УДК 621.391.2

А.Д. Синюк, И.Б. Саенко

ПРОТОКОЛ ФОРМИРОВАНИЯ СЕТЕВОГО КЛЮЧА ПО ОТКРЫТЫМ КАНАЛАМ СВЯЗИ С ОШИБКАМИ

Синюк А.Д., Саенко И.Б. **Протокол формирования сетевого ключа по открытым каналам связи с ошибками.**

Аннотация. В статье предлагается протокол формирования сетевого ключа по открытым каналам связи с ошибками. Дана постановка задачи формирования сетевого ключа. Предлагается включить в протокол три временные фазы. Первая фаза устанавливает криптосвязность в независимых группах объектов связи (ОС). Вторая фаза устанавливает криптосвязность между независимыми группами ОС. Третья фаза выбирает сетевой ключ из множества сформированных ключей и передает его всем ОС сети. Рассматривается протокол формирования сетевого ключа. Предлагаются модель канальной связности и процедуры этого протокола. Выполняется оптимизация параметров протокола и обсуждается его эффективность.

Ключевые слова: открытый канал связи без ошибок, сетевой ключ, энтропия Шеннона, ключевые последовательности, модель канальной связности.

Sinjuk A.D., Saenko I.B. **Network key formation protocol on open communication channels with errors.**

The summary. The article proposes a network key formation protocol on open communication channels with errors. The task formulation of forming a network key is done. It is proposed that the protocol include three time phases. The first phase establishes crypto connection in independent groups of communication objects (CO). The second phase establishes crypto connection between independent groups of CO. The third phase selects the network key from the set of generated keys, and transmits it over the network. The protocol of the network key formation is discussed. A model of a channel connection with the procedures of this protocol is proposed. The parameters of the protocol are optimized, and its effectiveness is discussed.

Keywords: an open communication channel without error, the network key, Shannon entropy, key sequence, model of channel connectivity.

1. Введение. В современных телекоммуникационных системах особенно важны вопросы защиты информации при ее передаче по открытым каналам связи. Одна из важнейших задач в этой области, настоятельно требующая своего решения, — разработка протокола формирования сетевого ключа (СК) по открытым каналам связи с ошибками.

Постановка данной задачи заключается в следующем. Пусть W объектов связи сети связаны между собой множеством открытых каналов связи с ошибками и каждый из них имеет аппаратуру шифрования, реализующую единый в сети алгоритм шифрования. Необходимо разработать способ формирования СК для W объектов связи (ОС) сети за

минимальное время, осуществляя обмен данными конечной длины между ними по каналам сети, доступным нарушителю E. Требуется обеспечить формирование СК с высокой достоверностью для ОС и обеспечить формирование СК с малой вероятностью совпадения с ключом E. Предполагается, что нарушитель пассивен [1].

Предлагается включить в способ три временные фазы:

1) установления криптосвязности (получения единого ключа) в Ng независимых группах ОС, причем Ng групп ОС охватывают все W объектов связи сети;

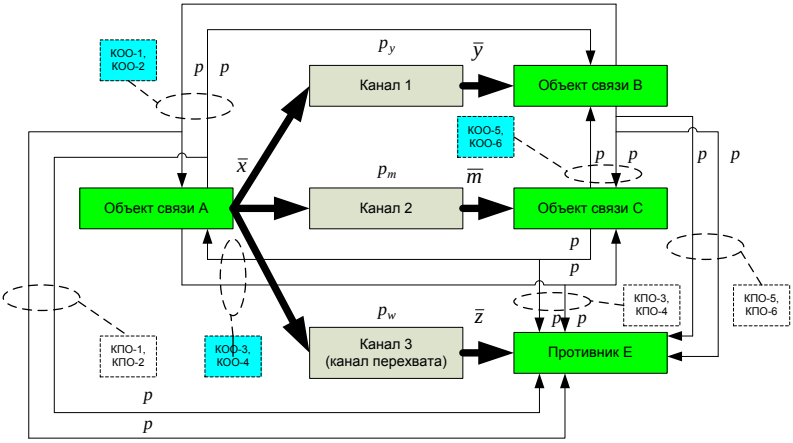
2) установления криптосвязности между Ng независимыми группами ОС, т.е. формирование единого ключа в каждой из Ng смежных групп ОС, причем в каждую смежную группу ОС включаются по одному ОС из двух-трех независимых групп ОС первой фазы;

3) выбора СК из множества сформированных ключей и передача его всем ОС сети.

В качестве СК выбирается ключ одной из групп первой или второй фазы. Передача СК начинается одновременно всеми ОС группы СК и осуществляется по каналам связи, закрытым с помощью групповых ключей, полученных на предыдущих фазах.

2. Протокол формирования группового ключа первой и второй фаз. Необходимо синтезировать протокол формирования группового ключа (ПФГК) трех объектов связи A, C и B, осуществляя обмен данными конечной длины между ними по каналам, доступным нарушителю E. При этом требуется обеспечить формирование группового ключа (K) с высокой достоверностью для объектов связи и обеспечить формирование группового ключа (ГК) с малой вероятностью совпадения с ключом E. ОС (санкционированных участников информационного обмена), нарушителя, связанных каналами связи, можно представить моделью канальной связности (МКС) ОС A, C и B и нарушителя E (см. рисунок).

Предположим, что каналы МКС описываются моделями двоичных симметричных каналов связи без памяти (ДСК). Канал 1 — это канал связи с ошибками в направлении от A к B, описывается моделью ДСК с вероятностью ошибки p_y, а канал 2 — это канал связи с ошибками в направлении от A к C, полагается ДСК с вероятностью ошибки p_m. Совокупность каналов 1 и 2 описывается моделью двоичного широковещательного канала без памяти (ДвШКБП) [2].



