УДК 004.056.5

Н.К. Жердев[1], И.В. Пампуха[1], Г.Б. Жиров[1], Ю.И. Хлапонин[2]

[1] *Военный институт Киевского национального университета имени Т. Шевченка, Киев*
[2] *Национальный авиационный университет, Киев*

АЛГОРИТМ ШИФРОВАНИЯ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ УПРАВЛЯЕМОГО, СЛУЧАЙНОГО И НЕЛИНЕЙНОГО ЭЛЕМЕНТА ГЕНЕРАЦИИ КЛЮЧЕЙ

В статье рассматривается новый перспективный подход к построению криптографических алгоритмов шифрования (дешифрования) информации, которая передается в телекоммуникационных сетях. В основу разработанного алгоритма криптографического преобразования положена идея отказа от детерминированных ключей и перехода к ключам, которые генерируются случайным образом, при этом их длина должна быть равна длине сообщения. Такая схема получила название ленты однократного использования, при этом вероятность ее «взлома» практически равна нулю.

Ключевые слова: *информационная система, алгоритм, криптографическая защита, шифрование, криптоанализ, ключ.*

Постановка проблемы в общем виде и анализ литературы

При повсеместном использовании современных телекоммуникационных систем, вопросы безопасности и защиты информации от несанкционированного доступа выходят на первый план.

Лавинообразное распространение компьютерных систем и их взаимодействие в сетях создало большую зависимость пользователей от компьютерных вирусов, хакеров, электронного подслушивания, мошенничества и т.д. Защита пересылаемой по сети и хранящейся в таких системах информации, стала одной из важнейших проблем современности.

Современные устройства защиты информации используемые в телекоммуникационных сетях могут быть реализованы с помощью традиционных алгоритмов криптографического преобразования и алгоритмов криптографического преобразования с открытым ключом [1].

Традиционные алгоритмы предполагают генерацию, распределение, хранение ключей и передача их абонентам, при этом круг лиц, которым они известны расширяется – это то обстоятельство, которое может привести к их разглашению. Кроме того, современные средства шифрования информации, использующие данные алгоритмы, являются "детерминированными" (заведомо известна структура алгоритма преобразования США – DES, ГОСТ-28147-89 и пр.). При современном уровне вычислительных средств, информация зашифрованная этими способами, может быть дешифрована за относительно короткое время.

Алгоритмы с открытым ключом требует использования мощных вычислительных средств. Например, для работы устройства при шифровании/дешифровании в реальном масштабе времени необходим 512-ти разрядный спецвычислитель. Исходя из этого, существующие алгоритмы шифрования с открытым ключом в настоящее время ограничиваются областями управления ключами и приложениями цифровой подписи.

Таким образом, возникает задача разработки алгоритма криптографического преобразования информации со случайными ключами на новых перспективных подходах, у которого недостатки существующих алгоритмов были бы исключены.

В основу разработанного алгоритма криптографического преобразования со случайными ключами положена идея Вернама, в которой он предложил отказаться от детерминированных ключей, а генерировать ключ случайным образом, при этом длина ключа должна быть равна длине сообщения. Такая схема получила название ленты однократного использования (или схемы с одноразовым блокнотом). В результате применения данной схемы на выходе получается случайная последовательность, не имеющая статистической взаимосвязи с открытым текстом. Таким образом, в данном случае, шифрованный текст не дает никакой информации об открытом тексте, и следовательно нет способа взломать ключ.

Сложность практического применения этого алгоритма заключается в том, что и отправитель и получатель должны иметь один и тот же случайный ключ. Поэтому, несмотря на преимущества способа Вернама по сравнению с другими способами, выполненными на электронных устройствах, на практике его реализовать сложно и весьма дорого. Основная трудность состоит в том, что генераторы случайных чисел на передающей и приемной сторонах должны работать синхронно и синфазно.

Авторам разработанного алгоритма удалось обеспечить синхронную и синфазную работу генераторов случайных чисел на передающей и приемной сторонах, при этом отправитель и получатель имеют один и тот же случайный ключ. Таким образом, в предложенном алгоритме реализована схема Джозефа Моборна на электронных устройствах. В алгоритме используются как симметричные случайные так и личные ключи. Математически доказано, что определить их практически невозможно. Использование данных ключей и хеш-функций позволяет решать ряд дополнительных задач, а именно: защита сетей и терминалов от несанкционированного доступа, аутентификация, электронная подпись и др. При этом ключи специально не генерируются, никому не назначаются и не распределяются, а автоматически формируются случайными генераторами, которые работают синхронно и синфазно на передающей и приемной сторонах. Это обстоятельство позволяет свести к минимуму влияние человеческого фактора при защите информации.

