УДК 004.056.55

Альтернативные режимы шифрования данных в системах электронного документооборота

Пилькевич С.В., Глобин Ю.О.

В современных условиях постоянного увеличения интенсивности информационного взаимодействия, на первое место выходят проблемы создания автоматизированных систем, обеспечивающих всю совокупность управленческих процессов как в масштабах отдельно взятых организаций, так и государства в целом.

Создание подобных систем предполагает построение распределенной системы управления, реализующей решение полного спектра задач, связанных с управлением документами и процессами их обработки. Одну из основных ролей при этом играют системы электронного документооборота.

В свете выше изложенного необходимо отметить, что в РФ в рамках утвержденной в августе 2007 года Концепции «Электронное правительство» получила развитие Федеральная целевая программа «Электронная Россия». Реализация данной целевой программы также невозможна без создания систем электронного документооборота.

Электронный документооборот (ЭДО) - единый механизм по работе с документами, представленными в электронном виде, с реализацией концепции «безбумажного делопроизводства» [24].

ЭДО включает: создание документов, их обработку, передачу, хранение, вывод информации, циркулирующей на предприятии, посредством использования компьютерных сетей. Под управлением ЭДО в общем случае принято понимать организацию движения документов между подразделениями предприятия, группами пользователей или отдельными пользователями. При этом под движением документов подразумевается не их физическое перемещение, а передача прав на их применение с уведомлением конкретных пользователей и контролем за их исполнением.

Электронный документооборот обладает многочисленными достоинствами, состоящими в реализации следующих функций:

1) многокритериальный поиск документов;

2) контроль исполнения документов;

3) регистрация документов;

4) ввод резолюций к документам;

5) распределенная обработка документов в сети;

6) распределение прав доступа к различным документам и функциям системы;

7) ведение нескольких картотек документов;

8) работа с проектами документов;

9) распределение находящихся на исполнении документов по «папкам» в зависимости от стадии исполнения документа: поступившие, на исполнении, на контроле и другие;

10) формирование стандартных отчетов;

11) обмен документами по электронной почте;

12) списание документов в дело;

13) отслеживание перемещений бумажных оригиналов и копий документов, ведение реестров внутренней передачи документов;

14) ведение пользовательских списков должностных лиц, организаций, тематических рубрик, групп документов;

15) редактирование шаблонов выходных печатных форм[8, 23].

Введение электронного документооборота позволяет снизить количество служб, занятых работой с документами (курьеров, канцелярских работников и т. п.).

На рисунке 1 приведена диаграмма, иллюстрирующая перераспределение времени, затрачиваемого на различные этапы работы с документами при переходе от бумажного к электронному документообороту [7]. Необходимо отметить, что внедрение ЭДО позволяет существенно увеличить долю времени, отводимого непосредственно для работы над содержимым документа.

Отсутствие необходимости вручную размножать документы, отслеживать перемещение бумажных документов внутри организации, контролировать порядок передачи конфиденциальных сведений существеннейшим образом снижает трудозатраты делопроизводителей. Сквозной автоматический контроль исполнения на всех этапах работы с документами кардинально повышает качество работы исполнителей, делает сроки подготовки документов более прогнозируемыми и управляемыми.

Рисунок 1 – Время, затраченное на отдельные этапы работы с документами

Совместное использование систем электронного делопроизводства и хранилищ информации позволяет систематизировать и объединять информацию, что облегчает ее анализ и составление отчетов. Для поиска скрытых закономерностей в больших массивах данных можно применять более эффективные решения и действия, основанные на соответствующих технологиях извлечения информации из данных.

Перечисленные преимущества характерны только для систем управления, построенных на основе полностью электронного документооборота.

Министерство обороны РФ (МО РФ), следуя современным тенденциям развития информационных технологий, начало полномасштабно внедрять систему электронного документооборота (СЭДО) в своих подразделениях.

Под термином ***система электронного документооборота*** будем понимать автоматизированную многопользовательскую систему, сопровождающую процесс управления работой иерархической организации с целью обеспечения выполнения этой

организацией своих функций. При этом предполагается, что процесс управления опирается на человеко-читаемые документы, содержащие инструкции для сотрудников организации, необходимые к исполнению [21].

Специфика Вооруженных сил РФ предъявляет высокие требования по уровню защиты конфиденциальности и обеспечения аутентичности данных, циркулирующих в системах защищенного электронного документооборота в связи с чем, СЭДО МО РФ позволяет решать как общепринятые задачи, так и ряд специальных, обусловленных деятельностью МО РФ:

1) обеспечение единых методологических, организационных и информационно-технологических решений, объединяющих различные виды документов (открытого и ограниченного распространения) и различные группы пользователей;

2) автоматизация процессов делопроизводства и регламентов, принятых в органах военного управления (ОВУ) МО РФ;

3) обеспечение контролируемости процесса документооборота (создание, согласование, регистрация, рассмотрение, исполнение и т.д.);

4) организация и систематизация единого хранилища электронных документов;

5) поиск электронных документов по обязательным реквизитам и содержанию;

6) обеспечение юридической значимости документооборота;

7) исключение утери документов;

8) обеспечение разграничения доступа к документам;

9) создание и обеспечение требуемых характеристик и надежного функционирования подсистемы телекоммуникационного обмена информацией, инфраструктуры и механизмов гарантированной доставки сообщений;

10) построение и обеспечение требуемых характеристик и надежного функционирования системы удостоверяющих центров в области ЭЦП, подсистемы обеспечения информационной безопасности информационно-телекоммуникационной инфраструктуры;

11) подключение (при соблюдении требований и ограничений по обеспечению информационной безопасности) к СЭДО МО РФ всех объектов информатизации МО, в первую очередь, ОВУ Центрального аппарата [4].

