УДК 621.391.2

Синюк А.Д., Козленко А.В., Чирушкин К.А.

ИНФОРМАЦИОННО-ТЕОРЕТИЧЕСКАЯ МОДЕЛЬ ФОРМИРОВАНИЯ КЛЮЧА ПО ОТКРЫТЫМ КАНАЛАМ БЕЗ ОШИБОК

Синюк А.Д., Козленко А.В., Чирушкин К.А. **Информационно-теоретическая модель формирования ключа по открытым каналам без ошибок.**

Аннотация. В статье проводится анализ условий передачи сообщений по открытым каналам без ошибок. Предлагается модель формирования неопределенностей легальных пользователей и нарушителя. Оценивается энтропия Шеннона участников информационного обмена. Проводится сравнительный анализ полученных результатов, на основе которых формируются выводы и предложения по проведению дальнейших исследований.

Ключевые слова: открытые каналы без ошибок, модель формирования неопределенностей легальных пользователей и нарушителя, энтропия Шеннона участников информационного обмена, потенциальные условия формирования ключа, ключевые последовательности, модель канальной связности.

Sinjuk A.D., Kozlenko A.V., Chirushkin K.A. **Informational-theoretical model of key sharing based on noiseless public channels.**

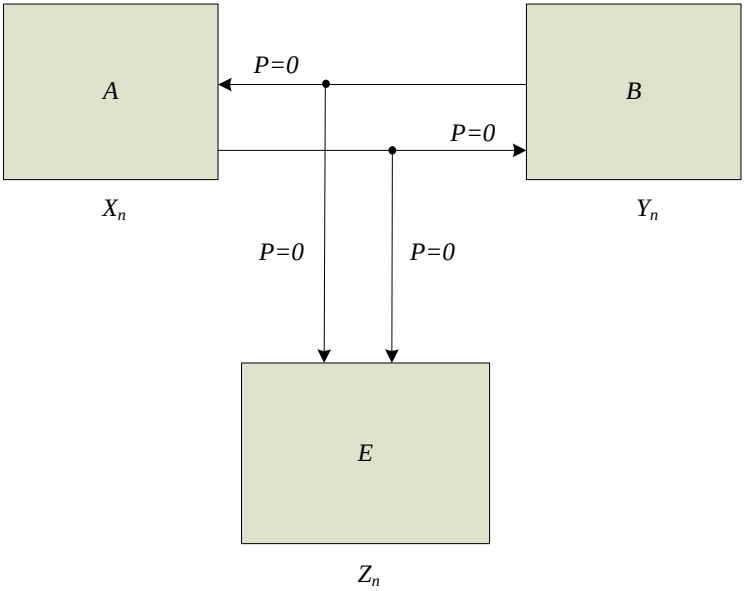
Abstract. In article the analysis of conditions of message transfer on the noiseless public channels. The model of formation uncertainty legal users and eavesdropper is offered. Shannon entropy participants of an information exchange is estimated. The comparative analysis of the received results on the basis of which conclusions and offers on carrying out of the further researches are formed is carried out.

Keywords: noiseless public channels, model of formation uncertainty legal users and eavesdropper, Shannon entropy participants of an information exchange, potential conditions of key sharing, key sequences, model of channel connectivity.

1. Введение. В статье проводится анализ условий передачи сообщений по открытым каналам без ошибок на основе информационно-теоретической модели формирования неопределенностей легальных пользователей и нарушителя.

2. Основная часть. Необходимо сформировать ключевые последовательности (КлП) (из которых затем вырабатывается общий ключ) для легальных пользователей A и B, осуществляя обмен данными между ними по двунаправленному каналу без ошибок, доступному нарушителю E по безошибочному каналу перехвата. При этом требуется обеспечить формирование КлП с высокой достоверностью для пользователей (минимальную неопределенность для пользователей) и обеспечить заданное малое количество информации о КлП для E (максимальную неопределенность для нарушителя). Предполагается,

что нарушитель пассивен. Пользователей A и B и нарушителя E, которые связаны каналами связи, можно представить моделью канальной связности (МКС) (см. рисунок).



Модель канальной связности пользователей A и B и нарушителя E.

В общем виде модель можно описать следующим образом. A и B имеют двоичные источники без памяти (ДИБП) для формирования первичных последовательностей (ПП) X^N и Y^N длиной N бит, соответственно. Дуплексный канал связи без ошибок между пользователями A и B назовем основным каналом. Совокупность каналов связи без ошибок от пользователя A к нарушителю E и от пользователя B к E назовем каналом перехвата (КП).

Процесс формирования КлП можно разделить на три этапа.