Алгоритм АСК-59140А-06 предназначен для криптографического преобразования цифровой информации в телекоммуникационных сетях. Он может быть реализован как программно, так и программно-аппаратно, а также удовлетворяет криптографическим требованиям, и по своим возможностям может быть использован для защиты конфиденциальной информации.

1. Пример использования АСК-59140А-06 при передаче данных в телефонных сетях

Принцип работы алгоритма рассмотрим на простом примере защиты сетей и терминалов от несанкционированного доступа для двух абонентов реализованного в устройстве ПЗМТ-1.

1.1. Структурная схема реализации АСК-59140А-06 для двух абонентов при обмене с использованием COM – порта (аналогично могут использоваться и другие виды портов USB, LPT и т.д.) представлена на рис. 1. Открытые (незашифрованные) данные (ОД) с выхода ЭВМ поступают на устройство ПЗМТ-1, где шифруются, и уже «закрытые» данные (ЗД) поступают на модем, в котором преобразуются и подаются в линию связи. По линии связи зашифрованные данные через АТС и др. элементы поступают на модем приемной части. С выхода модема ЗД подаются на ПЗМТ-1, где дешифруются и передаются на ЭВМ потребителя.

Исходя из структурной схемы видно, что ПЗМТ-1 включен в сеть последовательно с ЭВМ, и соответственно выполняет функцию фильтра информации. Если эта информация не соответствует ключу, то она разрушается на выходе ПЗМТ-1. Таким образом, устройство защищает не только информацию в сети, но и ЭВМ, как от атак вирусов, так и от несанкционированного доступа к ней через данную сеть.

1.2. Структурная схема организации обмена между абонентами приведена на рис. 2. На этапе производства, при программировании устройства ПЗМТ-1, память которого надежно защищена от несанкционированного доступа, абонентам попарно присваиваются личные и случайные ключи. Например, для абонентов A_1 и A_2 присваивается ключ $K_{12} = K$. Для сети (рис. 2), принцип построения ключей приведен в табл. 1.

Криптографическое преобразование в алгоритме АСК-59140А-06 осуществляется поблочно, размер которого составляет 128 бит.

2. Структурная схема алгоритма криптографического преобразования (криптосхема) при шифровании ОД

Структурная схема алгоритма (рис. 3) состоит из трех блоков:

а) подалгоритма формирования ключей;

б) подалгоритма шифрования ОД;

в) генератора случайных чисел (ГСЧ) с равномерным распределением 0 и 1 на выходе блоков, (при преобразованиях используется блок размерностью 16 байт).

2.1. Схема подалгоритма формирования ключей, рис. 3, содержит следующие структурные элементы: управляемый, случайный и нелинейный элемент; постоянное запоминающее устройство; оперативное запоминающее устройство микроконтроллера; перепрограммируемое запоминающее устройство. Рассмотрим их более детально.

Управляемый, случайный и нелинейный элемент (УСНЭ-1) – Γ_1, имеет два входа и два выхода. На его 1-й вход параллельным кодом поступает ключ управления режимами – $K_у$, в качестве которого используются ключи $K_н \oplus K_с$, где $K_н$ – начальный ключ, а $K_с$ – сеансовый ключ (при первом включении $K_с = \text{const}$), или ключ блока – $K_{бл.}$, или ключ пакета – $K_{пак.}$. На 2-й вход поступает либо const, либо случайная информация (СИ) либо ОД либо хеш-функция (ХФ).

С выхода 3 УСНЭ-1 снимается хеш-функция – ХФ, которая рассчитывается автоматически и позволяет автоматически в совокупности с индивидуальными ключами осуществлять цифровую подпись, аутентификацию и т.д.

Примечание: особенностью данной ХФ является то, что при искажении хотя бы одного бита передаваемой информации она изменяет свое значение. При существующих способах формирования хеш-функций могут возникать случаи, когда при измене-

нии определенных бит информации, хеш-функция не изменяет своего значения. Поэтому она не может использоваться для синхронного и синфазного управления случайными генераторами.

