрицательное решение.

дача классификации. И от того, насколько точно и достоверно в результате классификации анализируемых данных будет принято решение о принадлежности их к аномалии или нет, будет напрямую зависеть качество алгоритма. Чем выше качество алгоритма обнаружения сетевых аномалий, тем более вероятно, что программное средство, реализующее данный алгоритм, способно выявить аномалию или возможную атаку в сети предприятия с минимальными пропусками или ложными срабатываниями. Следовательно, актуально решение задач, связанных с оценкой качества алгоритмов обнаружения сетевых аномалий.

Процедура оценки качества алгоритма обнаружения сетевых аномалий. Так как при обнаружении аномалии алгоритмов в первую очередь решается задача классификации, то авторами в данной работе в качестве основного критерия качества алгоритма предлагается использовать F-меру, которая представляет собой функцию от полноты и точности алгоритма. Под точностью, полнотой и F-мерой понимается следующее [2, 3]:

1) точность – это отношение правильно обнаруженных аномалий алгоритмом к сумме правильно обнаруженных аномалий алгоритмом и ошибок второго рода;

2) полнота – это отношение правильно обнаруженных аномалий алгоритмом к сумме правильно обнаруженных аномалий алгоритмом и ошибок первого рода;

3) F-мера – это удвоенное отношение произведения оценок полноты и точности к сумме оценок полноты и точности.

Таким образом, чем меньше будет ошибок первого и второго рода при обнаружении аномалий, тем более полным и точным будет алгоритм по их обнаружению [3]. Возможные результаты классификации аномалий алгоритмами обнаружения сетевых аномалий представлены в таблице 1.

Из определения полноты следует, что она вычисляется по следующей формуле 1:

$$Recall = \frac{TP}{TP + FN} \quad (1)$$

Из определения точности следует, что она вычисляется по следующей формуле 2:

$$Precision = \frac{TP}{TP + FP} \quad (2)$$

Из определения F-меры следует, что она вычисляется по следующей формуле 3:

$$F = 2\frac{Precision*Recall}{Precision + Recall} \quad (3)$$

В качестве объекта исследования авторами был выбран алгоритм обнаружения сетевых аномалий на основе дискретного вейвлет-преобразования (ДВП). Для оценки качества классификации алгоритмом был разработан программный комплекс, который в процессе функционирования позволяет собрать следующие данные, характеризующие алгоритм:

1) ошибки первого рода – FN;

2) ошибки второго рода – FP;

3) количество правильно идентифицированных аномалий – TP.

На основании собранных данных проводится оценка полноты и точности алгоритма, на основании которых затем вычисляется значение F-меры.

Методика оценки качества алгоритма с использованием в качестве инструментального средств разработанного программного комплекса может быть представлена в виде следующей последовательности шагов:

1) Установить необходимый минимальный размер окон в программе.

2) Для текущего размера окна сгенерировать модель трафика с заданным числом аномалий (N) и числом интервалов (M).

3) Обработать текущую модель с помощью алгоритма ДВП. Перенести значения N, TP, FN, FP в таблицу.

4) Повторить шаги 2–3 несколько раз для более точной вероятностной оценки.

5) Посчитать математическое ожидание для TP, FN, FP.

6) Посчитать точность и полноту по формулам (1) и (2) для текущего размера окна и текущего числа аномалий.

7) Повторить шаги 2–6 для других значений N при том же значении M. Для полноты и качества анализа желательно взять значения показательной функции от ряда чисел. Например, $N = 2^x$, где x = [1, 2, 3…9] при M = 2200.

8) Посчитать среднее для точности и полноты для текущего размера окна.

9) Увеличить размер окна и повторить шаги 1–8. В приведенном примере размеры окон принимались от 10 до 30 с шагом 5.

Экспериментальные исследования точности и полноты алгоритма дискретного вейвлет-преобразования. Входными данными при проведении экспериментов являются: размер окна 1 (W1), размер окна 2 (W2), число интервалов (I=2200) и количество поданных аномалий (A). Экспериментальные исследования состояли из пяти опытов для каждой выборки значений входных данных, приведенных в таблице 2.

Таблица 2. Значение выборок входных данных экспериментальных исследований

Параметры	Значение параметров									
№ выборки	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
W1	15	15	15	15	15	15	15	15	15	15
W2	10	10	10	10	10	10	10	10	10	10
A	1	2	4	8	16	32	64	128	256	512
№ выборки	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
W1	20	20	20	20	20	20	20	20	20	20
W2	15	15	15	15	15	15	15	15	15	15
A	1	2	4	8	16	32	64	128	256	512
№ выборки	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**
W1	25	25	25	25	25	25	25	25	25	25
W2	20	20	20	20	20	20	20	20	20	20
A	1	2	4	8	16	32	64	128	256	512

Затем на каждой выборке входных значений был проведён анализ сетевого трафика на предмет аномалий и для полученных результатов алгоритма вычислены значения полноты и точности по формулам 1, 2. Пример проведения анализа результатов работы алгоритма ДВП для входного параметра размер окна W= 10 представлен в таблице 3.