Первый этап — предварительное открытое распределение параметров вероятностного распределения последовательностей X^N и Y^N, их длина N, порядок действий, описывающих протокол исправления несовпадений.

Второй этап — генерирование ПП — исходного материала для формирования КлП.

Третий этап предназначен для обеспечения формирования КлП с высокой достоверностью. Это достигается путем устранения (исправления) несовпадающих символов в КлП на основе информационного обмена дополнительной информацией. Предполагается, что нарушитель перехватывает ее по каналу перехвата и использует для формирования своей версии КлП. Ему известны параметры вероятностного распределения последовательностей X^N и Y^N, их длина N, протокол (алгоритм) исправления несовпадений.

Предлагается следующий алгоритм генерирования ПП. A передает B по основному каналу без ошибок параметры распределения: N — длину формируемой ПП X^N и $p1$ — вероятность генерирования выбранного символа (например, символа «1»).

A и B генерируют с помощью ДИБП двоичные последовательности X^N и Y^N соответственно. Допускается преобладание вероятности генерирования любого символа. Пусть вероятности генерирования символа $x=1$ в ПП X^N и $y=1$ в ПП Y^N равны между собой и выполняется условие

$$p1 = P\{x=1\} = P\{y=1\} > 0.5 \quad (1)$$

$$1-p1 = P\{x=0\} = P\{y=0\} < 0.5 \quad (2)$$

Пусть α_{ij} — совместная вероятность события, при котором информационный символ $x=i$ сгенерирован A и информационный символ $y=j$ сгенерирован B, где $i \in \{0,1\}$ и $j \in \{0,1\}$, тогда

$$\begin{aligned} \alpha_{00} &= (1-p1)^2, \\ \alpha_{10} &= p1(1-p1), \\ \alpha_{01} &= (1-p1)p1, \\ \alpha_{11} &= p1^2. \end{aligned} \quad (3)$$

Определим p — вероятность события, при котором соответствующие биты ПП X^N и ПП Y^N не совпадают:

$$p = \alpha_{10} + \alpha_{01} = 2\alpha_{10} = 2p1(1-p1). \quad (4)$$

Утверждение. Соответствующие биты в сгенерированных ПП пользователей A и B, согласно распределению вероятностей описываемому выражениями (1) и (2), совпадают (согласовываются) с вероятностью больше 0,5.

Доказательство. Чтобы доказать, что сгенерированные ПП X^N и Y^N побитно совпадают (согласовываются) с вероятностью больше чем 0.5, достаточно показать, что

$$(1-p)-p>0. \tag{5}$$

Анализ выражений (2) и (3) показывает, что $P\{x=1\}>P\{x=0\}$ или $p1>1-p1$. Определим величину ε как разницу между $P\{x=1\}$ и $P\{x=0\}$, тогда

$$\varepsilon = p1-(1-p1)=2p1-1. \tag{6}$$

Очевидно, что $\varepsilon>0$. Подставим выражения (4) в (6) и учитывая, что $1-p=(1-p1)^2+p1^2$ получим:

$$(1-p)-p=(1-p1)^2+p1^2-2p1(1-p1). \tag{7}$$

Перегруппируем выражение (7) с общими множителями и, подставляя (6) в (7), получаем:

$$(1-p)-p=(1-p1)(-\varepsilon)+p1\varepsilon. \tag{8}$$

Выносим общий множитель и, подставляя (6) в (8), получаем

$$(1-p)-p=\varepsilon^2. \tag{9}$$

Так как $\varepsilon>0$, тогда выражение (6) истинно. Что и требовалось доказать.

Сгенерированные ПП X^N и Y^N не совпадают с высокой вероятностью. Процедура исправления побитовых несовпадений (ошибок) может быть реализована с использованием *помехоустойчивого кодирования с обнаружением ошибок.* Для этого A с помощью предлагаемого конструктивного линейного кода (параметры которого предварительно открыто распределены) находит проверочные символы к информационной последовательности X^N и посылает проверочные символы к B по бесшумному ОК-каналу в составе последовательности проверочных символов (ППС). B обнаруживает несовпадения в Y^N, используя принятые проверочные символы и конструктивный алгоритм декодирования для выбранного кода.

Для формирования ППС предлагается использовать код (n,k), где k — длина информационного слова в битах, n — длина кодового слова в битах, причем $n=2k-1$. Тогда длина блока проверочных

символов (БПС) равна $k-1$. Формирование каждого j-го бита БПС pr_j, где $j=1,\ldots,k-1$, осуществляется по правилу:

$$pr_j = i_1 \oplus i_{j+1}, \tag{10}$$

где i_f — f-й символ информационного слова, $f=2,\ldots,k$; $\oplus$ — суммирование по модулю 2.