Модель канальной связности.

Передача сигналов по ДвШКБП определяется составляющими каналами 1 и 2 с алфавитами входным X, выходными Y и M и матрицами переходных вероятностей:

$$P_1 = \{p(y/x)\},\ P_2 = \{p(m/x)\},\ x \in X,\ y \in Y, m \in M.$$

На вход ДвШКБП ОС A подается последовательность $\bar{x} \in X^N$, где X^N — декартова N-я степень множества X. ОС B принимает на выходе канала 1 (КС-1) последовательность $\bar{y} \in Y^N$. ОС C принимает на выходе канала 2 (КС-2) последовательность $\bar{m} \in M^N$. Канал связи с ошибками в направлении от ОС A к E называется каналом перехвата (КП), который описывается моделью ДСК с вероятностью ошибки p_w с алфавитами входным X и выходным Z и матрицей переходных вероятностей $P_3 = \{p(z/x)\}, x \in X, z \in Z$. Нарушитель E принимает на выходе КП последовательность $\bar{z} \in Z^N$. В МКС также имеются каналы, которые позволяют сформировать между ОС группу каналов решающей обратной связи (РОС) [3]. Канал РОС от A к B назовем каналом открытого обсуждения 1 (КОО-1), соответственно от B к A — КОО-2, от A к C — КОО-3, от C к A — КОО-4, от B к C — КОО-5), канал РОС от C к B — КОО-6. Нарушитель контролирует каждый из КОО соот-

ветствующим каналом перехвата обсуждения (КПО). КОО и КПО описываются моделью ДСК с вероятностью ошибки $p = 0$. КС-1, КС-2, КОО и КПО являются независимыми каналами.

Протокол формирования K в МКС можно условно разделить на три последовательных этапа:

1) формирование «виртуальных» ДвШКБП и КП — генерирование начальных данных (НД) ОС A последовательности $\overline{x}$ и получение НД ОС B и C последовательностей $\overline{y}$ и $\overline{m}$ длиной N' бит на выходах КС-1 и КС-2 как исходного материала для формирования K. Нарушитель получает по КП свою версию НД — $\overline{z}$, которая называется начальными данными нарушителя (НДН);

2) обеспечение формирования K с высокой достоверностью путем устранения (исправления) ошибок, которые происходят при передаче последовательности по составляющим каналам ДвШКБП с ошибками. Исправление производится ОС B и C относительно НД ОС A при использовании дополнительной информации. Она передается от A к B и C по КОО. Предполагается, что нарушитель перехватывает ее по КПО и использует для устранения ошибок в НДН. В результате ОС формируют ключевые последовательности (КлП;

3) обеспечение формирования группового K с малой вероятностью совпадения с ключом нарушителя E путем сжатия тождественных КлП ОС. Предполагается, что E знает точное описание действий, выполняемых ОС, и для получения K нарушитель производит оптимальную обработку доступной информации известными методами обработки.

Для решения задач первого этапа разработан *простейший протокол*, или *Примитив*, который определяет совокупность действий, выполняемых ОС в заданной последовательности. Примитив реализуется следующим образом:

1) ОС A выбирает двоичный информационный символ (ИС) x с равномерным законом распределения вероятностей;

2) ОС A с использованием кода с повторениями (n, 1) формирует из x кодовое слово (КС) путем повторения данного символа n раз и запоминания этой последовательности в качестве КС x_n;

3) ОС A подает x_n на вход ДвШКБП (и КП) и передает;

4) ОС *B* принимает последовательность принятого слова (ПС) y_n, ОС *C* получает ПС m_n, *E* получает ПС z_n;

5) ОС *B* предварительно принимает y_n, если все его символы «1» или «0», и выносит решение о предварительном приеме y_n. В противном случае ОС *B* выносит решение о стирании y_n. Решение передается по КОО-2 к *A* и по КОО-5 к *C*. ОС *C* предварительно принимает m_n, если все его символы «1» или «0» и выносит решение о предварительном приеме m_n. В противном случае *C* стирает m_n. Решение передается по КОО-4 к *A* и по КОО-6 к *B*;

6) ОС *A* сохраняет ИС *x*, которому соответствует КС x_n, если на выходе КОО-2 от *B* получено предварительное решение о приеме y_n и на выходе КОО-4 получено предварительное решение о приеме m_n. В противном случае *A* стирает *x*. ОС *B* выносит решение об ИС *y*, соответствующем ПС y_n, путем выделения первого символа из y_n и сохраняет *y*, если *B* предварительно принял y_n и на выходе КОО-6 получено предварительное решение о приеме m_n. В противном случае *B* стирает y_n. ОС *C* выносит решение об ИС *m*, соответствующем m_n, путем выделения первого символа из m_n и сохраняет *m*, если *C* предварительно принял m_n и на выходе КОО-5 получено предварительное решение о приеме y_n. В противном случае ОС *C* стирает m_n.

Утверждение. Пусть ОС используют *Примитив*. Тогда для «виртуальных» ДвШКБП и КП вероятности ошибок составляющих каналов «виртуального» ДвШКБП равны

$$\tilde{p}_y = \frac{p_y^n}{p_y^n + \left(1 - p_y\right)^n}, \quad \tilde{p}_m = \frac{p_m^n}{p_m^n + \left(1 - p_m\right)^n}, \tag{1}$$

а вероятность ошибки «виртуального» КП равна

$$\tilde{p}_w = \sum_{i=\left\lfloor \frac{n}{2} \right\rfloor}^{n} C_n^i \beta(i,n)\, p_w{}^i (1 - p_w)^{n-i}, \tag{2}$$

где $\beta(i,n) = 0{,}5,$ если $i = n/2$, è $\beta(i,n) = 1$ в ином случае.