Таблица 3. Анализ результатов работы алгоритма ДВП для размера окон W1 = 15, W2 = 10

W1	15	15	15	15	15	15	15	15	15	15
W2	10	10	10	10	10	10	10	10	10	10
I	2200	2200	2200	2200	2200	2200	2200	2200	2200	2200
A	1	2	4	8	16	32	64	128	256	512
Опыт 1										
TP	1	1	2	5	10	20	26	6	4	0
FN	7	12	24	44	90	196	267	136	7	0
FP	0	1	2	3	6	12	38	122	152	512

Опыт 2										
TP	1	1	4	5	12	18	26	8	2	0
FN	12	18	32	52	104	159	274	95	5	0
FP	0	0	0	3	4	14	38	120	253	512
Опыт 3										
TP	1	1	2	4	6	18	22	10	2	0
FN	14	17	30	43	64	174	266	142	4	1
FP	0	1	2	4	10	14	42	118	254	512
Опыт 4										
TP	1	2	3	5	10	20	20	10	1	0
FN	3	14	31	49	101	182	270	139	6	0
FP	0	0	1	3	6	12	44	118	255	512
Опыт 5										
TP	0	0	2	6	15	19	25	8	0	1
FN	6	2	21	57	126	187	300	98	6	0
FP	1	2	2	2	1	13	39	120	256	512
Результирующая оценка алгоритма ДВП										
$TP_{средн.}$	0,8	1	2,6	5	10,6	19	23,8	8,4	1,8	0,2
$FN_{средн.}$	8,4	12,6	27,6	49	97	179,6	275,4	122	5,6	0,2
$FP_{средн.}$	0,2	0,8	1,4	3	5,4	13	40,2	119,6	234	512
Precision	0,8	0,55	0,65	0,62	0,66	0,593	0,37	0,065	0,007	0,00039
Recall	0,086	0,073	0,086	0,092	0,098	0,095	0,07	0,064	0,24	0,5

Далее по формуле 3 была рассчитана F-мера, зависящая от оценок полноты и точности для каждой выборки. Полученные значения F-меры представлены в таблице 4.

Таблица 4. Значения F-меры доя алгоритма ДВП

W1	15	15	15	15	15	15	15	15	15	15
W2	10	10	10	10	10	10	10	10	10	10
F	**0,156**	**0,129**	**0,152**	**0,161**	**0,171**	**0,164**	**0,131**	**0,065**	**0,148**	**0,00072**
W1	20	20	20	20	20	20	20	20	20	20
W2	15	15	15	15	15	15	15	15	15	15
F	**0,095**	**0,027**	**0,008**	**0,01**	**0,002**	**0,0014**	**0,0081**	**0,0056**	**0,0015**	**0,00075**
W1	25	25	25	25	25	25	25	25	25	25
W2	20	20	20	20	20	20	20	20	20	20
F	**0,073**	**0,022**	**0,004**	**0,007**	**0,001**	**0,005**	**0,007**	**0,003**	**0,0091**	**0,00077**

Для того чтобы более наглядно увидеть зависимость размера окна от F-меры, было рассчитано среднее значение F-меры для каждого размера окна. Результаты представлены в таблице 5 и на рисунке 1.

Таблица 5. Среднее значения F-меры для алгоритма ДВП

Размер окна	W1=15 W2=10	W1=20 W2=15	W1=25 W2=20
F	0,114	0,016	0,013

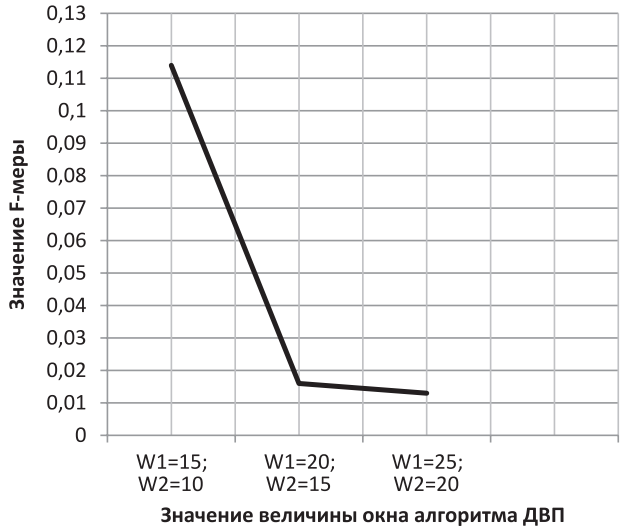

Рис.1. Зависимость F-меры от размера окна

Анализ полученных результатов исследования F-меры алгоритма дискретного вейвлет-преобразования показывает, что средние значения F-меры алгоритма напрямую зависят от такого входного параметра алгоритма, как размер окна. Чем меньше значение окна скользящего алгоритма, тем более высокое значение принимает F-мера, показывая лучшие значения (F=0,114) при величине окна W1=15;W2=10. Следовательно, можно сделать вывод, что для получения большего качества классификации алгоритмом необходимо при возможности минимизировать значение окон W1 и W2. А поскольку F-мера – это метрика, которая гармонически объединяет информацию о точности и полноте анализируемого алгоритма, то при использовании алгоритма ДВП для обнаружения сетевых аномалий необходимо еще в процессе обучения провести калибровку точности и полноты, варьируя значения окон W1 и W2, так как увеличение данных оценок влияет на увеличение качества классификации.