В системе СЭДО МО РФ циркулирует и хранится информация ограниченного доступа. Значительную часть составляют секретные документы, несанкционированное ознакомление с которыми может причинить существенный ущерб безопасности РФ. Построенная в МО РФ СЭДО имеет подсистему безопасности, осуществляющую разграничение доступа к ресурсам и обеспечивающую целостность информации. К основным методами, реализующим функционал подсистемы безопасности СЭДО относятся криптографические методы защиты информации.

В связи с необходимостью получения соответствующих сертификатов Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности и МО криптографические алгоритмы, лежащие в основе программно-технических средств обеспечения безопасности информации, циркулирующей в СЭДО должны быть стандартизированы в РФ.

В настоящее время в РФ имеются следующие национальные криптографические стандарты:

– ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования»;

– ГОСТ Р 34.10-94 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»;

– ГОСТ Р 34.10-2001 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»;

– ГОСТ Р 34.11 «Информационная технология. Криптографическая защита информации. Функция хэширования».

В тоже время для разработчиков средств информационной безопасности общепринятым считается использование механизмов, соответствующих международным стандартам. Базовый набор подобных стандартизованных криптографических

механизмов разрабатывается и принимается в Международной организации по стандартизации ИСО (International Organization for Standardization, ISO) [6].

К основным международно признанным криптографическим механизмам относятся следующие группы стандартов ИСО:

1) криптографические протоколы;
2) аутентификация сообщений;
3) электронная цифровая подпись;
4) шифрование и режимы шифрования;
5) выработка параметров.

Из криптографических стандартов ИСО в России принят только один: ГОСТ Р ИСО/МЭК 10116 «Информационная технология. Режимы работы для алгоритма поразрядного блочного шифрования»[21]. Тем не менее, данный стандарт утратил свою актуальность [6]. Причины этого отчасти состоят в том, что ГОСТ Р ИСО/МЭК 10116 описывает всего четыре режима шифрования данных.

Таким образом, видится целесообразным рассмотреть рабочие документы и проекты стандартов перспективных режимов блочного шифрования данных, опубликованных NIST в [13, 27-32] с целью расширения функциональности алгоритма блочного шифрования данных ГОСТ 28147-89 и сфер его применения для СЭДО.

Традиционно под режимом шифрования понимают способ получения алгоритма зашифрования, исходя из базового блочного алгоритма зашифрования. Выбор режима шифрования имеет целью обеспечение определенных свойств алгоритма шифрования (ограничение распространения искажений, простота синхронизации и др.) [9].

Криптографический режим шифрования обычно объединяет базовый шифр, обратную связь и ряд простых операций, при этом стойкость криптографического преобразования базируется на стойкости используемого шифра, а не режима. Более того, режим не должен компрометировать стойкость используемого алгоритма [10].

С целью устранения отрицательных свойств процесса шифрования и в зависимости от отрасли применяют ряд базовых режимов блочного шифрования [27], которые стандартизированы NIST [5]:

− режим электронной кодовой книги Electronic Codebook (ECB);

− режим сцепления блоков зашифрованного текста Cipher Block Chaining (CBC);

− режим обратной связи по зашифрованному тексту Cipher Feedback (CFB);

− режим обратной связи по выходу Output Feedback (OFB);

− режим счетчика Counter Mode (CTR).

Дадим краткую характеристику каждого из перечисленных режимов.

Режим электронной кодовой книги

Каждый блок открытого текста заменяется блоком шифртекста (см. рисунок 2). В ГОСТ 28147-89 данный режим называется режимом простой замены

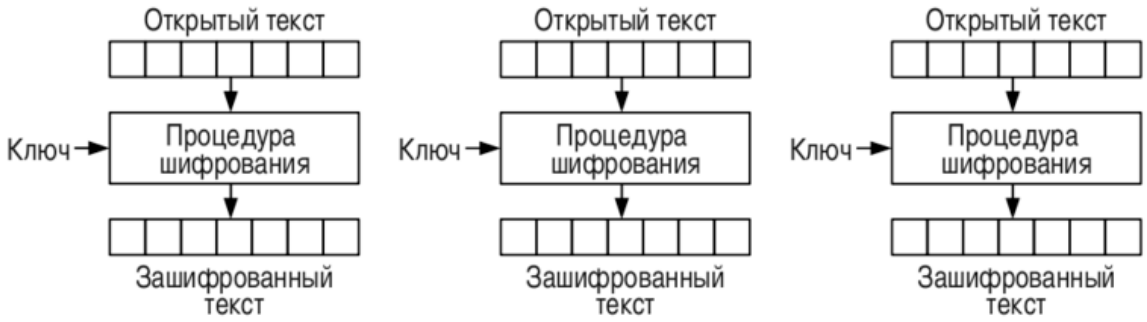

Рисунок 2 –Схема шифрования в режиме ECB

Основными преимуществами режима ECB являются возможность одновременно шифровать несколько блоков данных и поддержка самосинхронизации, т. е. повреждения *i*-го блока зашифрованного текста влияет только на тот же самый расшифрованный блок.

