УДК 681.324.06

Е.В. Горковенко

ПРИМЕНЕНИЕ НЕТРАДИЦИОННЫХ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ В СИСТЕМАХ С МАНДАТНОЙ ПОЛИТИКОЙ УПРАВЛЕНИЯ ДОСТУПОМ К ИНФОРМАЦИИ

Общепризнанными мерами по формированию режима информационной безопасности в компьютерных и телекоммуникационных системах являются методы криптографии и системы разграничения доступа. В настоящее время внедрение систем разграничения доступа для информации ограниченного пользования сдерживается недоверием ответственных работников, так называемого «первого отдела» и ограничивается только организационными и техническими мероприятиями по защите данных: хранить документы на бумажных носителях в сейфах или электронные документы на выделенном компьютере без сетевой поддержки.

Многоуровневое управление контролем доступа, реализующее полномочную (нормативную) политику безопасности, есть разграничение доступа субъектов к объектам, основанное на характеризуемой меткой конфиденциальности информации, содержащейся в объектах и официальном разрешении (допуске) субъектов обращаться к информации такого уровня конфиденциальности. Организация многоуровневого контроля при мандатном разграничении доступа осуществляется через понятия уровня секретности объекта и степени доверия субъекта.

Контроль полномочий доступа имеет характерные особенности в соответствии с принятыми в нашей стране процедурами работы с информацией ограниченного пользования. Это накладывает ряд ограничений при формировании правил разграничения доступа и управлении матрицей прав доступа. В предлагаемой модели мандатного разграничения доступа [1] реализованы: расширенный список прав доступа и управление доступом с учетом права реализации. Объекты защиты (файлы, директории, сообщения, записи) и субъекты защиты (пользователи, программы, процедуры) классифицированы и структурированы с целью оптимального управления доступом и реализации полной системы многоуровневой защиты при условия безызбыточного хранения данных в БД.

Множество $S = \{s_1,...,s_j,...,s_J\}, j = \overline{1,J}$ рассматривается как объединение двух подмножеств $S^{(1)}$ и $S^{(2)}$: $S = S^{(1)} \cup S^{(2)}$, где $S^{(1)}$ – подмножество субъектов (владельцы объектов), имеющих право подписи документов, право переписки, право на разрешение доступа к объектам и право ликвидации доступа; $S^{(2)}$ – подмножество субъектов, не имеющих вышеперечисленных прав, но имеющих право исполнения, как например редактирования и чтения документов. Каждому субъекту защиты (СЗ) s_j приписывается определенный уровень защиты $u(s_j), j \in U$, остающийся неизменным все время функционирования системы и сохранения статуса субъекта (его классификации и категории допуска), где $U = \{u_1,...,u_l,...,u_L\}, l = \overline{1,L}$ – множество уровней защиты. Каждый субъект определяется записью $(s_j, \lambda(s_j), \mu(s_j))$, где s_j – идентификатор СЗ, $\lambda(s_j)$ – классификация субъекта s_j, $\mu(s_j)$ – категория допуска субъекта s_j.

$O = \{o_1,...,o_i,...,o_I\}, i = \overline{1,I}$ – конечное множество объектов защиты, сгруппированное по типам $C(o_i) = \{c_q / q = \overline{1,Q}\}$, где Q – количество типов объектов защиты. Каждому объекту защиты (ОЗ) $o_i \in O$ присваивается уровень защиты $u(o_i)$, который соответствует уровню секретности информации $l_\varepsilon \in L$, хранящейся в объекте o_i (файл) или к которой обращается объект o_{ii} (программа). Каждый объект определяется записью следующего типа: $(o_i, s_j, \lambda(s_j), \lambda(o_i))$, где o_i – идентификатор объекта, s_j – идентификатор субъекта-владельца объекта o_i, $\lambda(s_j)$ – классификация субъекта, $\lambda(o_i)$ – степень секретности информации, хранящейся в объекте o_i.