Примечания

1. Мельников Д. А., Петров В. Р., Радько А. Н., Бурый Д. С., Хрусталев С. А. Обнаружение уязвимостей информационно-технологических систем на основе анализа сетевого трафика//Безопасность информационных технологий. – 2013. - № 4. – С. 83–87.

2. Амелькин С. А. Оценка эффективности рекомендательных систем //Труды 14-й Всероссийской научной конференции «Электронные библиотеки: перспективные методы и технологии, электронные коллекции» — RCDL-2012, Переславль-Залесский, Россия, 15–18 октября 2012 г. – С. 288–291.

3. Микова С. Ю., Оладько В. С., Нестеренко М. А., Кузнецов И. А. Критерии оценки качества алгоритмов обнаружения сетевых аномалий // Международный научно-исследовательский журнал. – 2015. - № 4 (35) – С. 87–88.

Микова Софья Юрьевна, студент, кафедра «Информационная безопасность», ФГАОУ ВПО «Волгоградский государственный университет». E-mail: sofya_mikova@mail.ru

Mikova Sophia Yurievna student, Department of «Information Security», Volgograd State University. E-mail: sofya_mikova@mail.ru

Оладько Владлена Сергеевна, кандидат технических наук, доцент кафедры «Информационная безопасность», ФГАОУ ВПО «Волгоградский государственный университет», (8442) 46-03-68. E-mail: oladko.vs @yandex.ru

Oladko Vladlena Sergeevna, PhD (Engineering), Associate Professor of Information Security of «Information Security» department, Volgograd State University, (8442) 46-03-68. E-mail: oladko.vs@yandex.ru

УДК 342.5 + 34 : 002 + 351/354

Минбалеев А. В.

ОТЗЫВ НА ДИССЕРТАЦИЮ Э. В. ТАЛАПИНОЙ НА ТЕМУ «МОДЕРНИЗАЦИЯ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ В ИНФОРМАЦИОННОМ ОБЩЕСТВЕ: ИНФОРМАЦИОННО-ПРАВОВОЕ ИССЛЕДОВАНИЕ»

Отзыв официального оппонента подготовлен на диссертацию, защита которой состоялась в диссертационном совете при Институте государства и права Российской академии наук. Диссертация посвящена актуальной проблеме информационного права – вопросам модернизации государственного управления в информационном обществе: информационно-правовое исследование.

Ключевые слова: *информационное право, информационное общество, отзыв, диссертация.*

Minbaleev A. V.

REVIEW ON DISSERTATION OF A. V. TALAPINA ON THEME «MODERNIZATION OF PUBLIC ADMINISTRATION IN THE INFORMATION SOCIETY: INFORMATION-LEGAL STUDIES»

Reviewed official opponent is prepared on a thesis defense which was held at the Dissertation Council of the Institute of State and Law of the Russian Academy of Sciences. The thesis is devoted to the actual problem of information law - the modernization of public administration in the information society: information and legal research.

Keywords: *informative right, informative society, thesis.*

Процесс расширения границ использования информационных технологий в современном обществе, всех его государственных и негосударственных структур приводит к расширению сферы отношений, регулируемых нормами информационного законодательства. Содержание таких отношений определяется постепенно под воздействием внешних, объективно происходящих и исторически обусловленных процессов социально-экономического, политического и иного характера. При взаимодействии информации и общества происходит изменение социальных регуляторов (морали, права), а также структурное изменение всего общества под воздействием технических и технологических процессов.

Актуальность диссертационного исследования во многом определяется объективно обусловленной необходимостью упорядочения современной правовой составляющей организации и функционирования системы государственного управления с учетом вызовов информационного общества. В связи с активным внедрением информационных технологий и информационных систем в деятельность органов власти, приводящим к формированию единого государственного информационного пространства, следует также признать, что тема представленного исследования полностью соответствует критерию актуальности, а её разработка может иметь серьезное научно-практическое значение.

Научная новизна исследования заключается в новой постановке и подходах к изучению правовых проблем процесса модернизации государственного управления в контексте трансформирующего эффекта информационно-коммуникационных технологий, что позволило автору научно обосновать варианты их решения, которые могут быть реализованы в процессе совершенствования российского законодательства, а также разработать концепцию правового регулирования процесса модернизации государственного управления в цифровую эпоху.

Используя сравнительно-правовой метод в исследовании зарубежного опыта, диссертант выявил общее и особенное в воздействии информационно-коммуникационных технологий на государственное управление. Автором обоснованы возможные направления универсализации и унификации правового регулирования в информационно-управленческой сфере в условиях информационного общества как динамического социального процесса. Новаторским является подход автора к рассмотрению государственного управления не как к исключительно субординационным отношениям, а как результативному управленческому процессу, характеризующемуся множественностью субъектов, вовлеченных в механизмы прямой и обратной связи с использованием информационно-коммуникационных технологий, позволяющих обществу влиять на принимаемые решения.

