



ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
**РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ  
УНИВЕРСИТЕТ ПРАВОСУДИЯ**

**Д. А. Ловцов**

**Системология правового  
регулирувания информационных  
отношений в инфосфере**

*Монография*

Москва  
2016

УДК 34.01:349:681

ББК 67

Л68

**Автор**

*Ловцов Д. А.*, доктор технических наук, профессор, заслуженный деятель науки РФ (Российский государственный университет правосудия)

**Рецензенты:**

*Запольский С. В.*, доктор юридических наук, профессор, заслуженный юрист РФ (Институт государства и права Российской академии наук)

*Исаков Б. В.*, доктор юридических наук, профессор, заслуженный юрист РФ (Национальный исследовательский университет «Высшая школа экономики»)

Л68 **Ловцов Д. А.** Системология правового регулирования информационных отношений в инфосфере: Монография. — М. : РГУП, 2016. — 316 с.

ISBN 978-5-93916-505-1

В монографии исследуются современное состояние системологии правового регулирования информационных отношений в инфосфере и подходы к информатизации правового регулирования на основе внедрения новых и традиционных информационных технологий. Раскрываются концептуально-теоретические и методологические проблемы правового регулирования данных отношений и его модельно-алгоритмическое, лингвистическое и организационно-правовое обеспечение, а также результаты научных исследований, проводимых в рамках межвузовского постоянно действующего научного семинара «Информатизация правосудия» кафедры информационного права, информатики и математики Российского государственного университета правосудия. Теоретические разработки иллюстрируются значительным количеством таблиц, схем, рисунков. Работа содержит приложения и глоссарий основных терминов.

Адресуется научным и научно-педагогическим работникам, специалистам в области информационного права, правовой информатологии и правовой информатики, а также магистрантам и бакалаврам, изучающим информационное право, современные информационно-правовые технологии, автоматизированные системы юридического назначения.

© Ловцов Д. А., 2016

© Российский государственный университет правосудия, 2016

ISBN 978-5-93916-505-1

## СОДЕРЖАНИЕ

|   |    |
|---|----|
| <b>Вступительное слово</b> .....  | 6  |
| <b>Список принятых сокращений</b> .....   | 10 |
| <b>Введение</b> .....   | 14 |
| <b>Глава 1. Системный анализ информационной сферы общественно-производственной деятельности и классификация информационных правоотношений</b> ..... | 24 |
| 1.1. Информационная деятельность, виды, атрибуты и качественные формы проявления информации в системах правового регулирования .....                | 26 |
| 1.2. Структурная декомпозиция качества и определение юридически значимых свойств содержательной информации .....                                    | 37 |
| 1.3. Логическая классификация информационных отношений в инфосфере и определение способов обеспечения информационной безопасности эргасистем ...    | 45 |
| 1.4. Продуктивная классификация информационных правоотношений и определение предмета и системы информационного права .....                          | 49 |
| 1.5. Функциональная систематизация информационных правоотношений в области средств массовой информации .....  | 58 |
| 1.6. Логическая организация правосознания и сознания информационного деятеля, классификация «информационного оружия» .....                          | 70 |
| <b>Глава 2. Теоретико-правовой анализ ключевых проблем правового регулирования информационных отношений в инфосфере</b> .....                       | 83 |
| 2.1. Международно-правовое обеспечение глобального информационного обмена .....   | 83 |

|   |     |
|---|-----|
| 2.2. Международно-правовые меры обеспечения информационной безопасности российских телематических сетей .....   | 94  |
| 2.3. Направления создания и развития единого информационного пространства систем правового регулирования .....  | 103 |
| 2.4. Основные правовые понятия и способы правового сдерживания информационно-компьютерной преступности .....  | 115 |
| 2.5. Правовые меры обеспечения легитимности судебной экспертизы с использованием полиграфа .....  | 133 |
| 2.6. Проблема обеспечения эффективности систем правового регулирования информационных отношений в инфосфере .....   | 141 |
| <b>Глава 3.</b> Разработка концептуально-теоретических и научно-методологических вопросов системологии правового регулирования информационных отношений в инфосфере ..... | 147 |
| 3.1. Обоснование архитектуры информационно-правового знания и источников информационного права ..   | 148 |
| 3.2. Концептуально-логическая модель системы правового регулирования .....  | 155 |
| 3.3. Концепция комплексного «ИКС»-подхода к исследованию сложных правозначимых явлений как систем .....   | 162 |
| 3.4. Концептуально-логическая модель информационной сферы и соответствующий базис лингвистического обеспечения правового регулирования .....                              | 170 |
| 3.5. Концепция информационной безопасности правовой эргасистемы .....   | 173 |
| 3.6. Концепция гарантированной безопасности привилегированной информации в эргасистеме .....  | 181 |
| <b>Глава 4.</b> Разработка модельно-алгоритмического обеспечения правового регулирования информационных отношений в инфосфере .....                                       | 192 |