Для кода с $n=5$ перечень кодовых слов приведен в табл. 1.

Таблица 1. **Перечень кодовых слов**

Номер кодового слова	Длина кодового слова				
	Информационное слово			Блок проверочных символов	
	1 бит	2 бит	3 бит	1 бит	2 бит
1	0	0	0	0	0
2	0	0	1	0	1
3	0	1	0	1	0
4	0	1	1	1	1
5	1	0	0	1	1
6	1	0	1	1	0
7	1	1	0	0	1
8	1	1	1	0	0

Анализ табл. 1 показывает, что одинаковым БПС соответствуют два инвертированных информационных слова.

A и B разбивают свои ПП на Q информационных слов длиной k бит. Тогда

$$Q = \lfloor N/k \rfloor, \tag{11}$$

где выражение в скобках $\lfloor \bullet \rfloor$ означает округление до ближайшего меньшего целого числа.

Затем последовательно для каждого m-го информационного слова длиной k бит, где $m=1,\ldots,Q$, пользователи формируют m-й БПС по правилу (10) и запоминают его. Далее они объединяют Q БПС в последовательность ППС. Длины последовательностей равны w и определяются из выражения:

$$w = Q(k-1). \tag{12}$$

Пользователь A передает пользователю B ППС по основному каналу без ошибок. Пользователь B обнаруживает несовпадающие у

него с пользователем A информационные слова длиной k бит с помощью принятой от A ППС. По результатам обнаружения он формирует последовательность принятия решений (ППР). Для этого пользователь B последовательно разбивает свою ППС и принятую от A ППС на Q БПС длиной по $(k-1)$ бит согласно выражению (12). Затем последовательно для каждой m-й соответствующей пары БПС из своей и принятой ППС, где $m=1,\ldots,Q$, пользователь B формирует m-й бит ППР по правилу: в случае полного поразрядного совпадения в результате сравнения $(k-1)$ бит запоминается символ «1» или в противном случае запоминается символ «0». Затем он объединяет Q сформированных бит в ППР. Пользователь B передает ППР по основному каналу связи без ошибок пользователю A. Пользователи A и B стирают обнаруженные несовпадающие у них информационные слова при наличии в ППР символа «0» для соответствующего слова. Затем из нестертых информационных слов запоминают по 1 биту, например первому биту, а остальные отбрасывают. Сохраненные биты A и B объединяют и запоминают в КлП длиной s бит, причем $s \le Q$.

В рамках информационно-теоретического подхода оценки стойкости криптографических систем защиты информации [1] определенное соотношение неопределенностей (энтропии) легальных пользователей и нарушителя позволяет создать условия для формирования ключа [2–4]. Оценим энтропию Шеннона для КлП легальных пользователей.

Теорема 1. Пусть легальные пользователи A и B используют для формирования КлП алгоритм генерирования ПП, определенный в выражениях (1)–(4), и (n,k)-помехоустойчивый код с обнаружением ошибок, определенный выражениями (10)–(12). Тогда для пользователя A энтропия Шеннона сохраненного (не стертого) информационного слова длиной k бит равна

$$H_A = \frac{-1}{\sum_{d=0}^{k} C_k^d \left(\alpha_{11}^d \alpha_{00}^{k-d} + \alpha_{10}^k\right)} \sum_{d=0}^{k} \left[C_k^d \cdot \left\langle \alpha_{10}^k \log_2 \left\{ \frac{\alpha_{10}^k}{\alpha_{11}^d \alpha_{00}^{k-d} + \alpha_{10}^k} \right\} + \right.\right.$$

$$\left.\left. + \alpha_{11}^d \alpha_{00}^{k-d} \log_2 \left\{ \frac{\alpha_{11}^d \alpha_{00}^{k-d}}{\alpha_{11}^d \alpha_{00}^{k-d} + \alpha_{10}^k} \right\} \right\rangle \right],$$

где α_{ij} — совместная вероятность события, при котором информационный символ $x = i$ сгенерирован пользователем A и информационный символ $y = j$ сгенерирован пользователем B, где $i \in \{0,1\}$ и $j \in \{0,1\}$, определенная в выражении (3).