Целостность, достоверность и обоснованность представленной на обсуждение научного сообщества концепции и других сделанных автором выводов подтверждает комплекс факторов, в том числе сформированный автором понятийный аппарат, методологические вопросы, исследование особенностей информационно-правового регулирования использования информационных технологий.

В предмет исследования введены вопросы, ранее не в полной мере подвергавшиеся научному анализу в информационном праве: основные направления информационно-правового регулирования модернизации государственного управления, включая вопросы расширения состава субъектов государственного управления и усложнения режимов их взаимодействия в условиях информационного общества; гарантии возможностей участия граждан, институтов гражданского общества и бизнес-структур в принятии управленческих решений и осуществлении контроля за властью в условиях информационного общества; проблемы поглощения информационной открытости государственного управления универсальным принципом транспарентности, формирование и правовое закрепление антикоррупционного информационного стандарта. Автором обоснован ряд важных положений: антикоррупционный эффект транспарентности, расширение границ и объема применения сравнительно-правового метода на основе глубокого изучения зарубежного опыта, роль информационного права как катализатора процессов публицизации и приватизации права и связующего звена, способствующего во многом формированию баланса публичного и частного права.

Положения, выносимые на защиту, отвечают критерию научной новизны и в боль-

шинстве своем имеют убедительное обоснование.

Важной характеристикой проведенного исследования является широкая апробация его результатов и расширение круга источников. Основные теоретические положения, выводы и научно-практические рекомендации, изложенные в диссертации, получили отражение в 10 монографиях, учебниках, курсах лекций и иных научных и учебных изданиях и иных публикациях, 32 из которых размещены в ведущих рецензируемых журналах и изданиях, указанных в перечне ВАК Министерства образования и науки РФ. Ряд работ опубликован на английском и французском языках в ведущих иностранных журналах.

Основные идеи и положения, изложенные в диссертационном исследовании, нашли отражение в научных публикациях автора, в выступлениях и докладах на научных конференциях, круглых столах и международных конгрессах, в экспертной работе над законопроектами в составе Комитета по безопасности Государственной Думы Федерального Собрания Российской Федерации (в период с 2005 по 2008 год). Результаты диссертационного исследования использовались автором в работе в составе Совета при Президенте Российской Федерации по кодификации и совершенствованию гражданского законодательства, в качестве эксперта по проекту ОЭСР по вопросам электронного правительства и др.

Кроме того, выводы и научно-практические рекомендации в рамках разработанной Методики анализа коррупциогенности нормативных правовых актов были апробированы в ходе тренингов для сотрудников высших законодательных и исполнительных органов субъектов Российской Федерации (всего около трети от общего числа субъектов Российской Федерации), обеих палат Федерального Собрания РФ, Правительства РФ и ряда федеральных органов исполнительной власти. Разработанная методика положена в основу постановления Правительства РФ от 26.02.2010 г. № 96 «Об антикоррупционной экспертизе нормативных правовых актов и проектов нормативных правовых актов».

Следует отметить не только теоретическое, но и прикладное значение проведенного исследования, так как его результаты использовались при работе автора над проектами федеральных законов «Об организации предоставления государственных и муниципальных услуг» и «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона "Об организации предоставления государственных и муниципальных услуг"», при подготовке аналитических записок и заключений по вопросам присоединения Российской Федерации к Конвенции о преступности в сфере компьютерной информации (Будапешт, 23.11.2001 г.), создания Российской общественной инициативы и др. Отдельные положения, сформулированные в диссертационном исследовании, применены автором при разработке проекта федерального закона «Об административных процедурах» и концепции проекта федерального закона «Об основах государственного управления», методики анализа коррупциогенности нормативных правовых актов.

Полученные промежуточные и конечные результаты диссертационного исследования были представлены в виде научного доклада в Обществе сравнительного законодательства во Франции (Париж, апрель 2011 г., апрель 2015 г.). Результаты разных этапов исследования использовались в учебном процессе на факультете права Национального исследовательского университета «Высшей школы экономики», Московской высшей школы экономических и социальных наук, французских университетов Париж 1 Пантеон Сорбонна и Париж Запад Нантер Ля Дефанс в рамках преподавания курса «Административное право России».

Структура работы способствует полноценному и последовательному раскрытию темы, что в конечном итоге позволило автору успешно решить стоящие перед ним задачи.

Работа состоит из введения, пяти глав, включающих девятнадцать параграфов, заключения, списка использованной литературы и приложения.

Первая глава диссертации «Информационное общество как фактор модернизации государственного управления» развивает идеи современных специалистов в сфере информационного общества и информационного права о том, что оно во многом оказывает всестороннее влияние на сущность государственного управления, автор приходит к выводу, что качество государственного управления не может быть объективно оценено внутри самого государственного аппарата, а системы оценки качества должны учи-

тывать удовлетворенность государственным управлением граждан, институтов гражданского общества и бизнес-структур. Исследуя активное формирование информационного общества как качественно нового состояния цивилизации, обеспечивающего свободный и открытый доступ каждого человека к информационным ресурсам, автор во втором параграфе обоснованно, на наш взгляд, дает авторское определение и выделяет основные направления реализации в условиях информационного общества информационной функции государства, которая проявляется в действиях государственных органов власти всех трех ветвей: создание информации; сопровождение информации, имеющей государственное значение; установление режима открытости органов государственной власти и передача информации вовне; сбор, обработка, охрана и защита информации, необходимой для реализации функций государства; учреждение специализированных структур в сфере информации и регулирование их деятельности; информационный обмен между органами государственной власти (внутри государственного аппарата); использование информации во внутренних интересах государства; хранение, уничтожение, переработка информации и создание на ее базе новой.

