ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ ПРАВОСУДИЯ

Д. А. Ловцов

Системология правового регулирования информационных отношений в инфосфере

Монография

Москва
2016

ŋqdqуeɤ ɓƎ dəqƎɓɤзə d єɔɑɓɔɤ Ɉqdqɤqɤè

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 информологии и правовой информатики, а также магистрантам и бакалаврам, изучающим информационное право, современные информационно-правовые технологии, автоматизированные системы юридического назначения.

ISBN 978-5-93916-505-1

СОДЕРЖАНИЕ

ŋqdqyeY bE dedEbYse d eaqbaY Jqddyqyè

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):

$Y = (X + 3) mod 27$,

где $mod 27$ — 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 $mod 27$ (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-

ŋqqqʎɐʎ bƎ dəqƎbʎɜə d ɛɔɑbɔʎ Ɉqqqʎqʎè

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 mod27	9+3	19+3	27+3 mod27	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 значения[1]; 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 ($Y = X^m mod N$). Не зная

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

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

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 $<K, K^*>$ 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^*:

$Y = X^{K} \, mod \, N$;

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

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. Запылаева*
Верстка, оформление: *А.А. Гришин*

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

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