Рис 1. Структурная схема включения ПЗМТ-1 в сеть обмена между абонентами

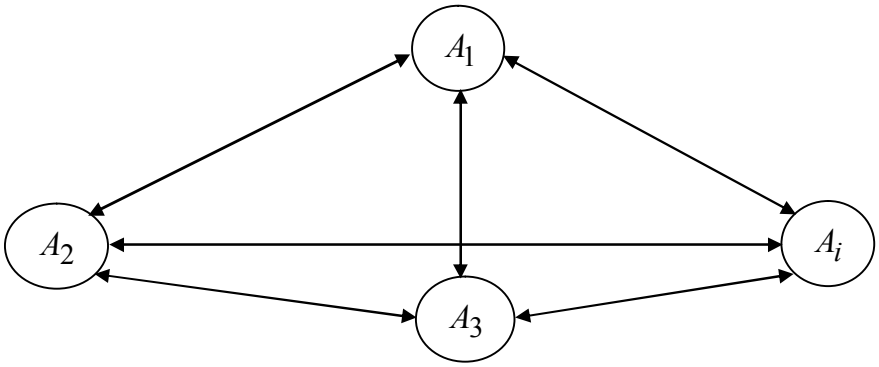

Рис. 2. Структурная схема организации обмена между абонентами

Таблица 1

Принцип построения ключей для сети

A_i / A_j	A_1	A_2	A_3	…	A_j
A_1		K_{12}	K_{13}	…	K_{1j}
A_2	K_{21}		K_{23}	…	K_{2j}
A_3	K_{31}	K_{32}		…	K_{3j}
…	…	…	…		…
A_i	K_{i1}	K_{i2}	K_{i3}	…	

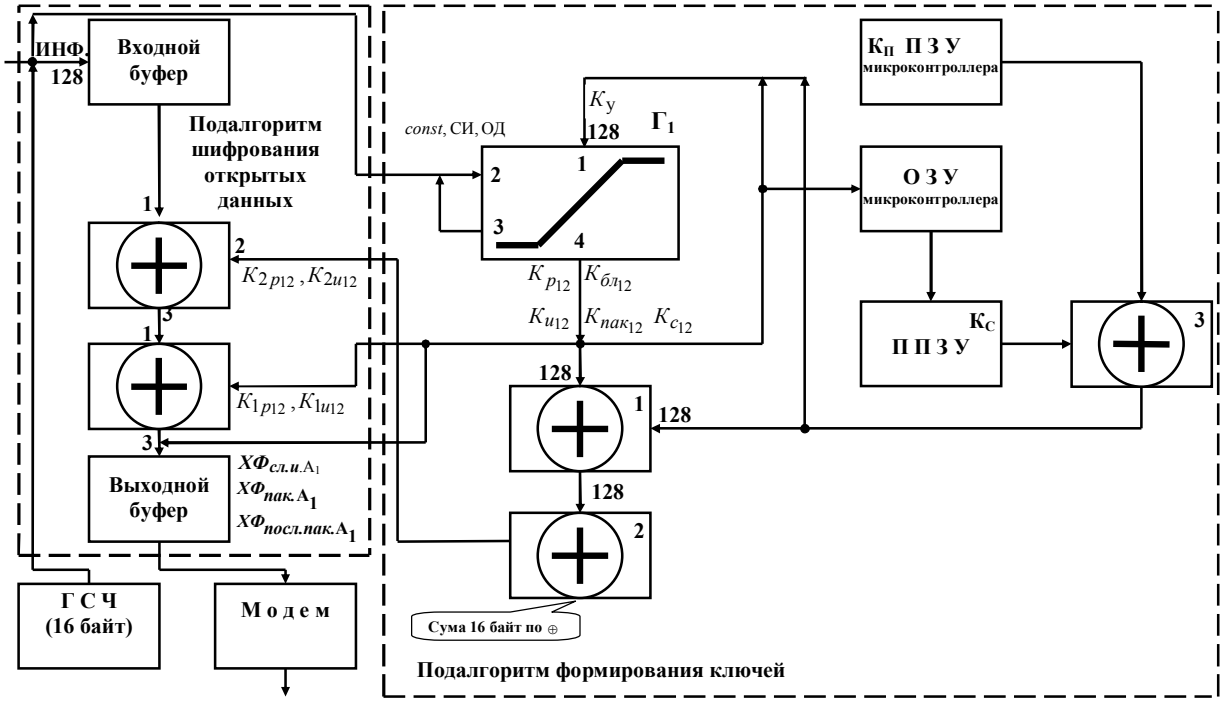

Рис. 3. Структурная схема алгоритма криптографического преобразования с использованием случайных ключей (АСК-59140А-06)при зашифровании открытых данных