В качестве недостатков режима ECB необходимо отметить следующие:

− одинаковые блоки открытого текста обуславливают появление одинаковых блоков зашифрованного текста;

− перестановка блоков зашифрованного текста вызывает перестановку соответствующих блоков открытых текстов, что приводит к нарушению целостности информации;

− отсутствует возможность сокрытия структуры информации, подлежащей защите;

− уязвимость к атакам на основе пар известных текстов и зашифрованных текстов, и на основе парадокса дней рождения [20].

Режим сцепления блоков шифротекста

Каждый блок открытого текста (кроме первого) побитно складывается по модулю 2 (операция XOR) с предыдущим результатом шифрования (см. рисунок 3).

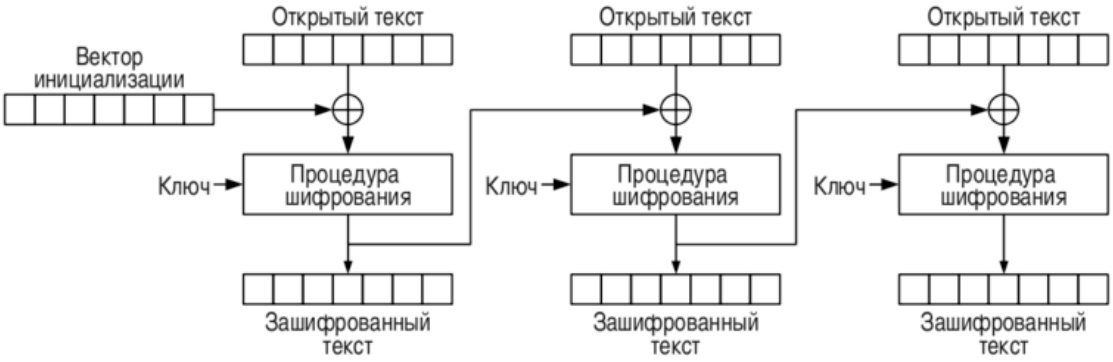

Рисунок 3 – Схема шифрования в режиме CBC

Отличительной особенностью режима CBC является то, что каждый блок зашифрованного текста зависит от всех блоков открытого текста, обработанных до него. Кроме того, чтобы сделать каждое сообщение уникальным, в первом блоке должен использоваться вектор инициализации [16].

Режим CBC позволяет распараллелить процесс расшифрования блоков зашифрованного текста и поддерживает самосинхронизацию. Если во время передачи или записи данных был поврежден текущий блок зашифрованного текста, то этот и следующий за ним блоки открытого текста будут повреждены при расшифровывании [15].

Одинаковые блоки открытого текста обуславливают появление разных блоков зашифрованного текста, что в свою очередь делает невозможным перестановку блоков зашифрованного текста для модификации содержания открытого текста в отличие от режима ECB. За счет этого режим шифрования CBC также используют в качестве средства для обеспечения целостности и защиты информации от фальсификации [5].

Основными недостатками данного режима являются:

– последовательный характер процедуры зашифрования;

– необходимость дополнения исходного текста сообщения до числа кратного размеру блока шифра.

В ряде случаев, используя атаку на основе парадокса дней рождения злоумышленник, обладая несколькими наборами зашифрованных текстов, может подменить целые группы блоков зашифрованных текстов [5].

Режим обратной связи по шифротексту

Для шифрования открытого текста в режиме обратной связи по шифротексту (или в режиме гаммирования с обратной связью) текущий блок складывается по модулю 2 с результатом шифрования предыдущего блока (см. рисунок 4).

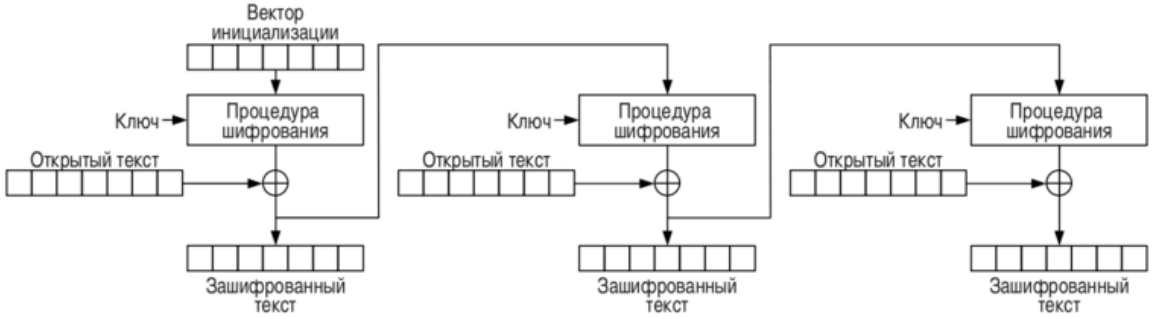

Рисунок 4 – Схема шифрования в режиме CFB

К положительным свойствам режима CFB относят возможность скрывать структуру открытого текста и поддержку самосинхронизации. Как и в режиме CBC процесс расшифрования поддерживает распараллеливание, а процесс зашифрования – нет, поскольку каждый следующий блок зашифрованного текста зависит от всех предыдущих блоков.

Режим CFB имеет тот же недостаток по отношению к атаке на основе парадокса дней рождения, что и режим CBC.