Доказательство. Код с повторениями содержит два КС: первое состоит из n символов «0», а второе — из n символов «1». Шаг 1 Примитива определяет, что КС равновероятны. После передачи A КС x_n B принимает y_n с вероятностью

$$P_B = p_y^n + \left(1 - p_y\right)^n . \tag{3}$$

Объект C принимает m_n с вероятностью

$$P_C = p_m^n + \left(1 - p_m\right)^n . \tag{4}$$

Совместная вероятность P_{ac} событий того, что A сохраняет x, B сохраняет y, C сохраняет m, равна

$$\begin{aligned} P_{ac} = P_B P_C = \left(p_y^n + \left(1 - p_y\right)^n \right)\left(p_m^n + \left(1 - p_m\right)^n \right) = \\ = p_y^n p_m^n + p_y^n \left(1 - p_m\right)^n + \left(1 - p_y\right)^n p_m^n + \left(1 - p_y\right)^n \left(1 - p_m\right)^n . \end{aligned} \tag{5}$$

Условная вероятность события несовпадения сохраненного ОС A ИС x с сохраненным ОС B ИС y при условии, что ОС сохранили свои ИС, равна

$$\tilde{p}_y = \frac{p(x_n \neq y_n, ac)}{P_{ac}} = \frac{p_y^n P_C}{P_{ac}} = \frac{p_y^n}{p_y^n + \left(1 - p_y\right)^n} . \tag{6}$$

Условная вероятность события несовпадения сохраненного ОС A x с сохраненным ОС C символом m при условии, что ОС сохранили ИС, равна

$$\tilde{p}_m = \frac{p(x_n \neq m_n, ac)}{P_{ac}} = \frac{p_m^n P_B}{P_{ac}} = \frac{p_m^n}{p_m^n + \left(1 - p_m\right)^n} . \tag{7}$$

Опишем ситуацию у нарушителя E. На шаге 4 *Примитива E* принимает на выходе КП z_n. Решения B и C, передаваемые по КОО-2, КОО-5, КОО-4, КОО-6, перехватываются по КПО на шаге 5. E также может удалять символы, которые были стерты ОС. Однако соответствующие символы, сохраняемые E, не достаточно надежны, так как составляющие каналы ДвШКБП и КП независимы. Использование ОС КОО в ходе выполнения примитива эквивалентно построению системы передачи информации с решающей обратной связью (РОС) [3, 4].

Известно, что код $(n,1)$ характеризуется расстоянием Хемминга d, равным n. В этом случае ОС обнаруживают ошибки кратности $d-1$ и отбрасывают неуверенно принятые ПС. КПО не выполняют для E роли каналов РОС. Поэтому нарушитель не может обнаруживать, а вынужден исправлять ошибки кратности $(d-1)/2$. Равномерное распределение вероятностей КС определяет для нарушителя оптимальное правило — мажоритарное правило, которое соответствует правилу декодирования по критерию максимума правдоподобия [3, 4], позволяющее исправить ошибки кратности не более $\lceil (d-1)/2 \rceil$, где скобки $\lceil\ \rceil$ — операция округления до наименьшего целого числа. Рассмотрим случай, когда n — четное число, и нарушитель принял ПС с равным числом «1» и «0». В половине случаев нарушитель примет правильное решение, в другой половине — неправильное. Тогда в общем случае $\tilde{p}_w$ равна

$$\tilde{p}_w = \sum_{i=\left\lfloor \frac{n}{2} \right\rfloor}^{n} C_n^i \beta(i,n)\, p_w{}^i (1-p_w)^{n-i} . \qquad (8)$$

где скобки $\lfloor\ \rfloor$ — операция округления до наибольшего целого числа; $\beta(i,n) = 0{,}5,$ если $i = n/2$, è $\beta(i,n) = 1$ в ином случае.

Утверждение доказано.

Процедура исправления ошибок «виртуальных» составляющих каналов ДвШКБП может быть реализована с использованием метода *помехоустойчивого кодирования* [4]. Для этого A с помощью некоторого конструктивного линейного кода, параметры которого предварительно открыто распределены, находит проверочные символы к НД $\bar{x}'$ длиной N', полученным после реализации задач первого этапа. Объект A посылает проверочные символы к B и C по КОО-1 и КОО-3, соответственно. Объекты B и C исправляют ошибки в НД $\bar{y}'$ и $\bar{m}'$ соответственно, используя проверочные символы и конструктивный алгоритм декодирования выбранного кода. Число символов проверки НД r может быть определено с использованием границы Варшамова—Гильберта для минимального расстояния Хемминга d кода $(N'+r, N')$ [4]:

$$\frac{r}{N'+r} \geq h\left(\frac{d-2}{N'+r-1}\right). \quad (9)$$

Вероятность ошибочного декодирования НД объектом B определяется из формулы

$$P_{AB} = \sum_{i=\left\lfloor \frac{d-1}{2} \right\rfloor+1}^{N'} C_{N'}^{i} \tilde{p}_y^{i} (1-\tilde{p}_y)^{N'-i}. \quad (10)$$

Вероятность ошибочного декодирования НД для объекта C равна

$$P_{AC} = \sum_{i=\left\lfloor \frac{d-1}{2} \right\rfloor+1}^{N'} C_{N'}^{i} \tilde{p}_m^{i} (1-\tilde{p}_m)^{N'-i}. \quad (11)$$