С выхода 4 УСНЭ-1 снимаются случайные – исходный $К_и$, или рабочий $К_р$, или сеансовый $К_с$, или пакетный $К_{пак.}$ ключи с равновероятным распределением 0 и 1. Эти ключи являются исходными для формирования ключей $К_{1k}$ (где k – это $К_{1и}$, или $К_{1р}$, или $К_{1\,бл.}$, или $К_{1пак.}$, или $К_{1с}$) и $К_{2k}$ (где k – это $К_{2и}$, или $К_{2р}$, или $К_{2\,бл.}$, или $К_{2пак.}$, или $К_{2с}$). Ключ $К_1$ поступает в подалгоритм зашифрования ОД и является исходным для формирования ключа $К_2$.

Конструктивно элемент $Г_1$ может быть выполнен программно, аппаратно или программно-аппаратно.

Постоянное запоминающее устройство (ПЗУ), в частности ПЗУ микроконтроллера, в которое для каждого абонента записываются два столбца из табл. 1. Например, для абонента $А_2$ столбцы $А_i/А_j$ и $А_2$ – табл. 2.

Оперативное запоминающее устройство (ОЗУ) микроконтроллера.

Перепрограммируемое запоминающее устройство (ППЗУ). В подалгоритме формирования ключей с помощью ППЗУ за счет изменения $К_с$ изменяется структура подалгоритма формирования ключей.

Сумматор по модулю два №1, осуществляет операцию суммирования по модулю два: $К_и (К_р, К_{\,бл.}, К_{пак.}) \oplus (К_н \oplus К_с)$.

Сумматор по модулю два № 2, осуществляет побайтовую операцию суммирования по модулю два 16-ти байт с выхода первого элемента. При этом получается результирующий байт СВ, который используется для управления сдвигом влево ключа $К_2$.

Сумматор по модулю два №3 выполняет операцию суммирования по модулю два для ключей $К_н \oplus К_с$.

Таблица 2

ПЗУ для абонента $А_2$

$А_i/А_j$	$А_2$	$А_i/А_j$	$А_2$
$А_1$	$К_{12}$	$А_4$	$К_{42}$
$А_2$		...	...
$А_3$	$К_{32}$	$А_i$	$К_{i2}$

2.2. Схема подалгоритма зашифрования ОД содержит: входной и выходной буферы на 128 бит каждый; сумматоры по модулю два, в которых осуществляется сдвиг на i-разрядов влево в зависимости от ключа $К_{2k}$, суммирование значения $К_{1k}$ с информацией с выхода предыдущего сумматора [4–7].

3. Структурная схема алгоритма криптографического преобразования при расшифровании ЗД

Структурная схема алгоритма, (рис. 4) состоит из двух частей:

а) подалгоритма расшифрования ЗД;

б) подалгоритма формирования ключей.

3.1. Структурная схема подалгоритма формирования ключей содержит (рис. 3) те же элементы, что и структурная схема подалгоритма формирования ключей структурной схемы алгоритма криптографического преобразования при зашифровании ОД.

3.2. Структурная схема подалгоритма расшифрования ЗД рис. 4 содержит все те же элементы, что и структурная схема подалгоритма зашифрования ОД, при этом сумматоры по модулю два включены в зеркальном отображении относительно подалгоритма зашифрования ОД, а также дополнительно введены два новых элемента: «Сравнения» и «Регистратор».