Режим обратной связи по выходу

Режим OFB переводит блочный алгоритм шифрования в синхронный потоковый шифр [20]. В процессе выработки блока шифртекста блок исходного текста складывается по модулю 2 с результатом зашифрования вектора инициализации (для первого блока) или выходом процедуры шифрования предыдущего блока (см. рисунок 5).

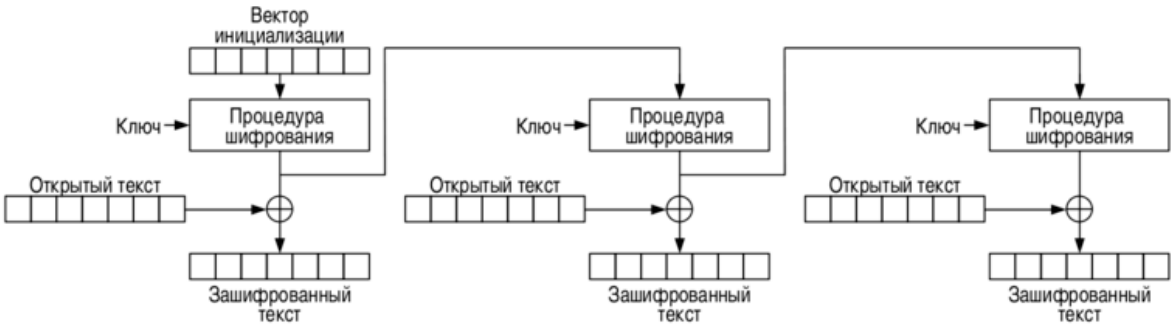

Рисунок 5 – Схема шифрования в режиме OFB

Каждая операция шифрования в режиме OFB зависит от всех предыдущих и поэтому не может быть выполнена параллельно. Однако, из-за того, что открытый текст используется только на финальной стадии раунда шифрования, операции блочного шифра могут быть выполнены заранее, позволяя осуществлять заключительное шифрование параллельно с открытым текстом [16].

Недостаток режима OFB в том, что он более уязвим к атакам модификации потока сообщений, чем CFB (инверсия бит в зашифрованном тексте приводит к соответствующей инверсии бит в открытом тексте) [19].

Режим Счетчика

Режим счетчика предполагает подачу на вход соответствующего алгоритма блочного шифрования значения счетчика, накопленного с момента старта. При увеличении значения счетчика, алгоритм блочного шифрования образует строку битов, которая используется в качестве ключа шифра Вернама, т.е. к ключу и блокам исходного сообщения применяются операции XOR [20].

Значения счетчика должны быть различны для всех итераций алгоритма в которых блочный шифр использует один и тот же ключ шифрования. Требование уникальности входных данных процедуры шифрования при фиксированном значении ключа выполняется при использовании генератора псевдослучайных последовательностей, но в этом случае необходим начальный вектор инициализации для генераторов со стороны отправителя и получателя сообщений. Режим шифрования CTR проиллюстрирован на рисунке 6 [15].

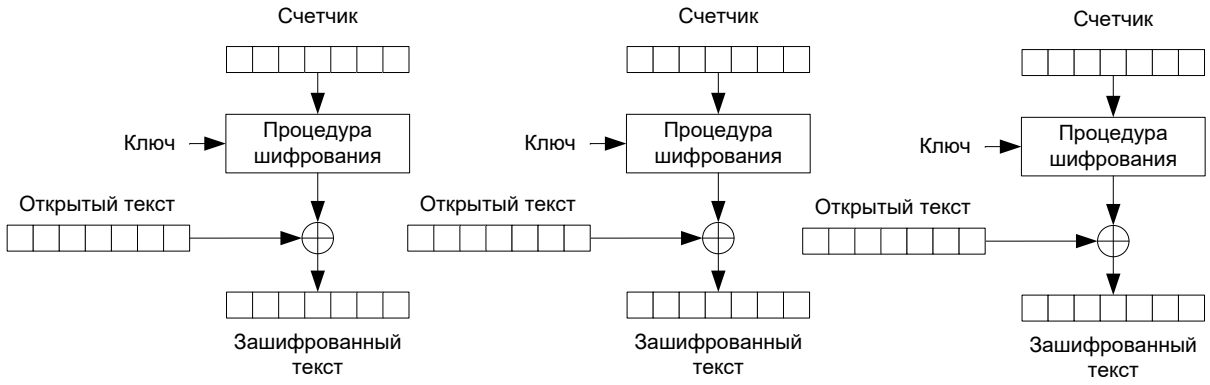

Рисунок 6 – Схема шифрования в режиме CTR

Режим CTR обладает всеми достоинствами режима ECB:

- параллельное исполнение;
- простота и возможность непосредственного за- и расшифрования любого блока сообщения по отдельности и независимо от других блоков.

Кроме того, режим CTR исправляет все недостатки шифрования в режиме электронной кодовой книги:

- одинаковые блоки открытого текста преобразовываются в различные блоки шифротекста;
- отпадает необходимость дополнения последнего блока шифротекста [15].

В настоящее время разрабатываются новые режимы шифрования, а на базе уже созданных продолжают совершенствоваться новые. При этом основными задачами, стоящими перед исследователями являются интеграция, в рамках применения блочного алгоритма, функций обеспечения конфиденциальности и аутентичности передаваемых данных, а также повышение скорости обработки информации за счет реализации возможности применения конвейерной обработки и распараллеливания выполнения операций зашифрования/расшифрования.

