



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

Д. А. Ловцов

**Системология правового
регулирования 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

Вступительное слово	6
Список принятых сокращений	10
Введение	14
Глава 1. Системный анализ информационной сферы общественно-производственной деятельности и классификация информационных правоотношений	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
Глава 2. Теоретико-правовой анализ ключевых проблем правового регулирования информационных отношений в инфосфере	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
Глава 3. 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
Глава 4. Разработка модельно-алгоритмического обеспечения правового регулирования информационных отношений в инфосфере	192

Содержание

4.1. Реляционная модель юридического понятия «тайна» ..	192
4.2. Обоснование рациональных моделей правового регулирования отношений в области коммерческой тайны	198
4.3. Модели правового регулирования отношений в области применения электронной подписи и соответствующего базового информационного правоотношения	217
4.4. Модели и меры обеспечения информационной безопасности системы судебного правоприменения	226
4.5. Модельно-алгоритмическое обеспечение правового регулирования отношений в области электронного документооборота в правовых эргасистемах	243
4.6. Модельно-алгоритмическое обеспечение защиты результатов интеллектуальной деятельности в инфосфере глобальных телематических сетей	256
Заключение	276
Список литературы	284
Глоссарий	298
Приложение 1. Проблемы развития и внедрения государственной автоматизированной системы РФ «Правосудие»	304
Приложение 2. Концептуальная формализация базовых элементов информационных правоотношений 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 *mod27* — 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 *mod27* (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

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

Таблица П2.2

Шифрование сообщения по методу Цезаря

G	A	M	E	—	I	S	—	O	V	E	R
$7+3$	$1+3$	$13+3$	$5+3$	$27+3 \bmod 27$	$9+3$	$19+3$	$27+3 \bmod 27$	$15+3$	$22+3$	$5+3$	$18+3$
J	D	P	H	C	L	V	C	R	Y	H	U

Все дальнейшие усовершенствования данного «шифра Цезаря» (путем введения в формулу шифра десятичных при X коэффициентов или замены коэффициента сдвига, равного 3, на другие значения¹; 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 ($Y = X^m \bmod N$). Не зная

¹ Например, сменивший Цезаря император Октавиан не без того же успеха писал в шифровках просто следующую букву алфавита, т. е. $Y = (X + 1) \bmod 27$.

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 60х90¹/₁₆. Усл. печ. л. 19,75.
Тираж 100 экз. (1-ый завод)

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