Доказательство. Рассмотрим ситуацию у легальных пользователей A и B. Пусть k — длина информационного принятого (нестертого) слова a в битах, n — длина кодового слова в битах, причем $n = 2k - 1$ (см. выражение (10)). Обозначим через $|a|$ вес Хемминга (число единиц) блока a длиной k, сохраненного пользователем A. Легко показать, что совместная вероятность события, состоящего в том, что пользователь A принял блок, содержащий d единиц, $|a| = d$, равна

$$P(|a| = d, \text{принят} A) = \alpha_{11}^{d}\alpha_{00}^{k-d} + \alpha_{10}^{d}\alpha_{01}^{k-d} = \alpha_{11}^{d}\alpha_{00}^{k-d} + \alpha_{10}^{k}, \qquad (13)$$

где α_{ij} — совместная вероятность события, при котором информационный символ $x = i$ сгенерирован A и информационный символ $y = j$ сгенерирован B, где $i \in \{0,1\}$ и $j \in \{0,1\}$, определенная в выражении (3).

Легко определить, что совместная вероятность события, состоящего в том, что пользователь A принял блок безошибочно, содержащий d единиц, $|a| = d$, равна

$$P(|a| = d, \text{бо}, \text{принят} A) = \alpha_{11}^{d}\alpha_{00}^{k-d}. \qquad (14)$$

Совместная вероятность события, состоящего в том, что пользователь A ошибочно принял блок, содержащий d единиц, $|a| = d$, равна

$$P(|a| = d, \text{но}, \text{принят} A) = \alpha_{10}^{d}\alpha_{01}^{k-d} = \alpha_{10}^{k}. \qquad (15)$$

Используя теорему Байеса, получаем следующие вероятности безошибочного и ошибочного приема A информационных k-слов, при условии, что A принял блок $|a| = d$:

$$P(\text{бо}/|a| = d, \text{принят} A) = \frac{\alpha_{11}^{d}\alpha_{00}^{k-d}}{\alpha_{11}^{d}\alpha_{00}^{k-d} + \alpha_{10}^{d}\alpha_{01}^{k-d}} = \frac{\alpha_{11}^{d}\alpha_{00}^{k-d}}{\alpha_{11}^{d}\alpha_{00}^{k-d} + \alpha_{10}^{k}}, \qquad (16)$$

$$P(\text{но}/|a| = d, \text{принят} A) = \frac{\alpha_{10}^{d}\alpha_{01}^{k-d}}{\alpha_{11}^{d}\alpha_{00}^{k-d} + \alpha_{10}^{d}\alpha_{01}^{k-d}} = \frac{\alpha_{10}^{k}}{\alpha_{11}^{d}\alpha_{00}^{k-d} + \alpha_{10}^{k}}. \qquad (17)$$

Тогда энтропия Шеннона принятого информационного слова a, при условии, что A принял блок $|a| = d$, равна

$$H(d, \text{принят}A) = \\ = -\left\langle P(но/|a| = d, \text{принят}A) log_2 \left\{P(но/|a| = d, \text{принят}A)\right\} + \right. \\ \left. + P(бо/|a| = d, \text{принят}A) log_2 \left\{P(бо/|a| = d, \text{принят}A)\right\}\right\rangle . \quad (18)$$

Подставим в (18) выражения (16) и (17) и получим

$$H(d, \text{принят}A) = \\ = -\left\langle \frac{\alpha_{10}^k}{\alpha_{11}^d \alpha_{00}^{k-d} + \alpha_{10}^k} log_2 \left\{ \frac{\alpha_{10}^k}{\alpha_{11}^d \alpha_{00}^{k-d} + \alpha_{10}^k} \right\} + \right. \\ \left. + \frac{\alpha_{11}^d \alpha_{00}^{k-d}}{\alpha_{11}^d \alpha_{00}^{k-d} + \alpha_{10}^k} log_2 \left\{ \frac{\alpha_{11}^d \alpha_{00}^{k-d}}{\alpha_{11}^d \alpha_{00}^{k-d} + \alpha_{10}^k} \right\} \right\rangle . \quad (19)$$

Найдем вероятность приема пользователем A слова длиной k бит, используя выражение (13):

$$P(\text{принят}A) = \sum_{\forall a} P(a, \text{принят}A) = \\ = \sum_{d=0}^{k} C_k^d P(|a| = d, \text{принят}A) = \sum_{d=0}^{k} C_k^d (\alpha_{11}^d \alpha_{00}^{k-d} + \alpha_{10}^k) . \quad (20)$$

Используя теорему Байеса, получаем вероятность наличия у k информационного k-слова с весом $|a| = d$, при условии, что A принял блок a:

$$P(|a| = d / \text{принят}A) = \frac{P(|a| = d, \text{принят}A)}{P(\text{принят}A)} = \frac{\alpha_{11}^d \alpha_{00}^{k-d} + \alpha_{10}^k}{\sum_{d=0}^{k} C_k^d (\alpha_{11}^d \alpha_{00}^{k-d} + \alpha_{10}^k)} \quad (21)$$