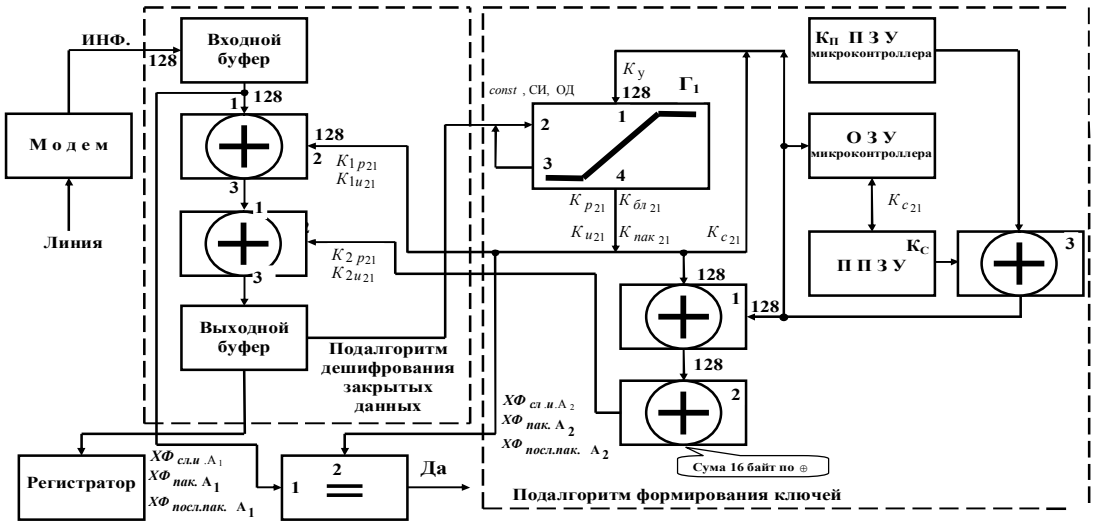

Рис. 4. Структурная схема алгоритма криптографического преобразования с использованием случайных ключей (АСК-59140А-06)при расшифровании открытых данных

Криптографический алгоритм с использованием случайных ключей имеет три режима работы: режим максимального быстродействия; режим среднего быстродействия; режим минимального быстродействия [4 – 7].

4. Режим максимального быстродействия

Шифрование / дешифрование ОД / ЗД в режиме максимального быстродействия проводится, если ключ управления режимами определяется выражением $K_у = K_н \oplus K_с$. Принцип работы алгоритма рассмотрим на примере передачи информации от абонента A_1 к абоненту A_2, т.о. абонент A_1 проводит шифрование ОД, а A_2 – расшифрование ЗД.

При первоначальном включении, алгоритм устанавливается в исходное состояние, при этом:

– на открытом ключе устанавливается связь $A_1 \leftrightarrow A_2$;

– если связь установлена, то абонент A_2 выдает квитанцию абоненту A_1 о готовности к работе. Абонент A_1, используя табл. 3, в соответствии набранному телефонному номеру, запоминает открытый номер абонента (например № телефона 1582051 соответствует открытый номер – 0002) и по этому номеру из табл. 4 считывает в программу закрытый ключ $K_{н_{12}} = K_{\ 21}$ (например 111...10). Кроме этого он выдает свой открытый номер (0001) абоненту A_2. В свою очередь, абонент A_2 из табл. 5, соответственно принятому открытому номеру считывает в программу закрытый ключ $K_{н_{12}} = K_{\ 21}$ (например 111...10).

Таблица 3

Открытые номера абонентов

№ телефона	Открытый номер абонента
4339077	0001
1582051	0002
.....	.....
4832051	4095
4852051	4096

Таблица 4

Закрытее ключи для абонента A_1

Открытый номер абонента	Закрытый ключ (16 байт)
0001	
0002	111...10
.....	.....
4095	011...00
4096	101...11

Таблица 5

Закрытее ключи для абонента A_2

Открытый номер абонента	Закрытый ключ (16 байт)
0001	111...10
0002	
.....	.....
4095	011...00
4096	101...11

В результате этого, абонентами A_1 и A_2 на элементы $Г_1$ подаются ключи

$$K_{н_{12}} \oplus K_{с_{12}} = K_{н_{21}} \oplus K_{с_{21}},$$

а так как при первом включении $K_{с_{12}} = K_{с_{21}}$ =const то на вход 1, в виде параллельного кода, поступают ключи управления режимами

$$K_у = K_{н_{12}} \oplus \text{const} = K_{н_{21}} \oplus \text{const};$$

– с ПЗУ на вход 2 элемента $Г_1$ подается const в качестве СИ для установки его в исходное состояние;

– с выхода 4 элемента $Г_1$ снимается ключ $K_и = K_{1и_{12}}$. Также, ключ $K_и$ используется для формирования второго исходного ключа $K_{2и_{12}}$, который поступает на один из самматоров подалгоритма шифрования цифровой информации.