Вероятность ошибочного декодирования НД объектами B и C «виртуального» ДвШКБП определяется из формулы

$$P_E = 1-(1-P_{AB})(1-P_{AC}). \quad (12)$$

Предполагается, что вероятность битовой ошибки равномерно распределяется по КлП. Тогда вероятность ошибки на 1 бит в КлП объекта B определяется следующим выражением:

$$\overline{p}_y = 1-(1-P_{AB})^{\frac{1}{N'}}. \quad (13)$$

Аналогично вероятность ошибки на 1 бит в КлП объекта C может быть определена из выражения

$$\overline{p}_m = 1-(1-P_{AC})^{\frac{1}{N'}}. \quad (14)$$

Нарушитель E так же, как и B и C, использует конструктивный алгоритм декодирования кода $(N'+r, N')$. Вероятность ошибочного декодирования НДН равна

$$P_W = \sum_{i=\left\lfloor \frac{d-1}{2} \right\rfloor+1}^{N'} C_{N'}^{i} \tilde{p}_w^{i} (1-\tilde{p}_w)^{N'-i}. \quad (15)$$

Вероятность ошибки на 1 бит в КлП нарушителя E (в декодированной последовательности НДН) может быть определена из выражения

$$\overline{p}_w = 1-(1-P_W)^{\frac{1}{N'}}. \quad (16)$$

Выполнение задач третьего этапа, связанных с обеспечением формирования K малой вероятности совпадения группового K с клю-

чом E, достигается путем сжатия КлП объектов A, C и B, которые были получены после процедуры исправления ошибок «виртуального» ДвШКБП. Необходимость сжатия КлП с целью уменьшения вероятности совпадения с K нарушителя подробно рассматривается в [1], где предлагается использовать простой алгоритм сжатия символов (ПАСС). Этот алгоритм может применяться для достижения цели размножения ошибок в версии K нарушителя E.

Пусть длины КлП равны N', и параметр длины блока битов КлП v предварительно открыто распределен. Алгоритм состоит в следующем. Объекты A, C и B выделяют из своих КлП l соответствующих блоков битов длины v, причем

$$l = N'/v. \tag{17}$$

Блоки с нечетным числом символов «1» сжимаются (символы блока суммируются по модулю 2) в символ «1», а с четным числом символов «1» сжимаются в «0». Полученные символы объединяются в ключ.

Вероятность несовпадения битов в сформированных ключах объектов A и B описывается следующим соотношением [5]:

$$p_{AB}^{l} = \frac{1-(1-2\overline{p}_y)^v}{2}. \tag{18}$$

Аналогично, вероятность несовпадения бит в ключах объектов A и C равна

$$p_{AC}^{l} = \frac{1-(1-2\overline{p}_m)^v}{2}. \tag{19}$$

Вероятность несовпадения сформированных K группы ОС определяется из выражения

$$P_E^l = 1-\left(1-p_{AB}^l\right)^l\left(1-p_{AC}^l\right)^l. \tag{20}$$

Нарушитель E использует ПАСС для формирования своей версии K. Вероятность несовпадения битов в ключах объекта A и нарушителя E описывается соотношением

$$p_{AE}^{l} = \frac{1-(1-2\overline{p}_w)^v}{2}. \tag{21}$$

Вероятность совпадения K нарушителя E с групповым K определяется выражением

$$P_S = \left(1 - p_{AE}^{l}\right)^{l}. \qquad (22)$$

3. Система показателей качества ГК. Для оценки эффективности протокола формирования ГК необходимо ввести систему функциональных показателей качества ГК и систему требований, предъявляемых к нему.

Определение 1. Скоростью R_3 формирования ключа для трех ОС называется отношение конечной длины l сформированного ГК (в двоичных символах) к длине последовательности $\overline{x}'$, равной N бит, поданной A на вход ДвШКБП и переданной к B и C:

$$R_3 = \frac{l}{N}. \qquad (23)$$

В определении R_3 не учитываются длины последовательностей символов, которые передаются по КОО для формирования ГК трех объектов связи.

В состав системы функциональных показателей качества сформированного ГК предлагаются следующие показатели:

1) показатель *своевременности* формирования ГК (определяется скоростью формирования ГК R_3);

2) комплексный показатель *безопасности* формирования ГК, включающий длину l сформированного ГК и вероятность совпадения ГК нарушителя E с общим сформированным ГК трех ОС P_S, учитывающую знания о ключе, которую получает нарушитель E в результате перехвата всей доступной ему информации, включающей информацию, полученную по каналу перехвата, каналам перехвата обсуждения, а также полное знание описания порядка взаимодействия и алгоритма вычисления ГК объектами A, C и B;

3) показатель *достоверности* формирования ГК, определяемый вероятностью несовпадения сформированных объектом A ГК K_A, объектом B ГК K_B и объектом C ГК K_C длиной l бит, равной $P_E^l = 1 - P\{K_A = K_B\} \cdot P\{K_A = K_C\}$.

Система функциональных показателей качества сформированного ГК включает в себя минимальное время формирования ГК, обладающего минимальной избыточностью при достоверной передаче после-

довательностей битов по ДвШКБП каналу связи, а также при обеспечении малой вероятности совпадения ГК нарушителя E с общим сформированным ГК трех ОС. Эта система является основой предлагаемой системы требований, предъявляемых к сформированному ГК с использованием для формирования ГК последовательностей конечной длины. В качестве основного показателя качества выберем R_3, так как его максимизация определяет минимальное время формирование ГК, а остальные показатели рассматриваются в качестве ограничений.