В частности, после принятия нового стандарта блочного шифрования данных AES в NIST было объявлено о потребности обновления классических режимов и возможности рассмотрения новых режимов шифрования.

На сегодняшний день NIST одобрены девять режимов, опубликованные в серии документов [26, 27, 31]. К ним относятся: шесть режимов обеспечения конфиденциальности (ECB, CBC, OFB, CFB, CTR и XTS-AES), один - аутентификации

(CMAC) [28] и два объединенных режима обеспечения конфиденциальности и установления подлинности (CCM и GCM) [29, 30].

Кроме того большой перечень режимов (см. таблицы 1-4 [17]) представлен NIST для рассмотрения и апробирования научной общественностью.

Таблица 1 – Альтернативные режимы шифрования, обеспечивающие конфиденциальность, целостность и подлинность сообщения

Режим	**Полное наименование режима**	**Авторы**
CCM	Counter with CBC-MAC	*R. Housley, D. Whiting, N. Ferguson*
CS	Cipher-State	*R. Schroeppel*
CWC	Carter Wegman (authentication) with Counter (encryption)	*T. Kohno, J. Viega, D. Whiting*
EAX	A Conventional Authenticated-Encryption Mode	*M. Bellare, P. Rogaway, D. Wagner*
GCM	Galois/Counter Mode	*D. McGrew, J. Viega*
IACBC	Integrity Aware Cipher Block Chaining	*C. Jutla*
IAPM	Integrity Aware Parallelizable Mode	*C. Jutla*
OCB	Offset Codebook	*P. Rogaway*
PCFB	Propagating Cipher Feedback	*H. Hellström*
SIV	Synthetic IV	*P. Rogaway, T. Shrimpton*
XCBC	eXtended Cipher Block Chaining Encryption	*V. Gligor, P. Donescu*
EAX'	EAX' (EAX-prime) Cipher Mode	*M. Burns, E. Beroset, A. Moise, T. Phinney*
RKC	Random Key Chaining (RKC)	*P. Kaushal, R. Sobti, G. Geetha*

Таблица 2 – Альтернативные режимы шифрования, обеспечивающие аутентификацию

Режим	**Полное наименование режима**	**Авторы**
OMAC	OMAC: One-Key CBC	*T. Iwata, K. Kurosawa*
PMAC	Parallelizable Message Authentication Code	*P. Rogaway*
RMAC	Randomized MAC	*E. Jaulmes, A. Joux, F. Valette*
TMAC	Two-Key CBC MAC	*K. Kurosawa, T. Iwata*
XCBC (MAC)	Extended Cipher Block Chaining MAC	*J. Black, P. Rogaway*
XECB (MAC)	eXtended Electronic Code Book MAC	*V. Gligor, P. Donescu*

Таблица 3 – Альтернативные режимы шифрования, обеспечивающие конфиденциальность

Режим	Полное наименование режима	Авторы
2DEM	2D-Encryption Mode	*A. A. Belal, M. A. Abdel-Gawad*
ABC	Accumulated Block Chaining	*L. Knudsen*
CTR	Counter Mode Encryption	*H. Lipmaa, P. Rogaway, D. Wagner*
FCEM	Format Controlling Encryption Mode	*U. Mattsson*
FFX	Format-preserving Feistel-based Encryption Mode	*M. Bellare, P. Rogaway, T. Spies*
IGE	Infinite Garble Extension	*V. Gligor, P. Donescu*
BPS	Format Preserving Encryption Proposal	*E. Brier, T. Peyrin, J. Stern*
VFPE	VISA Format Preserving Encryption	*VISA USA Inc., Attention John Sheets or Kim R. Wagner*
CSPEM	Character Set Preserving Encryption Mode	*Gary S. Sarasin*

Таблица 4 – Альтернативные режимы сцепления ключей и выработки хэш

Режим	Полное наименование режима	Авторы
KFB	Key Feedback Mode	*J. Håstad, M. Naslund*
AES-hash*	AES-hash	*B. Cohen*

* требует алгоритм Rijndael с размером блока 256 бит, а не 128 бит (в соответствии с AES).

Предварительный анализ публикаций, описывающих представленные режимы, показал, что в большинстве своем режимы ориентированы главным образом на использование алгоритмов TripleDES, AES (Rijndael) и Skipjack.

Таким образом, реализация режимов, представленных в таблицах 1-4, применительно к алгоритму ГОСТ 28147-89 представляется затруднительнгой. Изложенная ситуация требует поиска альтернативного пути построения режимов блочного шифрования. Такой подход существует и состоит в использовании различных ключей шифрования для каждого блока данных.

Любой симметричный блочный шифр описывается двумя главными составляющими: процедурой развертывания ключей и процедурой шифрования. Процедуру развертывания ключей используют для формирования набора подключей, которые в дальнейшем используют в процедуре шифрования. Процедура шифрования

выполняет непосредственное преобразование данных, т. е. зашифрование и расшифрование блоков данных.