Аналогично формируются ключи подалгоритмом формирования ключей алгоритма криптографического преобразования при расшифровании ЗД.

Таким образом, у абонентов A_1 и A_2 устанавливаются исходные ключи с равновероятным распределением ключей, которые в виде гаммы-шифра подаются на подалгоритм шифрования (дешифрования) ОД (ЗД).

Процедура шифрования ОД происходит следующим образом:

Генератор случайных чисел (рис.3.) формирует 128 битный последовательный код, который поступает на входной буфер и элемент $Г_1$ (вход 2) подалгоритма формирования ключей.

С выхода «Входного буфера» случайная информация параллельным кодом поступает на 1-й вход сумматора по модулю 2. На 2-й его вход подается ключ $K_{2и_{12}}$. С выхода данного элемента информация подается на второй сумматор (вход 1), а на вход 2 параллельным кодом ключ – $K_{1и_{12}}$. С выхода сумматора, зашифрованная случайная информация через «Выходной буфер» подается на модем и далее в линию.

Кроме того, случайная информация с ГСЧ подается последовательным кодом на вход 2 элемента $Г_1$, а на его 1-й вход продолжает поступать ключ $K_{н_{12}}$. Ключ $K_р$ считывается в буфер элемента $Г_1$. С его 3-го выхода считывается хеш-функция случайной информации, которая подается последовательным кодом на вход 2 элемента $Г_1$ и проходит все те же операции, что и случайная информация. С выхода 4 хеш-функция $ХФ_{сл.и.A_1}$ поступает на вход «Выходного буфера», модем и далее линию связи. Таким образом, процесс шифрования ОД завершен.

Процедура расшифрования ОД происходит следующим образом:

Зашифрованная случайная информация из модема через «Входной буфер» поступает на вход 1

сумматора по модулю два, а на вход 2 этого же элемента подается параллельным кодом ключ $К_{1и_{21}}$. С сумматора информация, в виде параллельного кода, поступает на вход второго сумматора, а на 2-й его вход которого подается ключ – $К_{2и_{21}}$.

Расшифрованная информация снимается с 3-го выхода второго сумматора по модулю два и подается в «Выходной буфер», с которого далее, в виде последовательного кода, поступает на вход 2 элемента $Г_1$ подалгоритма формирования ключей и «Регистратор».

Принцип формирования рабочих ключей такой же, как и у абонента $А_1$: формируются случайные рабочие ключи $К_{1р_{21}} = К_{1р_{12}}$ и $К_{2р_{21}} = К_{2р_{12}}$ с равновероятным распределением ключей, которые впоследствии будут использованы для расшифрования первого блока закрытых данных.

Хеш-функция СИ считывается с 3-го выхода элемента $Г_1$, и подается на вход 2 элемента сравнения.

На «Входной буфер» абонента $А_2$, кроме случайной информации, с модема поступает хеш-функция – $ХФ_{сл.и.А_1}$, которая далее подается на 1-й вход элемента сравнения. В элементе сравнения сравниваются хеш-функции $ХФ_{сл.и.А_1}$ и $ХФ_{сл.и.А_2}$, в случае если:

– $ХФ_{сл.и.А_1} \neq ХФ_{сл.и.А_2}$, то абонентом $А_2$ видаётся квитанция для повторной установки ключей $К_{1р_{21}} = К_{1р_{12}}$ и $К_{2р_{21}} = К_{2р_{12}}$;

– $ХФ_{сл.и.А_1} = ХФ_{сл.и.А_2}$, то абонентом $А_2$ видаётся квитанция о том, что случайные рабочие ключи равны, то есть $К_{1р_{21}} = К_{1р_{12}}$, $К_{2р_{21}} = К_{2р_{12}}$. Эти ключи подаются на подалгоритм зашифрования (расшифрования) открытых (закрытых) данных и абоненты готовы к обмену информацией.

Обмен информацией между абонентами $А_1$ *и* $А_2$.