Развивая обоснованные идеи И. Л. Бачило о рассмотрении гражданского общества как социального, демократического и правового (информационное гражданское общество), диссертант аргументировано выявляет важные закономерности развития современного гражданского общества: тенденция граждан к виртуальному объединению при реализации права на управление (форумы, гражданские интернет-инициативы, социальные сети) и тенденция прогрессивной субъективизации прав в публично-правовой сфере. Также в первой главе автор приходит к обоснованному выводу о недостаточной системности регулирования информации и ИКТ как основных инструментов информационного общества, что, в свою очередь, оставляет открытым вопрос, является ли имеющееся правовое регулирование достаточным для отражения процессов модернизации государственного управления. В связи с этим автор систематизирует и рассматривает задачи современного права (информационного права, административного права и других отраслей) в контексте модернизации государственного управления.

Во второй главе «Правовые основы электронизации государственного управления» автором выделяются и рассматриваются этапы в развитии электронного правительства, предлагается ряд изменений в законодательство Российской Федерации в части оказания государственных и муниципальных услуг, поднимается проблема участия негосударственных субъектов в оказании государственных услуг и справедливо предлагается введение в наше законодательство категории юридического лица публичного права. В работе проводится качественный анализ опыта модернизации государственного управления в зарубежных странах, в том числе во Франции, сделаны аргументированные предложения по заимствованию ряда институтов и норм (параграф 5).

Интерес представляет и произведенный автором анализ открытого правительства, которое автор предлагает рассматривать как следующую стадию процесса модернизации государственного управления. Достаточно обоснованно автором указывается, что если электронное правительство концентрируется в основном на применении ИКТ в деятельности органов государственной власти, то открытое правительство имеет целью создание правового режима транспарентности информации в целях общественного контроля за властью (параграф 4).

В третьей главе «Информационная открытость государственного управления: правовое регулирование» исследуются особенности права на информацию как в контексте основных прав и свобод с позиции международных и российских стандартов, так и с позиции эволюции данного права в сфере государственного управления. В третьем параграфе «Актуализация проблемы права на информацию, которой обладают негосударственные субъекты» автор поднимает очень важную проблему для эффективного осуществления государственного управления – проблему доступа к информации, которой располагают негосударственные субъекты, в особенности, если это они осуществляют публично значимые функции. Данная проблема существует сегодня на практике. Например, негосударственные субъекты не являются субъектами, информация о деятельности которых может быть запрошена в силу Федерального закона «Об обеспечении доступа к информации о деятельности органов государственной власти и органов местного са-

моуправления». Также в данной главе автором поднимается проблема обеспечения доступа к правовой информации в цифровую эпоху и проблема ограничения доступа к информации.

Четвертая глава «Универсализация транспарентности как принципа правового регулирования государственного управления» посвящена анализу и обоснованию необходимости нормативного закрепления принципа транспарентности. Автором убедительно доказывается, что посредством этого принципа должен устанавливаться правовой режим транспарентности, который предполагает не просто открытость и доступность социально значимой информации (пассивная сторона), но и участие граждан, институтов гражданского общества и бизнес-структур в управлении и контроль публичной деятельности со стороны общества (активная сторона). В работе выделяется ряд элементов правового режима транспарентности государственного управления, дается их характеристика, на основе общего правового режима транспарентности государственного управления в целях противодействия коррупции разрабатывается специальный правовой режим – антикоррупционный информационный стандарт.

В пятой главе «Информационное право как регулятор государственного управления» определяется место информационного права в системе российского права. Автор справедливо отмечает, что у информационного права сегодня появляется функция посредника, оно способно «связывать» публичное и частное право, способствуя их балансу. В работе делается ряд предложений, направленных на развитие информационного законодательства, а, соответственно, и информационного права в целом.

Соискатель глубоко и всесторонне разобрался в теоретических основах исследуемых вопросов, а представленная им работа позволяет констатировать основательность проведенного исследования.

Работа написана понятным, юридически грамотным языком, рассуждения автора убедительны, логичны и последовательны. Используемые факты и иные данные достоверны, а сформулированные выводы научно обоснованы и юридически состоятельны.

В целях более полного раскрытия темы в тексте приводятся многочисленные практические примеры. Кроме того, следует особо отметить широкое использование международного опыта регулирования использования информационных технологий в государственном управлении и модернизации государственного управления в информационном обществе в целом.

Положительной оценки заслуживает научная смелость соискателя, его стремление к конструктивным решениям выявленных проблем. Диссертант умело использует междисциплинарные связи, что придает исследованию дополнительную глубину и масштабность. На основе полученных выводов предложены многочисленные изменения и дополнения в действующее законодательство. Считаем, что их реализация будет способствовать повышению эффективности правового регулирования использования информационных технологий в государственном управлении в условиях эволюции информационного общества.