Применительно к алгоритму ГОСТ 28147-89 необходимо отметить, что процедура развертывания ключей реализуется следующим образом. В соответствии со структурной схемой алгоритма ключевое запоминающее устройство (КЗУ) обладает емкостью 256 бит и состоит из восьми 32-разрядных накопителей $(X_0, X_1, X_2, ..., X_7)$. При записи ключа $(W_1, W_2, ..., W_{256})$, $W_i \in \{0,1\}$, $i = 1 \div 256$, в КЗУ значение W_1 вводится в 1-й разряд накопителя X_0, значение W_2 вводится во 2-й разряд накопителя X_0, ... , значение W_{32} вводится в 32-й разряд накопителя X_0; значение W_{33} вводится в 1-й разряд накопителя X_1, значение W_{34} вводится во 2-й разряд накопителя X_1, ... , значение W_{64} вводится в 32-й разряд накопителя X_1; значение W_{65} вводится в 1-й разряд накопителя X_2 и т.д., значение W_{256} вводится в 32-й разряд накопителя X_7 [2].

В [5] авторы предлагают в зависимости от функционального назначения процедуры развертывания ключей подразделять их на две группы.

Первую группу образуют процедуры развертывания ключей, которые формируют подключи для последовательностей блоков данных. Ко второй группе относятся процедуры развертывания ключей, которые формируют подключи для раундов шифрования одного блока данных и включают три основных этапа модификации ключа: начальный, главный и конечный.

Начальный этап модификации ключа предназначен для выполнения начальных преобразований над секретным ключом и формирования набора входных значений для этапа главной обработки ключа. На втором этапе из полученных данных формируют набор подключей для их дальнейшего использования на этапе конечной модификации.

На этапе конечной модификации ключа выполняют преобразование набора подключей в форму пригодную для их использования в процедуре шифрования.

Вышеуказанные этапы модификации ключа используют для получения набора подключей раундов шифрования первого блока данных $\{S\}_1$, который фактически является первым раундовым ключом секретного ключа шифрования K. В [5] Предлагаются следующие режимы сцепления блочных подключей.

1) ***Итеративный режим*** сцепления подключей. Для формирования набора подключей $\{S\}_i$ ($i=\overline{2,N}$, где N – количество наборов подключей) выполняют следующие преобразования

$$S_{1,i} = f_t\,(S_{k,i-1})\,,\; S_{j,i} = f_t\,(S_{j-1,i}),$$

где $S_{j,i}$ – j-ый m-битный подключ i-го блокового ключа, $j=\overline{1,k}$, k – количество подключей в наборе; f_t – функция произвольного отображения m-бит в m-бит, в случае исполнения операции шифрования t, $t=\{e, d\}$, e – операции зашифрования, d – операция расшифрования; m – разрядность подключей [5].

При выполнении данного режима для формирования первого набора подключей $\{S\}_1$ используют секретный ключ шифрования K. Для получения первого подключа i-го блочного ключа k-ый подключ (i-1)-го блокового ключа посылают на функцию f_t. Для формирования j-го подключа i-го блокового ключа (j-1)-ый подключ i-го блокового ключа посылают на функцию f_t и т. д. Схема данного режима приведена на рисунке 7.

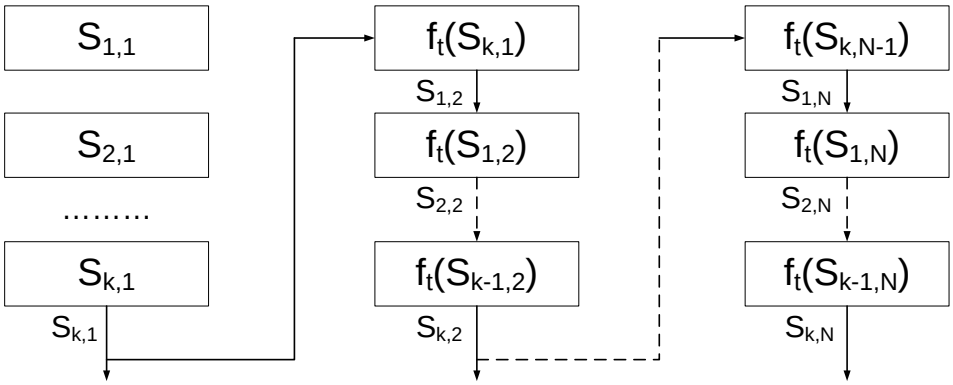

Рисунок 7 – Схема итеративного режима сцепления подключей

Для данного режима невозможно распараллелить процесс вычисления подключей, поскольку для вычисления j-го подключа используются значения (j-1)-го подключа и для вычисления i-го блокового ключа используют (i-1)-ый раундовый ключ.

2) ***Последовательный режим*** сцепления подключей используют для формирования набора подключей $\{S\}_i$ по следующему правилу

$$S_{j,i} = f_t\,(S_{j,i-1}).$$

Как и в предыдущем режиме для формирования первого блокового ключа $\{S\}_1$ используют секретный ключ шифрования K. В полученном наборе подключей $\{S\}_1$, каждый подключ независимо друг от друга поступает на функцию f_t, с выхода которой получают следующий раундовый ключ $\{S\}_2$ и т. д. Схема данного режима приведена на рисунке 8.