Предлагаемая система мандатного контроля доступа реализована в виде монитора обработки запросов, который осуществляет идентификацию, аутентификацию и контроль доступа субъектов к выделенным типам объектов с одновременным управлением потоками информации различной степени секретности. Монитор построен таким образом, чтобы в течение всего времени функционирования информационно-вычислительной системы ни один пользователь не получил возможность осуществления недопустимых видов доступа к информации, первоначально имеющей несравнимый уровень секретности по отношению к уровню допуска пользователя и не имеющего разрешения на реализацию запрашиваемого вида доступа в данное время. При попытке несанкционированного доступа (НСД) к информационным ресурсам система реагирует на неавторизованных пользователей, на нарушения основных правил доступа и условий контроля доступа. Применение криптографических преобразований в информационных системах с мандатной политикой управления доступом является обязательным условием обработки информации различной степени секретности. Для электронных документов повышенной секретности должны быть предусмотрены процедуры криптопреобразований, криптостойкость которых должна быть не ниже установленных стандартом для хранения и передачи информации такой степени конфиденциальности [2]. Для субъектов с высокой категорией допуска $\mu(s_j)$ часть информации должна быть надежна зашифрована. В функции монитора по обработке, контролю и анализу запросов пользователей в качестве дополнительной системы включены процедуры, поддерживающие процессы шифрования и дешифрования информации на базе нетрадиционного подхода, позволяющего варьировать надежность криптоалгоритма в зависимости от уровня защиты $u(o_i)$.

В рассматриваемой методологии многоуровневой защиты использование криптографических средств (рис.1) реализуется в функции аутентификации субъектов (шифрование паролей и подтверждение их целостности при попытке несанкционированной модификации) и в функции безопасного функционирования БД (шифрование хранимой или передаваемой по открытым каналам связи информации высокой степени секретности). Предусмотрены процедуры генерации и рассылки ключей для выполнения перечисленных выше функций.

Криптостойкость выбираемых методов шифрования должна соответствовать уровню секретности информации. Технологически предпочтителен вариант, при котором выбор количества разных алгоритмов шифрования зависит от уровней секретности объектов защиты и способов обработки информации.