Исходя из этого к ГК целесообразно предъявить следующие требования:

$$R_3 \to \max; \tag{24}$$

$$l \geq l^{\text{доп}}, \tag{25}$$

где $l^{\text{доп}}$ — допустимая минимальная длина сформированного ГК K;

$$P_S \leq P_S^{\text{доп}}, \tag{26}$$

где $P_S^{\text{доп}}$ — минимальная допустимая вероятность совпадения ГК нарушителя E с общим сформированным ГК трех ОС;

$$P_E^l \leq P_E{}^{\text{доп}}, \tag{27}$$

где $P_E{}^{\text{доп}}$ — допустимая вероятность несовпадения сформированных объектом A ГК K_A, B — ГК K_B и C — ГК K_C.

Особенность выполнения объектами *Примитива* в ПФГК заключаются в том, что в шаге 6 объекта A сохраняется двоичный символ x, которому соответствует кодовое слово x_n, B сохраняет информационный символ y, соответствующий принятому слову y_n, и C сохраняет информационный символ m, соответствующий принятому слову m_n с вероятностью P_{ac} определенной в (5). ОС из символов x, y и m формируют свои НД длиной N' бит. Исправляя несовпадения в НД с помощью помехоустойчивого кодирования, ОС формируют КлП длиной N' бит. Далее ОС используют ПАСС для формирования ГК длиной l бит. Длина ГК должна удовлетворять неравенству $l \geq l^{\text{доп}}$ согласно требованию (24). Учитывая (17), можно определить требование по минимальной длине КлП:

$$N' \geq \nu l^{\text{доп}}. \tag{28}$$

Длина КлП N' является случайной величиной. Тогда необходимо определить P_r — вероятность риска невыполнения требования по $l^{\text{доп}}$, определяющая N — число кодовых слов кода (n, 1), которое на шаге 3 объект A должен передать для формирования НД с минимальной длиной N' бит. Тогда вероятность риска можно определить как

$$P_r = \sum_{i=0}^{N'-1} C_N^i P_{ac}^{\ i} \left(1 - P_{ac}\right)^{N-i} . \tag{29}$$

Необходимо, чтобы

$$P_r \le P_r^{\text{доп}}, \tag{30}$$

где $P_r^{\text{доп}}$ — допустимая минимальная вероятность риска невыполнения требования $l^{\text{доп}}$ по длине формируемого ГК K.

Требование (30) необходимо добавить к системе требований (24)–(27). Согласно этим требованиям, необходимо обеспечить установление криптосвязности A, C и B в сроки, не превышающие допустимые. Это вызывает необходимость подбора следующих параметров протокола: примитива, помехоустойчивого кодирования (ПК), ПАСС, при которых протокол обеспечивал бы минимальное время формирования ГК, что эквивалентно задаче определения параметров элементов протокола, при которых достигается максимальное значение R_3. Тогда *задача оптимизации* представляет собой определение параметров протокола, при которых достигается максимальная R_3. Задачу оптимизации протокола можно записать в следующем виде:

$$\begin{cases} R_3 = f\left(p_y, p_m, n, N, v\right) \to \max; \\ l = f1\left(N, v\right) \ge l^{\text{доп}}; \\ P_S = f2\left(p_w, n, N, N+r, v\right) \le P_S^{\text{доп}}; \\ P_E^l = f3\left(p_y, p_m, n, N, N+r, v\right) \le P_E^{\text{доп}}; \\ P_r = f4\left(p_y, p_m, n, N\right) \le P_r^{\text{доп}}. \end{cases} \tag{31}$$

В табл. 1 приведена оценка максимально достижимой скорости R_3 для требований $l = 256$ бит, $P_S^{\text{äîï}} = 2{,}939 \cdot 10^{-39}$, $P_E^{\text{äîï}} = 10^{-4}$, $P_r^{\text{доп}} = 10^{-5}$ и интервалов изменения вероятностей ошибок в первом

составляющем канале ДвШКБП $p_y \in [0.01; 0.05]$ и КП $p_w \in [0.01; 0.1]$ при фиксированной вероятности ошибки во втором составляющем канале ДвШКБП $p_m = 0.01$.

Таблица 1. **Максимальные значения скорости R_3 при $p_m = 0.01$**

p_w	p_y				
	0.01	0.02	0.03	0.04	0.05
0.01	0	0	0	0	0
0.02	0	0	0	0	0
0.03	0.021	0	0	0	0
0.04	0.026	0.023	0	0	0
0.05	0.04	0.028	0.025	0	0
0.06	0.053	0.033	0.028	0.026	0
0.07	0.071	0.042	0.033	0.029	0.028
0.08	0.083	0.056	0.036	0.033	0.029
0.09	0.1	0.067	0.045	0.033	0.033
0.10	0.111	0.083	0.059	0.04	0.036

Выше описан ПФГК для трех ОС. Для формирования СК необходимо рассмотреть ПФГК для двух ОС. Для указанного протокола можно использовать такой же метод, как и для трех ОС, с той лишь разницей, что необходимо сделать следующее предположение: в МКС вероятность ошибки p_m во втором составляющем канале ДвШКБП (канале связи КС-2) равна нулю, т.е. $p_m = 0$. Таким образом, из рассмотрения исключается объект *C*.

4. Выбор сетевого ключа и передача его *W* объектам сети. Оценка эффективности формирования сетевого ключа. В качестве СК выбирается ключ одной из групп первой или второй фазы ПФГК. Передача СК начинается одновременно всеми ОС группы СК и осуществляется по каналам связи, закрытым с помощью групповых ключей, полученных на предыдущих фазах. Исследуем эту фазу на примере формирования СК для восьми ОС, т.е. $W = 8$. После выполнения первой или второй фазы протокола формирования СК (ПФСК) каждый ОС может использовать ПФГК для трех ОС или ПФГК для двух ОС. В итоге формируются группы, включающие три или две ОС. Обозначим число таких групп в фазе *N3* или *N2* соответственно.