Обмен информацией проводится пакетами, которые состоят из блоков по 128 бит. Шифрование / расшифрование блока ОД (ЗД) осуществляется таким же образом, как шифрование / расшифрование случайной информации при установке случайных рабочих ключей $К_{р_{21}} = К_{р_{12}}$. При этом формируются новые случайные рабочие ключи $К'_{1р_{21}} = К'_{1р_{12}}$ и $К'_{2р_{21}} = К'_{2р_{12}}$, а хеш-функция блока в алгоритме не используется.

Следующий блок ОД шифруется уже на новых случайных, рабочих ключах $К'_{1р_{21}} = К'_{1р_{12}}$ и $К'_{2р_{21}} = К'_{2р_{12}}$. Аналогичным образом последовательно передаются все блоки пакета информации. В конце пакета осуществляется проверка правильности передачи информации по хеш-функции пакета абонентов ($ХФ_{пак.\ А_1}$ и $ХФ_{пак.\ А_2}$), если:

– $ХФ_{пак.\ А_1} \neq ХФ_{пак.\ А_2}$, то абонент $А_2$ выдает квитанцию для повторной передачи пакета, при этом снова устанавливаются ключи

$$К''_{1р_{21}} = К''_{1р_{12}} \text{ и } К''_{2р_{21}} = К''_{2р_{12}};$$

– $ХФ_{пак.А_1} = ХФ_{пак.А_2}$, то абонент $А_2$ выдает квитанцию о том, что пакет принят правильно, новый случайный ключ $К_р$ устанавливается по случайной информации, и абонент $А_2$ готов к приему следующего пакета.

По окончании сеанса проверяется правильность установления ключа сеанса

$$К_{1р_{21\ посл.пак.}} = К_{1р_{12\ посл.пак.}} = К_{с_{12}} = К_{с_{21}}$$

по хеш-функции последнего пакета ($ХФ_{посл.пак.А_1}$ и $ХФ_{посл.пак.А_2}$).

5. Режим среднего быстродействия

Шифрование / расшифрование ОД (ЗД) в режиме среднего быстродействия проводится, когда $К_у = К_{пак.}$.

Процесс обработки информации в режиме среднего быстродействия такой же, как и в режиме максимального быстродействия.

6. Режим минимального быстродействия

Шифрование/расшифрование ОД (ЗД) в режиме минимального быстродействия проводится, когда $К_у = К_{бл}$.

Процесс обработки информации в режиме минимального быстродействия такой же, как и в режиме максимального быстродействия.

При реализации алгоритма АСК – 59140А – 06 ключи никому не назначаются и не распределяются. Это обстоятельство разрешает дополнительно обеспечить надежную защиту информации и сократить силы и средства, которые выделяются в других системах для обеспечения конфиденциальности.

7. Краткий криптоанализ алгоритма АСК – 59140А – 06

Уравнение шифрования:

$$\vec{b}_i = (\vec{a}_i \rightarrow \vec{И}_i) \oplus \vec{К}_{1i},$$

где: $\vec{b}_i$ – исходный вектор с 128 бит при i-м ключе; $\vec{К}_i$ – i-й вектор ключа, который изменяется с изменением каждого блока ОД (128 бит); $\vec{И}_i$ – i-й вектор

процедуры сдвига в зависимости от вектора i-го ключа (7 бит); $\vec{a}_i$ – i-и вектор ОД (128 бит).

Уравнение расшифрования ЗД является обратным процессом шифрования ОД:

$$\vec{a}_i = (\vec{b}_i \oplus \vec{K}_{1i}) \leftarrow \vec{И}_i.$$

Выводы

Таким образом, разработанный и предложенный алгоритм криптографического преобразования обладает следующими характеристиками:

1. Ключи симметричные. Формируются случайным образом, никому не назначаются и не распределяются, являются личными, случайными и единственными на множестве 2^n (где n – число разрядов в обрабатываемом блоке) в процессе обмена информацией между двумя абонентами. При этом их длинна соизмерима с длинной передаваемых сообщений.

2. При реализации алгоритма обеспечивается:

– автоматический контроль обмена информацией между абонентами;

– высокая степень криптографической защиты информации с эквивалентной длиной ключа $K = n \times 2^{3n}$ на один блок информации;

– высокая надежность передачи информации, так как она косвенно попакетно сравнивается на приемной и передающей сторонах с помощью хеш-функции;

При этом разработанный алгоритм может быть применен в таких областях, как: телефонные сети и объектов, спутниковые системы связи, системы охранной сигнализации, системы спутниковой охраны и наблюдения за объектами, защита банковских счетов и операций в банкоматах, защита информации на электронных носителях, защита глобальной сети интернет, защита корпоративных сетей путем анализа входного потока информации.