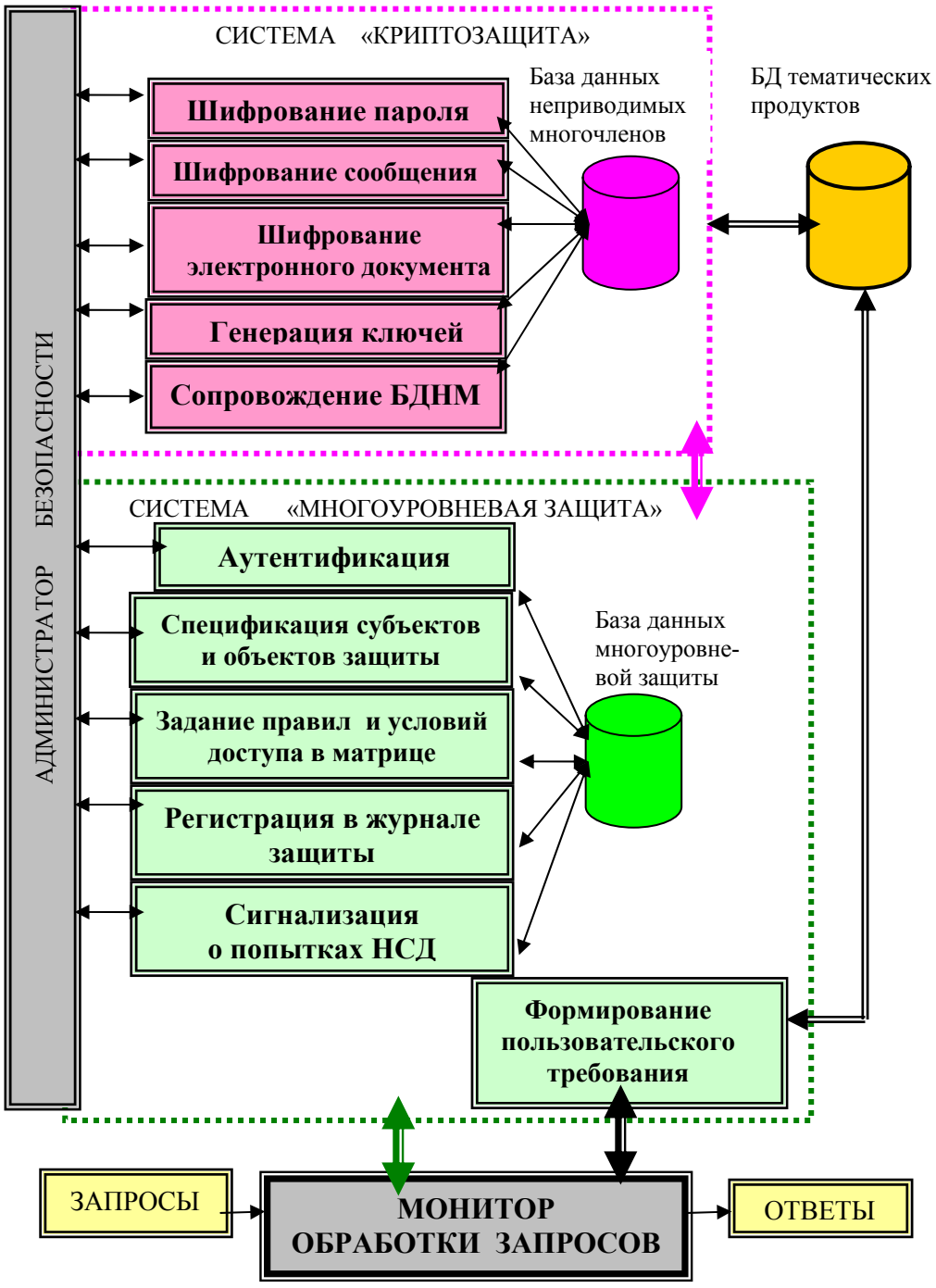

Рис 1. Использование криптографических преобразований в системах с мандатным разграничением доступа к информации

В табл. 1 приведены параметры шифрования СТРК 1073-2002 и криптостойкость P алгоритмов криптографической защиты, вычисленная как обратная величина вероятности вскрытия ключей, соответственно приведенным уровням безопасности:

$$P = \frac{1}{2^{l_{сим}}}.$$

Длина ключа является, безусловно, одним из показателей криптостойкости алгоритмов, но не самым лучшим. Известны работы показывающие, что из всех возможных подстановок, «хорошими» являются около 15%, т.е. при их использовании получаются удовлетворительные замешивания. Поэтому правильнее в качестве критерия использовать не длину ключа, а криптостойкость алгоритма.

Таблица 1

Отношение между уровнями безопасности и конфиденциальностью объектов защиты

Основные критерии криптографической защиты СТРК 1073-2002			Степень секретности информации $\lambda(o_i)$	Установленная криптостойкость P
Уровень безопасности	Вычислительная сложность алгоритма вскрытие криптографической защиты	Длина ключа симметричных алгоритмов $l_{сим}$		
1	$\geq 2^{48}$	$\leq$ 56 бит	ДСП	10^{-17}
2	$\geq 2^{96}$	$\leq$ 112 бит	Секретно	10^{-33}
3	$\geq 2^{128}$	$\leq$ 168 бит	Сов. секретно	10^{-50}
4	$\geq 2^{192}$	$\leq$ 256 бит	Особой важности	10^{-77}

Рассмотрим алгоритм нетрадиционного метода шифрования в непозиционной полиномиальной системе, в которой криптостойкость $P_{рас}$ зависит не только от длины ключа, но и от выбранной системы полиномиальных оснований, а также их распределения (порядка следования) [3]. Пусть $p_1(x), p_2(x), \ ..., p_n(x)$ неприводимые многочлены с двоичными коэффициентами, используемые в качестве основного (рабочего) диапазона. Тогда любой объект $o_i \in O$ может быть представлен в виде блочного сообщения M, где в качестве длины блока можно использовать наиболее распространенный пакет в 256 бит. Сообщение M длиной N бит можно интерпретировать как последовательность остатков $\alpha_1(x), \alpha_2(x),..., \alpha_n(x)$ от деления некоторого многочлена $F(x)$ на основания $p_1(x), p_2(x),..., p_n(x)$ соответственно.