Если $W \bmod(3) = 0$, тогда

$$N3 = W/3, \quad N2 = 0. \tag{32}$$

Если $W \bmod(3) = 1$, тогда

$$N3 = (W-4)/3, \quad N2 = 2. \tag{33}$$

Если $W \bmod(3) = 2$, тогда

$$N3 = (W-2)/3, \quad N2 = 1. \tag{34}$$

Для $W = 8$ имеем $N3 = 2$ и $N2 = 1$.

Формирование СК по сравнению с ГК имеет следующие особенности. Каждый из ОС группы СК передает его на своем ГК второй фазы ОС из своих групп. В данном случае число тактов передачи СК $G = 1$. В случаях, когда $W > 9$ и (или) группами из двух или трех ОС не удалось в фазе охватить всех ОС, может быть $G > 1$. Особенностью выполнения ОС ПФГК для трех ОС является такое событие, при котором совпадает ключ только между двумя ОС, а с третьим ОС группы не совпадает. Это событие происходит с вероятностью P_2, которую на основании (20) можно определить как

$$P_2 = \left(1-p_{AC}^l\right)^l \left(1-\left(1-p_{AB}^l\right)^l\right) + \left(1-p_{AB}^l\right)^l \left(1-\left(1-p_{AC}^l\right)^l\right), \tag{35}$$

где p_{AB}^l — вероятность несовпадения битов в сформированных ключах *A* и *B,* определенная в (17); p_{AC}^l — вероятность несовпадения битов в сформированных ключах ОС *A* и *C,* определенная в (19).

Возникновение таких событий при формировании ГК на первой и второй фазах ПФСК при определенной конфигурации позволяет криптографически связать группы ОС, охватывающих всех *W* ОС сети. В такой ситуации *G* может быть более 1, и маршрут передачи СК может существенно отличаться от тривиального маршрута. С учетом этого можно сказать, что после выполнения первой и второй фаз протокола формирования СК (ПФСК) каждый ОС может иметь криптографическую связность с четырьмя или с тремя, или с двумя другими ОС, или с одним другим ОС или не иметь ее ни к каким ОС сети.

Введем теперь систему функциональных показателей качества СК и разработаем систему требований, предъявляемых к нему.

Определение 2. Скоростью R_W формирования СК для *W* объектов называется отношение конечной длины *l* сформированного СК (в дво-

ичных символах) к суммарной максимальной длине последовательностей, передаваемых по каналам связи с ошибками при выполнении ПФГК на первой и второй фазах ПФСК, и последовательности передачи СК:

$$R_W = \frac{l}{N1_{\max} + N2_{\max} + GX}, \tag{36}$$

где X — длина последовательности с зашифрованным СК на ГК.

В определении R_W не учитываются длины последовательностей символов, которые передаются по КОО для формирования ГК трех (двух) ОС.

Предлагается следующая система функциональных показателей качества сформированного СК:

1) показатель *своевременности* формирования ГК — R_W;

2) показатель *безопасности* формирования СК — вероятность $P1_S$ совпадения СК нарушителя E с общим сформированным СК, учитывающая знания о ключе, которую получает нарушитель E;

3) показатель *достоверности* формирования СК — вероятность P_{CK} невозможности шифрованной передачи СК;

4) показатель *риска невыполнения* требований к СК — вероятность $P1_r$ риска невыполнения требований к СК.

Определим связь показателей качества СК с показателями качества ГК. Связь $P1_S$ и P_S определяется выражением

$$P1_S = \sum_{i=0}^{N23}\sum_{j=1}^{N23} C_{N23}^{i} C_{N23}^{j} P_S^{i+j} (1-P_S)^{2N23-i-j} + \\ + \sum_{i=1}^{N23} C_{N23}^{i} P_S^{i} (1-P_S)^{2N23-i}, \tag{37}$$

где $N23$ — общее число групп, включающих по три или два объекта в фазе ПФСК, $N23 = N2 + N3$.

Связь P_{CK} и P_E^l определяется выражением

$$P_{CK} = 1 - \left(\sum_{i=0}^{N3} \left[\left[WC_{N3}^{i-1} + C_{N3}^{i} + A(i) + B(i) \right] p^i (1-p)^{R1-i} \right] \right). \tag{38}$$

где $p = 1 - \sqrt{1 - P_E^l}$ — эквивалентная вероятность несовпадения ГК для ПФГК; $R1$ — общее число возможных криптосвязностей между двумя ОС в сети из W ОС, $R1 = W + N3$;

$$A(i)=\begin{cases} 0, \text{ если } i<2, \\ \sum\limits_{k=2}^{i} C_{N3}^{k-1} 2^k C_{N3-(k-1)}^{i-k}, \quad \text{если } i\geq 2; \end{cases}$$

$$B(i)=\begin{cases} 0, \text{если } i<3, \\ \sum\limits_{k=2}^{i-1} C_{N3}^{k-1} 2^k C_{N3-(k-1)}^{i-1-k} 2(N3-(k-1)), \text{если } i\geq 3. \end{cases}$$

Связь $P1_r$ и P_r определяется выражениями (36)–(37) с заменой $P1_S$ на $P1_r$ и P_S на P_r.