---

|  |     |
|--|-----|
| 4.1. Реляционная модель юридического понятия «тайна» ..  | 192 |
| 4.2. Обоснование рациональных моделей<br>правового регулирования отношений<br>в области коммерческой тайны .....   | 198 |
| 4.3. Модели правового регулирования отношений<br>в области применения электронной подписи<br>и соответствующего базового информационного<br>правоотношения ..... | 217 |
| 4.4. Модели и меры обеспечения информационной<br>безопасности системы судебного правоприменения ....   | 226 |
| 4.5. Модельно-алгоритмическое обеспечение<br>правового регулирования отношений в области<br>электронного документооборота в правовых<br>эргасистемах .....       | 243 |
| 4.6. Модельно-алгоритмическое обеспечение<br>защиты результатов интеллектуальной деятельности<br>в инфосфере глобальных телематических сетей .....               | 256 |
| <b>Заключение</b> .....  | 276 |
| <b>Список литературы</b> .....   | 284 |
| <b>Глоссарий</b> .....   | 298 |
| <b>Приложение 1.</b> Проблемы развития и внедрения<br>государственной автоматизированной системы РФ<br>«Правосудие» .....  | 304 |
| <b>Приложение 2.</b> Концептуальная формализация<br>базовых элементов информационных правоотношений<br>в инфосфере .....   | 311 |

Тогда возможно дать следующее *определение*: 1 *бит* (*двед*) — это единица измерения количества информации, содержащейся в сообщении, выраженном одним из двух равновероятных взаимоисключающих (альтернативных) состояний.

## 2. Методы криптографических преобразований информации

Можно условно выделить три основных исторических периода применения криптографических методов для защиты содержательной информации:

- прикладная тривиальная криптография (50 г. до н. э. — 50-е гг. XX в.);
- симметричная криптография с закрытым (секретным) ключом (50-е гг. XX в. — 70-е гг. XX в.);
- асимметричная криптография с открытыми (публичными) ключами (70-е гг. XX в. — н/вр.).

Начало *первого* периода связано с применением так называемого «шифра Цезаря», суть которого состояла в том, что в зашифрованных сообщениях императора каждая буква  $X$  латинского алфавита (26 букв и пробел) заменялась на третью букву справа по формуле шифра (см. табл. П2.1):

$$Y = (X + 3) \bmod 27,$$

где  $\bmod 27$  — операция нелинейного (циклического) вычитания по модулю 27 (чтобы буквы в зашифрованном сообщении тоже соответствовали латинскому алфавиту).

*Пример.* Для передачи условного сообщения с текстом: «*Game is over*» в уме выполняются следующие операции побуквенного сложения и вычитания по  $\bmod 27$  (см. таб. П2.2).

В результате получается зашифрованное сообщение, содержащее текст: «*Jdphclvcryhu*», которое расшифровывается в обратном порядке.

Поскольку все языки имеют ярко выраженное частное распределение [94] (например, после пробела в латинском языке чаще всего используется буква  $E$ ), то текст, зашифрованный таким образом, легко (при условии его достаточной «длины») расшифровать на основе его частотного анализа и замены букв (например,  $C$  на про-

бел, *H* на *E* и др.). Как, например, это сделал герой рассказа О’Генри «Золотой жук», заменяя в пиратской криптопиктограмме на буквы английского языка знаки в виде пляшущих человечков в зависимости от частоты их использования.