Ключевую последовательность также длиной N можно интерпретировать как последовательность остатков $\beta_1(x, \beta_2(x),..., \beta_n(x)$ от деления некоторого

многочлена $G(x)$ по тем же основаниям системы. Тогда в качестве криптограммы $\omega_1(x),\omega_2(x),...,\omega_n(x)$ может рассматриваться некоторая функция $H(F(x),G(x))$, операции которой, в соответствии с операциями непозиционной системы счисления, выполняются параллельно по модулям полиномов, выбранных в качестве оснований системы. В этом случае полным ключом, кроме многочлена $G(x)$, является и конкретный набор оснований, выбранных из всего множества неприводимых многочленов степени не выше N. Криптостойкость такой системы будет определяться вероятностью определения оснований системы (порядка многочлена, их конкретный выбор и размещение), а также гаммы, используемой при шифровании:

$$P_{pac} = \frac{1}{2^{l_{сим}} \cdot C^{b_t}_{kol(m_\delta)} \cdot A^{b^*}},$$

где b_t – количество многочленов, покрывающих выбранную степень m_δ, $1 \le m_\delta \le N$; $kol(m_\delta)$- количество неприводимых многочленов, покрывающих систему оснований используемой степени m_δ; $kob(m_\delta)$ – количество бит, покрываемых неприводимыми многочленами; b^* – общее количество неприводимых многочленов различных степеней, которые можно выбрать в качестве оснований системы, запись вычетов по которым покрывает длину *N*:

$$b^* = \sum_{t=1}^{T} b_t, \forall m_\delta (\delta = \overline{1,\Delta}).$$

Поскольку с ростом порядка количество неприводимых многочленов с двоичными коэффициентами стремительно растет (табл. 2), очевиден широкий выбор решений уравнения. Экспериментальные расчеты показали [4], что предлагаемый алгоритм шифрации увеличивает криптостойкость P_{pac} до огромного числа при выборе оснований до 16-й степени включительно.

Таблица 2

Зависимость роста количества неприводимых многочленов от их степеней

m_δ	1	…	4	5	6	7	8	9	10	11	12	13	14	15	16
$kol(m_\delta)$	1	…	3	6	9	18	30	56	120	240	488	972	1938	3876	7749
$kob(m_\delta)$	1	…	12	30	54	126	240	504	1200	2640	5856	12636	27132	58140	123984

Если, например, N =*56* бит, то можно в качестве оснований выбрать неприводимые многочлены только 14-й степени. В этом случае число различных комбинаций есть C_{1938}^4, а так как в непозиционных системах существенен и порядок расположения оснований, общее число различных систем оснований в данном случае будет $C_{1938}^4 \times A_4^4$. Для N =*112* бит можно в качестве оснований выбрать неприводимые многочлены 10-й и 12-й степени. Соответственно получим:

$$P_{рас} = \frac{1}{2^{56} C_{1938}^4 A_4^4} \quad \text{и} \quad P_{рас} = \frac{1}{2^{112} C_{120}^{10} C_{488}^1 A_{11}^{11}}.$$

Для наиболее распространенной длины пакета в 256 байт=2048 бит можно, например, выбрать 80 многочленов 16-й степени, 60 многочленов 12-й степени и 6 многочленов 8-й степени, т.е. всего 146 многочленов.

В этом случае криптостойкость определяется выражением

$$P_{рас} = \frac{1}{2^{2048} C_{7749}^{80} C_{488}^{60} C_{30}^6 A_{146}^{146}},$$

что значительно меньше любой разумной величины, которая может быть задана в реальных условиях для системы шифрования. Приведенные в таблице 1 задаваемые значения криптостойкости P также покрываются различными вариантами $P_{рас}$ с использованием рассматриваемого алгоритма шифрации.