Список литературы

1. Столлингс В. Криптография и защита сетей: принципы и практика / В. Столлингс.– М.: Вильямс 2001. – 672 с.

2. Ленков С.В. Методы и средства защиты информации / Ленков С.В., Перегудов Д.А., Хорошко В.А. – К.: Арий, 2008. – Т. I. Несанкционированное получение информации. – 464 с.

3. Грайворонський М.В. Безпека інформаційно-комунікаційних систем / М.В. Грайворонський, О.М. Новіков. – К.: Видавнича група BHV, 2009. – 608 с.

4. Пат.88455 Украина, Спосіб зашифрування-розшифрування цифрової інформації з використанням керованого, випадкового, нелінійного і адаптивного елемента / заявник та патентовласник Всеукр. наук.-дослідн. ін-т зв'язку; заявл. 26.10.09.

5. Пат. 59140A, Україна, МПК[7] G 06 F 9/22, G 06 F 11/30. Ймовірносно-детермінований спосіб кодування цифрової інформації Жердєва-Пампухи / Жердєв М.К. (Україна), Пампуха І.В. (Україна); заявник та патентовласник Всеукр. наук.-дослідн. ін-т зв'язку. – № 2003021619; заявл. 24.02.03 ; опубл. 15.08.03, Бюл. № 8.

6. Пат. 2606, Україна, МПК[7] G 06 F 9/22, G 06 F 11/30. Спосіб шифрування цифрової інформації з відкритим ключем Жердєва-Пампухи / Жердєв М.К. (Україна), Пампуха І.В. (Україна); заявник та патентовласник Всеукр. наук.–дослідн. ін-т зв'язку. – № 2004010662; заявл. 29.01.04 ; опубл. 15.06.04, Бюл. № 6.

7. Пат. 5504, Україна, МПК[7] G 06 F 9/22, G 06 F 11/30. Спосіб шифрування цифрової інформації з відкритим ключем Жердєва-Галстяна-Пампухи / Жердєв М.К. (Україна), Пампуха І.В. (Україна) Галстян А.Р. (Україна); заявник та патентовласник Всеукр. наук.–дослідн. ін-т зв'язку. – № 20040604986; заявл. 23.06.04 ; опубл. 15.03.05, Бюл. № 3.

Поступила в редколлегию 23.03.2015

Рецензент: д-р техн. наук, проф. А.А. Смирнова, Кировоградский национальный технический университет, Кировоград.

АЛГОРИТМ ШИФРУВАННЯ ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ КЕРОВАНОГО, ВИПАДКОВОГО І НЕЛІНІЙНОГО ЕЛЕМЕНТУ ГЕНЕРАЦІЇ КЛЮЧІВ

М.К. Жердєв, І.В. Пампуха, Г.Б. Жиров, Ю.І. Хлапонін

У статті розглядається новий перспективний підхід до побудови криптографічних алгоритмів шифрування (дешифрування) інформації, яка передається в телекомунікаційних мережах. В основу розробленого алгоритму криптографічного перетворення покладена ідея відмови від детермінованих ключів і переходу до ключів, які генеруються випадковим чином, при цьому їх довжина повинна дорівнювати довжині повідомлення. Така схема отримала назву стрічки одноразового використання, при цьому ймовірність її «злому» практично дорівнює нулю.

Ключові слова: *інформаційна система, алгоритм, криптографічний захист, шифрування, криптоаналіз, ключ.*

INFORMATION ENCRYPTION ALGORITHM USING A CONTROL, RANDOM AND NON-LINEAR ELEMENT OF KEY GENERATION

N.K. Zherdev, I.V. Pampukha, G.B. Zhirov, Y.I. Khlaponin

The article discusses a new prospective approach to the construction of cryptographic algorithms of encryption (decryption) of the information that is transmitted in telecommunication networks. The basis of the developed algorithm of cryptographic transformation is the idea of non-deterministic keys and go to the keys that are generated randomly, and their length should be equal to the length of the message. This scheme is called the tape of a single use, the probability of its «hacking» is almost zero.

Keywords*: information system, algorithm, cryptographic protection, encryption, cryptanalysis, key.*