Таблица П2.1

**Латинская алфавитно-цифровая матрица**

|          |          |          |          |          |          |          |          |          |          |          |          |          |          |
|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|
| <i>A</i> | <i>B</i> | <i>C</i> | <i>D</i> | <i>E</i> | <i>F</i> | <i>G</i> | <i>H</i> | <i>I</i> | <i>J</i> | <i>K</i> | <i>L</i> | <i>M</i> | <i>N</i> |
| 1        | 2        | 3        | 4        | 5        | 6        | 7        | 8        | 9        | 10       | 11       | 12       | 13       | 14       |
| <i>O</i> | <i>P</i> | <i>Q</i> | <i>R</i> | <i>S</i> | <i>T</i> | <i>U</i> | <i>V</i> | <i>W</i> | <i>X</i> | <i>Y</i> | <i>Z</i> | –        |          |
| 15       | 16       | 17       | 18       | 19       | 20       | 21       | 22       | 23       | 24       | 25       | 26       | 27       |          |

Таблица П2.2

**Шифрование сообщения по методу Цезаря**

|          |          |          |          |            |          |          |            |          |          |          |          |
|----------|----------|----------|----------|------------|----------|----------|------------|----------|----------|----------|----------|
| <i>G</i> | <i>A</i> | <i>M</i> | <i>E</i> | –          | <i>I</i> | <i>S</i> | –          | <i>O</i> | <i>V</i> | <i>E</i> | <i>R</i> |
| 7+3      | 1+3      | 13+3     | 5+3      | 27+3 mod27 | 9+3      | 19+3     | 27+3 mod27 | 15+3     | 22+3     | 5+3      | 18+3     |
| <i>J</i> | <i>D</i> | <i>P</i> | <i>H</i> | <i>C</i>   | <i>L</i> | <i>V</i> | <i>C</i>   | <i>R</i> | <i>Y</i> | <i>H</i> | <i>U</i> |

Все дальнейшие усовершенствования данного «шифра Цезаря» (путем введения в формулу шифра десятичных при *X* коэффициентов или замены коэффициента сдвига, равного 3, на другие значения<sup>1</sup>; замены буквы *X* не на одну, а на несколько букв для «выравнивания» частотного распределения и др.) не намного повысили криптостойкость данного типа шифров.

*Второй* исторический период криптографии связан с именем американского ученого К. Шеннона и характеризуется использованием так называемых «труднообратимых» функций, т. е. нелинейных. Например, функций возведения в *m*-ю степень численного номера каждой буквы сообщения ( $Y = X^m \text{mod} N$ ). Не зная

<sup>1</sup> Например, сменивший Цезаря император Октавиан не без того же успеха писал в шифровках просто следующую букву алфавита, т. е.  $Y = (X + 1) \text{mod} 27$ .

значения  $m$  (ключ), криптоаналитику приходилось путем последовательного трудоемкого перебора извлекать корни различных степеней из чисел перехваченного зашифрованного сообщения ( $X = \sqrt[k]{Y \bmod N}$ ,  $k = 2, 3, 4, \dots$ ).

В этот период возникла *организационно-правовая проблема* тайного распределения множества  $M = n(n - 1)$  «симметричных» секретных ключей между  $n$  абонентами практически полносвязных (по принципу «каждый с каждым») развивающихся информационных сетей. Для решения этой проблемы американскими инженерами Диффи и Хеллманом была предложена современная система математически связанной пары «асимметричных» ключей  $\langle K, K^* \rangle$  абонента, один из которых  $K$  — открытый (объявляется всем абонентам и может передаваться по открытым информационным каналам), а другой  $K^*$  — тайный, хранимый абонентом в секрете.

*Третий* современный этап — это, главным образом, этап асимметричной криптографии, при которой необходимое количество ключей абонентов полносвязной (или любой другой) сети равно  $2n$ , что намного меньше  $n(n - 1)$ .

При этом и на передающей, и на приемной сторонах используется однотипная операция возведения в степень в модульной арифметике, причем на передающей стороне степень является значением открытого ключа  $K$  абонента-получателя, а на приемной — значением его закрытого ключа  $K^*$ :

$$Y = X^K \bmod N;$$

$$X = Y^{K^*} \bmod N.$$

Данная информационно-криптографическая технология применяется, в частности, для организации безопасного сетевого информационного обмена с использованием ЭЦП.

Научное издание

**Ловцов Дмитрий Анатольевич**

**СИСТЕМОЛОГИЯ  
ПРАВОВОГО РЕГУЛИРОВАНИЯ  
ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ  
В ИНФОСФЕРЕ**

*Монография*

Редактор *Е. В. Алферова*  
Корректор *Л. А. Затылаева*  
Верстка, оформление: *А. А. Гришин*

Подписано в печать 11.02.2016.  
Формат 60x90<sup>1</sup>/<sub>16</sub>. Усл. печ. л. 19,75.  
Тираж 100 экз. (1-ый завод)

Российский государственный университет правосудия  
117418, г. Москва, ул. Новочеремушкинская, д. 69а.