Шифрование объектов защиты. Процедура шифрования применяется к ОЗ, хранящимся в БД тематических продуктов в виде электронных документов или передаваемых по открытым каналам связи в виде сообщения. Уровень защиты объекта $u(o_i)$ должен соответствовать степени секретности информации $\lambda(o_i)$, хранящейся в нем, а надежность криптопреобразований должна быть не ниже установленных стандартом или требованиями заказчика $P_{зад}$ информации такой степени конфиденциальности. Алгоритм шифрования с заданной криптостойкостью строится на взаимосвязанном выполнении следующих процедур: выбора системы оснований, генерация гаммы с использованием генератора псевдослучайных чисел, выбора порядка следования оснований системы и самой шифрации сообщения. Для проведения итеративного выбора удовлетворительной $P_{рас}$ спроектирована база данных неприводимых многочленов (БДНМ), содержащая все неприводимые полиномы с двоичными коэффициентами различных степеней, которые можно выбрать в качестве оснований системы, запись вычетов по которым покрывает длину заданного сообщения *N*.

Аутентификация субъектов защиты. Аутентификации локальных, удаленных и доверенных абонентов (субъектов защиты) осуществляется через функцию подтверждения подлинности на основе пароля. Предусмотрен контроль качества назначаемых паролей (минимальное количество символов, различный класс символов и т.д.). Пароль хранится в зашифрованном виде в БД многоуровневой защиты, что существенно снижает риск его раскрытия. При аутентификации введенный

пользователем пароль также зашифровывается и сравнивается с хранящимся зашифрованным значением. Дважды неправильно ввод пароля – отказ в обслуживании и блокировка абонента, затем регистрация в журнале защиты попытки НСД.

Генерация ключей. Для каждого пользователя генерируются личные ключи – для его последующей аутентификации и для передачи (хранения) информации высокой степени секретности соответственно ее владельцу. Схема генерации и рассылки ключей может базироваться на одном из популярных протоколов ключевого соглашения при условии выполнения требуемой криптостойкости P. Генерация гаммы может осуществляться через реализацию алгоритмов формирования последовательности псевдослучайных чисел (например, ANSI X9.17), которых разработано достаточно много. Опубликованные в известных работах наборы псевдослучайных чисел не могут гарантировать надежность криптопреобразований $P_{зад}$. В дальнейшем планируется разработка оригинальных алгоритмов формирования последовательности псевдослучайных чисел.

Применение подобных схем криптопреобразований дает удовлетворительные характеристики надежности для сохранения конфиденциальности информации различной степени секретности при организации многоуровневого контроля доступа.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Горковенко Е.В.* Методология защиты при нормативном контроле доступа к информации. Управление защитой информации. – М.: ВНИИПВТИ. Том 11. 2007. №4. – С.427-432.

2. СТРК 1073-2002 «Средства криптографической защиты информации» // Общие технические требования. – Астана: Госстандарт РК, 2002.

3. *Бияшев Р.Г., Горковенко Е.В.* Шифраторы информации с заданной криптостойкостью. // Труды международной научно-практической конференции «Состояние, проблемы и задачи информатизации в Казахстане», КазНТУ им. К. Сатпаева. – Алматы, 2004. – С.27-37.

4. Анализ состава ключевой информации в соответствии с длиной шифруемого пакета // Раздел 1 промежуточного отчета «Разработка технологий по информационной безопасности (криптографическая защита информации на основе нетрадиционных подходов)», номер госрегистрации №0103РК00120, инвентарный номер №0204РК00016. – Алматы: ИПИУ, 2004. – С.14-25.

УДК 681.034

Д.П. Рублёв, В.М. Фёдоров, А.Б. Чумаченко, О.Б. Макаревич

УСТАНОВЛЕНИЕ АВТОРСКИХ ПРАВ ПО НЕОДНОРОДНОСТЯМ ЦИФРОВЫХ ОБРАЗОВ*

Одной из актуальных задач защиты информации является разработка методов защиты от копирования мультимедийных данных и как несанкционированного использования аппаратуры для их создания, так и производства контрафактной продукции. Это связано с массовым переходом на цифровые технологии получения, обработки, отображения и хранения мультимедиа информации. Благодаря этому практически полностью устранены изначально присущие аналоговым уст-

* Работа выполнена при поддержке грантов РФФИ №08-07-00253-а, № 08-07-00117а.