По аналогии с оценкой эффективности ГК система требований, предъявляемых к СК, включает в себя требования:

$$R_W \to \max, \tag{39}$$

$$P1_S \leq P1_S^{\text{доп}}, \tag{40}$$

где $P1_S^{\text{доп}}$ — минимально допустимая вероятность совпадения СК нарушителя E с СК;

$$P_{CK} \leq P_{CK}{}^{\text{доп}}, \tag{41}$$

где $P_{CK}{}^{\text{доп}}$ — допустимая вероятность невозможности шифрованной передачи СК;

$$P1_r \leq P1_r^{\text{доп}}, \tag{42}$$

где $P1_r^{\text{доп}}$ — допустимая вероятность риска невыполнения требования к СК.

По аналогии, связь между требованиями к СК и ГК определяется так же, как и для показателей качества СК и ГК

Сделаем предположения для исследуемого случая. Пусть максимальные длины последовательностей передаваемых по каналам связи с ошибками на первой и второй фазах $N1_{\max}, N2_{\max}$ определяются худшим соотношением вероятностей ошибок ПФГК. Тогда

$$N1_{\max} = N2_{\max} = N_{\max}.$$

Пусть любая обработка информации, выполняемая ОС, в ПФСК производится мгновенно, а для шифрования СК на третьей фазе используется метод гаммирования [6] и приняты меры защиты от ошибок при этой передаче. Тогда длина последовательности с зашифро-

ванным СК на ГК $X = l$. Учитывая, что число тактов передачи СК $G = 1$, выражение (23) и требование (24) ПФГК для скорости формирования ГК, выражение (36) перепишем в виде

$$R_W = \frac{(R_3)^2}{2R_3 + (R_3)^2}. \quad (43)$$

В табл. 2 приведена оценка максимально достижимой скорости R_W СК для исследуемого случая, требований $l = 256$ бит, $P1_S^{\text{доп}} = 1.763 \cdot 10^{-38}$, $P_{CK}{}^{\text{доп}} = 1.999 \cdot 10^{-7}$, $P1_r^{\text{доп}} = 5.999 \cdot 10^{-5}$ и интервалов изменения «худших» вероятностей ошибок составляющих каналов ДвШКБП ПФГК на первой и второй фазах ПФСК $p_y \in [0.01; 0.05]$ и КП $p_w \in [0.01; 0.1]$ при фиксированной $p_m = 0.01$.

Анализ табл. 2 показывает, что $R_3 > R_W$. R_W изменяется от $1.162 \cdot 10^{-4}$ до $9.781 \cdot 10^{-3}$. Соответственно для формирования 1 бита СК при выполнении ПФСК необходимо в среднем передавать по каналам связи с ошибками от 8605,851 до 102,239 бит информации.

Таблица 2. **Максимальные значения скорости R_W при $p_m = 0.01$**

p_w	p_y				
	0.01	0.02	0.03	0.04	0.05
0.01	0	0	0	0	0
0.02	0	0	0	0	0
0.03	$4.459 \cdot 10^{-3}$	0	0	0	0
0.04	$1.162 \cdot 10^{-4}$	$3.735 \cdot 10^{-3}$	0	0	0
0.05	$7.711 \cdot 10^{-3}$	$2.946 \cdot 10^{-3}$	$3.266 \cdot 10^{-3}$	0	0
0.06	$5.908 \cdot 10^{-3}$	$2.415 \cdot 10^{-3}$	$2.731 \cdot 10^{-3}$	$2.787 \cdot 10^{-3}$	0
0.07	$4.391 \cdot 10^{-3}$	$8.147 \cdot 10^{-3}$	$2.199 \cdot 10^{-3}$	$2.513 \cdot 10^{-3}$	$2.578 \cdot 10^{-3}$
0.08	$3.783 \cdot 10^{-3}$	$6.154 \cdot 10^{-3}$	$1.926 \cdot 10^{-3}$	$1.967 \cdot 10^{-3}$	$2.292 \cdot 10^{-3}$
0.09	$3.174 \cdot 10^{-3}$	$5.162 \cdot 10^{-3}$	$8.09 \cdot 10^{-3}$	$1.967 \cdot 10^{-3}$	$2.018 \cdot 10^{-3}$
0.10	$2.874 \cdot 10^{-3}$	$4.16 \cdot 10^{-3}$	$6.294 \cdot 10^{-3}$	$9.781 \cdot 10^{-3}$	$1.744 \cdot 10^{-3}$

5. Заключение. Предложенная МКС позволяет в полной мере охарактеризовать объекты, участвующие в формировании СК. В рамках данной модели разработан протокол формирования СК по открытым каналам связи с ошибками, включающий в себя ряд процедур, реализуемых на временных фазах протокола.

Предлагаемый ПФСК обладает рядом преимуществ:

1) он ориентирован на использование первичных каналов;

2) стойкость СК обеспечивается случайностью ошибок, всегда имеющих место в реальных каналах связи;

3) формирование СК производится без участия центра распределения ключей, что также увеличивает стойкость СК.

Однако ПФСК также не лишен и недостатков — необходимо точное управление его фазами.

Литература

1. *Симмонс Г. Дж.* Обзор методов аутентификации информации // ТИИЭР. Т.76, № 5. 1988. С. 105–125.
2. *Чисар И., Кернер Я.* Теория информации: теоремы кодирования для дискретных систем без памяти. М.: Мир, 1985. 400 с.
3. *Зюко А., Кловский Д., Назаров М., Финк Л.* Теория передачи сигналов. М.: Радио и связь, 1986. 355 с.
4. *Мак-Вильямс Ф., Слоэн Н.* Теория кодов, исправляющих ошибки. М.: Связь, 1979. 744 с.
5. *Галлагер Р.* Коды с малой плотностью проверок на четность. М.: Мир, 1966. 320 с.
6. *Молдовян Н. А., Молдовян А. А., Еремеев М. А.* Криптография: от примитивов к синтезу алгоритмов. СПб.: БХВ-Петербург, 2004. 448 с.