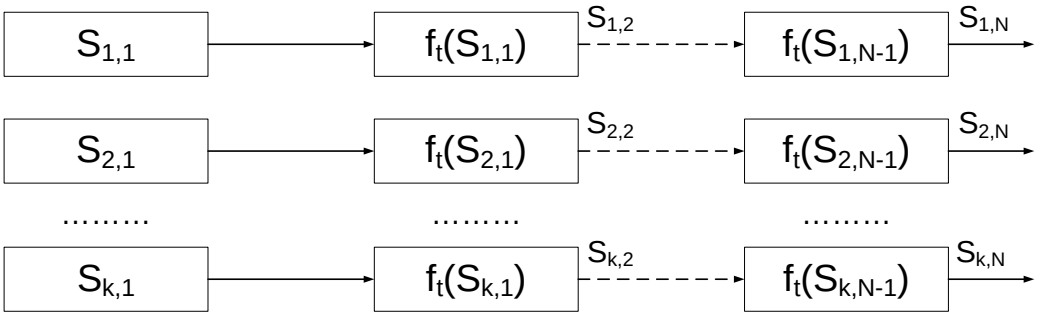

Рисунок 8 – Схема последовательного режима сцепления подключей

Поскольку j-ый и (j-1)-ый подключи i-го блокового ключа не связаны друг с другом, то для заданного режима можно организовать процесс параллельного вычисления значений подключей.

3) ***Комбинированный режим***. Данный режим заключается в одновременном использовании двух предыдущих режимов сцепления и описывается следующими выражениями

$$S_{1,i} = g_t(S_{k,i-1}, S_{1,i-1}) , \ S_{j,i} = g_t(S_{j-1,i}, S_{j,i-1}) , \qquad (*)$$

где g_t – функция произвольного отображения $2m$-бит в m-бит.

Таким образом, процесс получения второго блокового ключа состоит в выполнении нескольких шагов. Во-первых, на функцию g_t посылают первый $S_{1,i-1}$ и последний подключи $S_{k,i-1}$ $(i-1)$-го блокового ключа, для того, чтобы получить первый подключ i-го блокового ключа. Во-вторых, полученный подключ и второй подключ (i-1)-го блокового ключа принимают участие в формировании второго подключа $S_{2,i}$ второго блокового ключа, поступающих на функцию g_t. Для формирования j-го подключа i-го блокового ключа выполняют преобразование согласно формуле (*) Первый раундовый ключ вычисляют по правилам, которые задаются в процедуре развертывания ключа шифрования K. Схема данного режима приведена на рисунке 9.

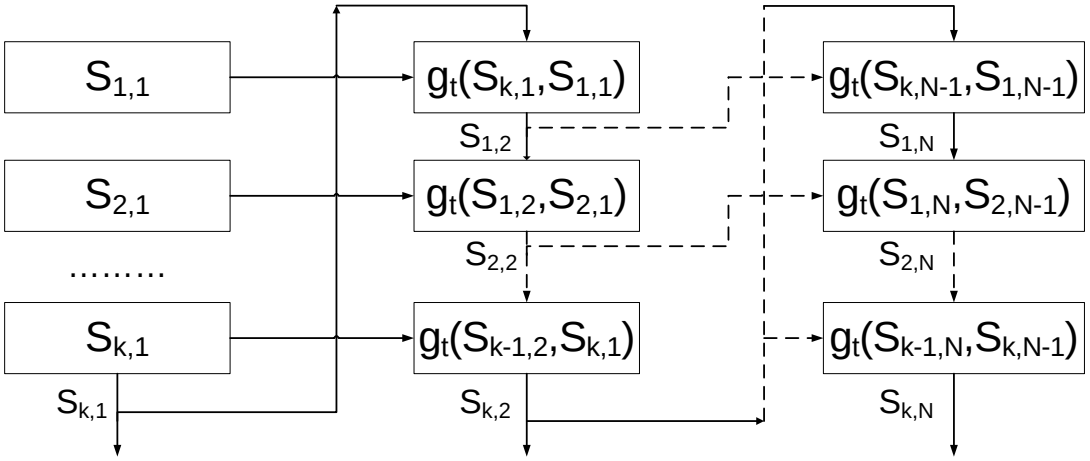

Рисунок 9 – Схема комбинированного режима сцепления подключей

Комбинированный режим не поддерживает процесс распараллеленного вычисления подключей для i-го блокового ключа, поскольку в формировании *j*-го подключа текущего блокового ключа участвует (*j*-1)-ый подключ этого же блокового ключа.

Ключи, сформированные в режиме сцепления ключей, обеспечивают следующие свойства:

− одинаковым блокам открытого текста соответствуют разные блоки зашифрованного текста;

− возможность скрывать структуру открытого текста;

− возможность определения факта нарушения целостности сообщения в случае перестановки блоков текста;

− процедура шифрования не требует векторов инициализации;

− возможность одновременного вычисления раундовых ключей и выполнения процесса шифрования блоков данных;

− отсутствие распространения ошибок (ошибка в одном блоке зашифрованного текста приводит к ошибочной расшифровке только этого блока).

Недостатком использования режима сцепления ключей является невозможность одновременно шифровать несколько блоков данных.

Также режимы сцепления ключей позволяют повысить устойчивость блокового шифрования к атаке, основанной на парадоксе дней рождения за счет использования раундовых ключей.

Предложенные в [5] режимы обеспечивают формирование собственных раундовых ключей для каждого блока данных, что повышает криптографическую стойкость процесса шифрования, сохраняя при этом большую часть преимуществ базовых режимов шифрования.

Таким образом, видится целесообразным с целью расширения функциональных возможностей и перечня решаемых задач, повышения криптографической стойкости, увеличения быстродействия и снижения ресурсоемкости выполняемых операций, включить в состав математического обеспечения подсистемы криптографической защиты информации СЭДО альтернативные режимы шифрования на базе алгоритма ГОСТ 28147-89, а также рассмотреть возможность модификации процедуры разворачивания раундовых подключей данного алгоритма.