Разработанные автором положения обогащают теорию информационного права и в своей совокупности создают теоретико-методологические предпосылки для решения проблем модернизация государственного управления в информационном обществе. Полученные диссертантом выводы по вопросам, не нашедшим достаточного отражения в научной литературе и действующих нормативных правовых актах, могут быть востребованы в ходе дальнейших научных исследований информационного права.

Практическая значимость исследования заключается в том, что сформулированные в нем выводы и практические рекомендации могут быть использованы в законотворческой и ведомственной нормотворческой деятельности в целях модернизация государственного управления в информационном обществе и совершенствования использования информационных технологий в государственном управлении на современном этапе.

Заключение работы отражает наиболее значимые выводы, полученные автором в ходе изучения всей темы. Все сделанные в работе выводы имеют рекомендации по их использованию в практической сфере и (или) при проведении дальнейших научных исследований.

Библиографический список содержит 652 источника и свидетельствует о комплексном подходе автора к подготовке диссертационного исследования.

Представленный автореферат в полной мере отражает основное содержание работы

и отвечает всем иным предъявляемым требованиям.

К числу вопросов и положений, требующих, на наш взгляд, обсуждения в ходе защиты диссертационного исследования, считаем необходимым отнести следующие.

1. Сложно согласиться однозначно с автором о неготовности информационного права к самостоятельному кодифицированному акту – Информационному кодексу. Одной из основных причин автор указывает отсутствие такого показателя (ориентира), как количественный. Указывается, в частности, что «кодификация действительно выйдет на повестку дня, когда собственно информационное законодательство хотя бы сравняется в объеме с межотраслевым информационным "блоком"» (с. 384). Полагаем все же, что нельзя брать за основу данный показатель. Межотраслевой информационный блок будет всегда неизменно расти, поскольку особенности развития современного общества как информационного диктуют всепроникающее значение информации и «вынужденность» отраслевого законодательства регулировать информационные отношения. Информационно-правовые нормы во многом появляются в ответ на увеличение объема межотраслевого информационного «блока» и появление новых институтов. Но «угнаться» за ним вряд ли когда получится, в связи с чем задачей информационно-правового регулирования является формирование базовых закономерностей регулирования отношений в информационной сфере, отражающих их особенности, которые бы использовались другими отраслями. К сожалению, сегодня приходится констатировать, что законодатель при регулировании информационных отношений в тех или иных отраслях не учитывает особенности информационных отношений и не использует информационно-правовые нормы как основу для их регулирования. В связи с этим Информационный кодекс необходим и как «авторитетный» источник для отраслевого законодательства, и как важный источник для черпания закономерностей регулирования информационных отношений в рамках специального информационного законодательства, и как важный ориентир для развития информационного права как отрасли права, отрасли законодательства, науки и учебной дисциплины.

Автор правильно указывает, что «кодекс нельзя создавать искусственно, лишь для оправдания существования правовой отрасли» (с. 385), но, как нам представляется, информационное право уже не просто существующая, а активно развивающаяся отрасль права и уже сложившийся массив информационно-правовых норм, понятийного аппарата, принципов, теоретических подходов говорят о возможности конструирования самостоятельного кодифицированного акта.

2. В диссертации автор рассматривает информационное право как комплексную отрасль российского права, которое расположено к общесистемному комплексному регулированию и даже инициирует его. Автор диссертации при этом, к сожалению, не столь детально исследовал вопросы предмета, метода, системы, принципов информационного права, закономерностей его развития как самостоятельной институциональной единицы. В связи с этим сделанный вывод о рассмотрении информационного права как комплексной отрасли представляется в недостаточной степени обоснованным. Полагаем, что сегодня информационное право уже можно рассматривать как самостоятельную отрасль российского права, для которой характерны следующие признаки: предмет; отраслевой метод информационного права, включающий базовые характеристики, присущие самостоятельным отраслям права, и обретающий закономерности собственного развития в тесном взаимодействии с предметом; принципы информационного права; механизм правового регулирования общественных отношений в информационной сфере, который приобретает специфические черты в виде комплекса самостоятельных юридических фактов, правоотношений, специальных субъектов, объектов правоотношений, самостоятельных субъективных прав и юридических обязанностей, особенностей их реализации с помощью уникального подбора и сочетания способов правового регулирования.

3. Исследуя разные стороны процесса внедрения ИКТ в функционирование органов государственной власти, диссертант справедливо отмечает проблему «цифрового неравенства» (с. 105, 196, 276, 317). При этом было бы желательно более глубокое изучение данного аспекта и, в особенности, различий информационно-правового сознания, что позволит успешно решать вопросы повышения правовой квалификации в сфере информационных отношений и готовности

представителей разных профессий к реальному использованию цифровых технологий.

Обозначенные положения носят дискуссионный характер и не влияют на общую положительную оценку представленной работы.