Синюк Александр Демьянович — канд. техн. наук, доцент; преподаватель кафедры Военной академии связи. Область научных интересов: обработка и передача данных по каналам связи, теория моделирования и математическая статистика, теория информации. Число научных публикаций — 101. eentrop@rambler.ru; Военная академия связи, Тихорецкий проспект, 3, Санкт-Петербург, 194064, РФ; р.т. +7(812)247-9342.

Sinjuk Aleksandr Dem'yanovich — PhD in Technical, associate professor; lecturer, Military academy of signal communication. Research interests: processing and transfer of data on data links, theory of modeling and mathematical statistics, information theory. The number of publications — 101. eentrop@rambler.ru; Military academy of signal communication, Tihoretskiy broad street, 3, St. Petersburg, 194064, Russia; office phone +7(812)247-9842.

Саенко Игорь Борисович — д-р техн. наук, проф.; ведущий научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации РАН (СПИИРАН), профессор кафедры Военной академии связи. Область научных интересов: автоматизированные информационные системы, информационная безопасность, обработка и передача данных по каналам связи, теория моделирования и математическая статистика, теория информации. Число научных публикаций — 220. ibsaen@mail.ru; СПИИРАН, 14-я линия В.О., д. 39, Санкт-Петербург, 199178, РФ; р.т. +7(812)328-2642, факс +7(812)328-4450.

Saenko Igor Borisovich — Ph.D., Doctor of Technical Sciences, professor; leading research scientist of laboratory of computer network security of Saint-Petersburg Institute for Information and Automation of RAS (SPIIRAS), professor of Military academy of signal communication. Research interests: automated information systems, information security, processing and transfer of data on data links, theory of modeling and mathematical statistics, information

theory. The number of publications — 220. ibsaen@mail.ru; SPIIRAS, 14th line, 39, St. Petersburg, 199178, Russia; office phone +7(812) 328-2642, fax +7(812)328-4450.

Рекомендовано лабораторией проблем компьютерной безопасности, заведующий лабораторией, д-р техн. наук, проф. И.В. Котенко.
Статья поступила в редакцию 10.12.2010.

РЕФЕРАТ

Синюк А.Д., Саенко И.Б. **Протокол формирования сетевого ключа по открытым каналам связи с ошибками.**

В статье рассматриваются вопросы разработки протокола формирования сетевого ключа по открытым каналам связи с ошибками.

Общая постановка задачи сводится к следующему: необходимо разработать способ формирования сетевого ключа для нескольких объектов связи сети за минимальное время, осуществляя обмен данными конечной длины между ними по каналам сети, доступным нарушителю. При этом требуется обеспечить формирование сетевого ключа с высокой достоверностью для объектов связи и обеспечить формирование сетевого ключа с малой вероятностью совпадения с ключом нарушителя. Объекты связаны между собой множеством открытых каналов связи с ошибками и каждый из них имеет аппаратуру шифрования, реализующую единый алгоритм шифрования. Предполагается, что нарушитель пассивен.

Разработанный протокол включает три временные фазы. Первая фаза устанавливает криптосвязность в независимых группах объектов связи. Вторая фаза устанавливает криптосвязность между независимыми группами объектов. Третья фаза выбирает сетевой ключ из множества сформированных ключей и передает его всем объектам связи сети.

Рассматривается модель канальной связности, которая включает в себя объекты связи как санкционированные участники информационного обмена и нарушителя, связанные следующими каналами: связи, перехвата и открытого обсуждения.

Дано описание примитива как простейшей процедуры протокола. Приведены расчетные выражения для оценки вероятностных характеристик примитива.

Предложены системы показателей эффективности формирования группового и сетевого ключа, а также предъявляемые требования по оперативности, безопасности и достоверности. Определена связь показателей качества группового ключа с показателями качества сетевого ключа. Обоснована постановка задачи оптимизации параметров протокола формирования сетевого ключа.

На основе предложенных показателей осуществлена экспериментальная оценка качества формирования группового и сетевого ключей и проведен сравнительный анализ полученных результатов, который выявил преимущества и недостатки предложенного протокола формирования сетевого ключа.

SUMMARY

Sinjuk A.D., Saenko I.B. **Network key formation protocol on open communication channels with errors.**

The article deals with the development of a protocol of forming a network key to open communication channels with errors.

General problem boils down to this: it is necessary to develop a method of forming a network key for multiple objects communication network in minimum time by exchanging data of finite length between them through the network, accessible infringer. It is required to ensure the formation of a network switch with high reliability for communication facilities and ensure the formation of a network key with a low probability match with a key offender. Objects are interconnected set of open communication channels with errors and each one has a hardware encryption provides a single encryption algorithm. It is assumed that the offender is inactive.

Designed protocol includes three time phases. The first phase establishes crypto connection in independent groups of communications. The second phase establishes crypto connection between independent groups of objects. The third phase selects the network key from the set of generated keys, and sends it to all objects of communication networks.

It is considered a model of channel connectivity, which includes the communications facilities as authorized by the members for information exchange and the offender involved in these channels: communication channels, interception channels and channels of open discussion.

A description of the primitive as a simple procedure protocol is defined. The calculated expressions for estimating the probability characteristics of the primitive are presented.

It is proposed a system of performance indicators forming a group key and a network key, as well as its demands on efficiency, safety and reliability. It is defined relationship between quality indicators of the group's and the network key. It is done the optimization task statement of the network key formation protocol parameters.

Based on the proposed indicators it is carried out an experimental evaluation of the quality of formation the group's and network keys, and a comparative analysis of the results, which showed the advantages and disadvantages of the proposed of the network key formation protocol.