Список литературы

1. Головашич С. А. Безопасность режимов блочного шифрования / С. А. Головашич // Радиотехника: Всеукр. межвед. научн.-техн. сб. – Х.: ХНУРЭ, 2001. – Вып. 119. – С. 135 – 145.

2. ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования

3. Дмитришин О. В. Режим керованого зчеплення блоків зашифрованого тексту / О. В. Дмитришин, В. А. Лужецький // Вісник ВПІ. – Вінниця, Видавництво Вінницького національного університету, 2009 – № 1. – С. 34 – 36.

4. Ефимов В.В. Организация электронного документооборота МО РФ. – СПб.: ВАС, 2011. Электронный ресурс.

5. *Лужецкий В.А., Дмитришин А.В.* Альтернативные режимы блокового шифрования // Научные труды ВНТУ, 2011, № 1

6. Лунин А. В. (Москва, ИнфоТеКС). Вопросы формирования набора российских криптографических стандартов // Труды Третьей Всероссийской конференции «Стандартизация информационных технологий и интероперабельность» 27 октября 2009 г. г. Москва, ВВЦ.

7. Печникова Т.В., Печникова А.В. Практика работы с документами в организации: учебное пособие.– М.: ЭМОС, 1999.– 208с.

8. Практика работы с документами в организации: учебное пособие/ Т.В. Печникова, А.В.Печникова. М.: ЭМОС, 1999. 208с.

9. Словарь криптографических терминов / Под ред. Б. А. Погорелова и В. Н. Сачкова. М.: МЦНМО, 2006. - 91 с.

10. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. - М.: Триумф, 2002. - 816 с.

11. Belal A. A. 2D-Encryption mode. / A. A. Belal, M. A. Abdel-Gawad // March, 2001. – P. 32. – Режим доступу до ресурсу: http://csrc.nist.gov/groups/ ST/toolkit/BCM/documents/proposedmodes/2dem/2dem-spec.pdf.

12. Bellare1 M. The FFX Mode of Operation for Format-Preserving Encryption. Draft 1.1. / M. Bellare1, Ph. Rogaway and T. Spies // February 20, 2010. – P. 18. – Режим доступу

до ресурсу: http://csrc.nist.gov/groups/ST/toolkit/BCM documents/proposedmodes/ffx/ffx-spec.pdf.

13. Brier E. BPS: a format-preserving encryption proposal / E. Brier, Th. Peyrin and J. Stern – P. 11. – Режим доступу до ресурсу: http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/bps/bps-spec.pdf.

14. Federal Information Processing Standards Publication 81 1980 Edition – DES MODES OF OPERATION // Computer Security Division Information Technology Laboratory National Institute of Standards and Technology, Gaithersburg, MD 20899-8930. December 1980.

15. http://citforum.ru/security/cryptography/rejim_shifrov/

16. http://cragen.narod.ru/bezo.htm

17. http://csrc.nist.gov/groups/ST/toolkit/BCM/index.html

18. http://en.academic.ru/dic.nsf/enwiki/1069304

19. http://ra32.ru/modules/news2/article.php?storyid=291

20. http://ru.wikipedia.org/

21. http://www.allgosts.info/standarts/gost-r-isomek-10116-93

22. http://www.documoborot.ru/

23. http://www.nbuv.gov.ua/e-journals/VNTU/2011_1/2011-1_ru.files/ru/11valobc_ru.pdf

24. http://www.wss-consulting.ru/workflow.php

25. Knudsen L. R. Block chaining modes of operation / L. R. Knudsen // Reports in informatics No 207, October 2000. – P. 16. – Режим доступу до ресурсу: http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/abc/abc-spec.pdf.

26. Lipmaa H. CTR-mode encryption / H. Lipmaa, Ph. Rogaway and D. Wagner // Submission of modes of operation, 2001. – P. 4. – Режим доступу до ресурсу: http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/ctr/ctr-spec.pdf.

27. NIST Special Publication 800-38A 2001 Edition – Recommendation for Block Cipher Modes of Operation. Methods and Techniques // Computer Security Division Information Technology Laboratory National Institute of Standards and Technology, Gaithersburg, MD 20899-8930. December 2001.

28. NIST Special Publication 800-38B 2005 Edition – Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication // Computer Security Division Information Technology Laboratory National Institute of Standards and Technology, Gaithersburg, MD 20899-8930. May 2005.

29. NIST Special Publication 800-38C 2004 Edition – Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality // Computer Security Division Information Technology Laboratory National Institute of Standards and Technology, Gaithersburg, MD 20899-8930. May 2004.

30. NIST Special Publication 800-38D 2007 Edition – Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC // Computer Security Division Information Technology Laboratory National Institute of Standards and Technology, Gaithersburg, MD 20899-8930. November 2007.

31. NIST Special Publication 800-38E 2010 Edition – Recommendation for Block Cipher Modes of Operation: XTS-AES Mode for Confidentiality on Storage Devices // Computer Security Division Information Technology Laboratory National Institute of Standards and Technology, Gaithersburg, MD 20899-8930. January 2010.

32. NIST Special Publication 800-38F 2011 Edition – Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping // Computer Security Division Information Technology Laboratory National Institute of Standards and Technology, Gaithersburg, MD 20899-8930. August 2011.