Общий вывод: представленная диссертационная работа по теме «Модернизация государственного управления в информационном обществе: информационно-правовое исследование» Эльвиры Владимировны Талапиной является завершенным, самостоятельным, монографическим исследованием, обладающим актуальностью, научной новизной, теоретической и практической значимостью. Актуальность рассмотренных вопросов, четкость аргументации, логичность и последовательность выводов, внутреннее единство работы, а также новые научные результаты и положения делают данную работу интересной не только для специалистов в области информационного и других отраслей права, но и для широкой аудитории читателей. Данное исследование, бесспорно, имеет серьезное научное, учебно-методическое и практическое значение. Принимая во внимание актуальность решенных в его рамках вопросов, можно говорить о том, что соискателем решена крупная научная проблема, имеющая существенное значение для отрасли информационного права. Диссертационная работа соответствует требованиям, предъявляемым к диссертациям на соискание ученой степени доктора юридических наук, установленным абзацем 1 п. 9 Положения о порядке присуждения ученых степеней, утвержденного постановлением Правительства Российской Федерации от 24 сентября 2013 г. № 842, является самостоятельно выполненным и завершенным исследованием, а ее автор заслуживает присуждения искомой ученой степени доктора юридических наук по специальности 12.00.13 – информационное право.

Минбалеев Алексей Владимирович, д.ю.н., доцент, профессор кафедры конституционного и административного права ЮУрГУ. E-mail: alexmin@bk.ru.

Minbaleev Aleksey Vladimirovich, Professor of department in the Department of Constitutional and Administrative Law at the South Ural State University (national research university). Doctor of Law. E-mail: alexmin@bk.ru.

ТРЕБОВАНИЯ К СТАТЬЯМ, ПРЕДСТАВЛЯЕМЫМ К ПУБЛИКАЦИИ В ЖУРНАЛЕ

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

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

В начале статьи помещаются: инициалы и фамилия автора (авторов), название статьи, **аннотация** на русском языке объемом **не менее 700 знаков или 10 строк,** ниже отдельной строкой — ключевые слова. **Ключевые слова** приводятся в именительном падеже в количестве до десяти слов. Инициалы и фамилия автора (авторов) дублируются транслитерацией. **Должны быть переведены на английский язык название статьи, аннотация, ключевые слова.**

В конце статьи перед данными об авторе должна быть надпись *«Статья публикуется впервые»,* ставится дата и авторучкой подпись автора (авторов). При пересылке статьи электронной почтой подпись автора сканируется в черно-белом режиме, сохраняется в формате *.tif или *.jpg и вставляется в документ ниже затекстовых сносок. (Либо сканируется последняя страница статьи с подписью и высылается по электронной почте отдельным файлом.)

Обязательно для заполнения: в конце статьи (в одном файле) на русском языке помещаются сведения об авторе (авторах) — полностью имя, отчество, фамилия, затем ученая степень, ученое звание, должность, кафедра, вуз (или организация, в которой работает автор); рабочий адрес вуза или организации (полные – включая название, город и страну – адресные сведения вместе с почтовым индексом, указывать правильное полное название организации, желательно – его официально принятый английский вариант), электронный адрес и контактные телефоны. **Эти данные об авторе должны быть переведены на английский язык.**

Для рассмотрения вопроса о публикации статьи в редакцию журнала необходимо выслать на электронную почту:

1) рукопись статьи, подписанную на последней странице всеми авторами. В рукописи должны быть полные сведения об авторах;

2) в случае, если статья имеет рецензию и заверена печатью, ее оригинал необходимо отправить в редакцию и по электронной почте в отсканированном виде с обязательным указанием контактов рецензента;

3) на статью необходимо выслать экспертное заключение о возможности открытого опубликования (образцы: заключение от руководителя эксперта (см. стр. 50) или заключение от экспертной комиссии (см. стр. 51))

Библиографические ссылки

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

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

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

Ниже приводятся образцы оформления ссылок:

а) на монографии:

[1] Белова М. С., Кинсбурская В. А., Ялбулганова А. А. Налоговый контроль и ответственность: анализ законодательства, административной и судебной практики / под ред. А. А. Ялбулганова.— М. : Знание, 2008.— С. 12.

б) на статьи из сборников:

[1] Клишина М. А. Новое в порядке составления проекта бюджета // Финансовое право России: актуальные проблемы / под ред. А. А. Ялбулганова.— М., 2007.— С. 101.

в) статьи из журналов и продолжающихся изданий:

[1] Глушко Е. К. Административно-правовая природа государственных корпораций // Реформы и право.— 2008.— № 3.— С. 38—43.

г) авторефераты диссертаций:

[1] Стрижова О. А. Правовое регулирование таможенной стоимости : автореф. дис. … канд. юрид. наук.— М., 2008.— С. 7.

д) интернет-страницы:

Противодействие коррупционным правонарушениям // Юридическая Россия: федеральный правовой портал. URL: http://law.edu.ru/news/news.asp?newsID=12954 (дата обращения: 08.01.2009).

В редакцию журнала статья передается качественно по электронной почте одним файлом (название файла — фамилия автора). Тема электронного письма: Вестник УрФО. Безопасность в информационной сфере.

Отправляемая статья должна быть вычитана автором; устранены все грамматические, пунктуационные, синтаксические ошибки, неточности; выверены все юридические и научные термины. За ошибки и неточности научного и фактического характера ответственность несет автор (авторы) статьи.

Поступившие в редакцию материалы возврату не подлежат.

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

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

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ
Должность руководителя
организации или лица с
соответствующими полномочиями
_____И. О. Фамилия
«___»_____2015 г.

ЗАКЛЮЧЕНИЕ № _____

о возможности открытого опубликования

_____
(наименование материалов, подлежащих экспертизе)

Руководитель-эксперт[1] _____

в период с «___»_____20___г. по «___»_____20___г. провел экспертизу материалов

_____
(наименование материалов, подлежащих экспертизе)

на предмет отсутствия (наличия) в них сведений, составляющих государственную тайну, и сведений, подпадающих под действие законодательства об экспортном контроле, и возможности (невозможности) их открытого опубликования.

Руководствуясь Законом Российской Федерации «О государственной тайне», Перечнем сведений, отнесенных к государственной тайне, утвержденным Указом Президента Российской Федерации от 30 ноября 1995 г. № 1203, а также Перечнем сведений, подлежащих засекречиванию Министерства образования и науки РФ, утвержденным приказом Минобрнауки РФ № 36с от 10.11.2014 г., а также Федеральным законом «Об экспортном контроле» от 18.07.1999 г. № 183-ФЗ и Указами Президента РФ № 1661 от 17.12.2011 г., № 1005 от 08.08.2001 г., № 36 от 14.01.2003 г., № 202 от 14.02.1996 г., № 1083 от 20.08.2007 г., № 1082 от 28.08.2001 г., руководитель-эксперт установил:

1) Сведения, содержащиеся в рассматриваемых материалах, находятся в компетенции *Наименование организации.*

2) Сведения, содержащиеся в рассматриваемых материалах, _____

_____
(указываются сведения, содержащиеся в материалах)

не подпадают под действие Перечня сведений, составляющих государственную тайну (статья 5 Закона Российской Федерации «О государственной тайне»), не относятся к Перечню сведений, отнесенных к государственной тайне, утвержденному Указом Президента Российской Федерации от 30 ноября 1995 г. № 1203, не подлежат засекречиванию, не подпадают под действие законодательства об экспортном контроле и данные материалы могут быть открыто опубликованы.

Руководитель-эксперт (Ф.И.О., подпись)

Секретарь ЭК (Ф.И.О., подпись)

[1] Если экспертиза материалов проводится руководителем структурного подразделения университета, в котором работает автор подготовленных материалов

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ
Должность руководителя
организации или лица с
соответствующими полномочиями
_____И. О. Фамилия
«___»_____2015 г.

ЗАКЛЮЧЕНИЕ № _____

о возможности открытого опубликования

_____
(наименование материалов, подлежащих экспертизе)

Экспертная комиссия в составе _____

в период с «___»_____20___г. по «___»_____20___г. провела экспертизу материалов

_____
(наименование материалов, подлежащих экспертизе)

на предмет отсутствия (наличия) в них сведений, составляющих государственную тайну, и сведений, подпадающих под действие законодательства об экспортном контроле, и возможности (невозможности) их открытого опубликования.

Руководствуясь Законом Российской Федерации «О государственной тайне», Перечнем сведений, отнесенных к государственной тайне, утвержденным Указом Президента Российской Федерации от 30 ноября 1995 г. № 1203, а также Перечнем сведений, подлежащих засекречиванию Министерства образования и науки РФ, утвержденным приказом Минобрнауки РФ № 36с от 10.11.2014 г., а также Федеральным законом «Об экспортном контроле» от 18.07.1999 г. № 183-ФЗ и Указами Президента РФ № 1661 от 17.12.2011г, № 1005 от 08.08.2001 г., № 36 от 14.01.2003 г., № 202 от 14.02.1996 г., № 1083 от 20.08.2007 г., № 1082 от 28.08.2001 г., экспертная комиссия установила:

1) Сведения, содержащиеся в рассматриваемых материалах, находятся в компетенции *Наименование организации.*

2) Сведения, содержащиеся в рассматриваемых материалах, _____

_____
(указываются сведения, содержащиеся в материалах)

не подпадают под действие Перечня сведений, составляющих государственную тайну (статья 5 Закона Российской Федерации «О государственной тайне»), не относятся к Перечню сведений, отнесенных к государственной тайне, утвержденному Указом Президента Российской Федерации от 30 ноября 1995 г. № 1203, не подлежат засекречиванию, не подпадают под действие законодательства об экспортном контроле и данные материалы могут быть открыто опубликованы.

Председатель комиссии (Ф.И.О., подпись)

Члены ЭК : (Ф.И.О., подпись)

Секретарь ЭК (Ф.И.О., подпись)

ВЕСТНИК УрФО
Безопасность в информационной сфере № 2(16) / 2015

Дата выхода в свет 30.06.2015. Формат 70×108 1/16. Печать трафаретная.
Усл.-печ. л. 4,5. Тираж 100 экз. Заказ 660/709.
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(16) / 2015

Date of publication of the 30.06.2015. Format 70×108 1/16. Screen printing.
Conventional printed sheet 4,5. Circulation – 100 issues. Order 660/709. Open price.

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