Тогда для пользователя A энтропия Шеннона не стертого информационного слова длиной k бит равна

$$H_A = \sum_{\forall a} P(a/\text{принят}A) H(a, \text{принят}A) = \\ = \sum_{d=0}^{k} C_k^d P(|a| = d / \text{принят}A) H(|a| = d, \text{принят}A) \quad (22)$$

Подставим в (22) выражения (21) и (19) и получим

$$H_A = \frac{-1}{\sum_{d=0}^{k} C_k^d (\alpha_{11}^d \alpha_{00}^{k-d} + \alpha_{10}^k)} \sum_{d=0}^{k} \left[C_k^d \cdot \left\langle \alpha_{10}^k \log_2 \left\{ \frac{\alpha_{10}^k}{\alpha_{11}^d \alpha_{00}^{k-d} + \alpha_{10}^k} \right\} + \right. \right.$$

$$\left. \left. + \alpha_{11}^d \alpha_{00}^{k-d} \log_2 \left\{ \frac{\alpha_{11}^d \alpha_{00}^{k-d}}{\alpha_{11}^d \alpha_{00}^{k-d} + \alpha_{10}^k} \right\} \right\rangle \right]. \quad (23)$$

Теорема доказана.

Очевидно, что для пользователей A и B.

$$H_A = H_B \quad (24)$$

Генерирование ПП создает условия, когда у нарушителя нет возможности оптимального выбора наблюдения за каким-то одним пользователем — они для него равноценны. Тогда пусть нарушитель наблюдает за пользователем A. Определим энтропию нарушителя.

Теорема 2. Пусть легальные пользователи A и B используют для формирования принятого информационного слова КлП длиной k бит алгоритм генерирования ПП, определенный в выражениях (1)–(4) и (n,k) -помехоустойчивый код с обнаружением ошибок, определенный выражениями (10)–(12). Пусть нарушитель E знает всю открыто распределенную информацию об алгоритме генерирования ПП, (n,k) - помехоустойчивом коде. Пусть нарушитель E перехватил по каналу перехвата без ошибок блок проверочных символов u длиной $n-k$ бит. Тогда для нарушителя E энтропия Шеннона не стертого информационного слова длиной k бит равна

$$H_E = \frac{-1}{\sum_{d=0}^{k} C_k^d (\alpha_{11}^d \alpha_{00}^{k-d} + \alpha_{10}^k)} \times$$

$$\times \sum_{d=0}^{k} C_k^d \left(\alpha_{11}^d \alpha_{00}^{k-d} + \alpha_{10}^k \right) \log_2 \left\{ \frac{\alpha_{11}^d \alpha_{00}^{k-d} + \alpha_{10}^k}{\alpha_{11}^d \alpha_{00}^{k-d} + \alpha_{11}^{k-d} \alpha_{00}^d + 2\alpha_{10}^k} \right\},$$

где α_{ij} — совместная вероятность события, при котором информационный символ $x = i$ сгенерирован A и информационный символ $y = j$ сгенерирован B, где $i \in \{0,1\}$ и $j \in \{0,1\}$, определенная в выражении (3).

Доказательство. Обозначим через $|a|$ вес Хемминга (число единиц) блока a длиной k, сохраненного пользователем A. Анализ табл. 1 для используемого (n,k) -помехоустойчивого кода показал, что двум инвертированным информационным словам с весами, равными d и $k-d$, соответствует один и тот же блок проверочных символов (БПС) u. Тогда совместная вероятность события, состоящего в том, что пользователь A принял блок, которому соответствует проверка u, равна

$$P(u,\text{принят}A) = P(|a|=d,u,\text{принят}A)+P(|a|=k-d,u,\text{принят}A) \quad (25)$$

где вероятности $P(|a|=d,u,\text{принят}A)$ и $P(|a|=k-d,u,\text{принят}A)$ определяются из (13).

Подставим в (25) выражение (13) и получим

$$P(u,\text{принят}A)=\alpha_{11}^{d}\alpha_{00}^{k-d}+\alpha_{11}^{k-d}\alpha_{00}^{d}+2\alpha_{10}^{k} \quad (26)$$

где α_{ij} — совместная вероятность события, при котором информационный символ $x=i$ сгенерирован A и информационный символ $y=j$ сгенерирован B, а $i\in\{0,1\}$ и $j\in\{0,1\}$, определенная в выражении (3).

Легко определить, что вероятность события, состоящего в том, что пользователь A принял блок, содержащий d единиц, $|a|=d$, при условии, когда нарушитель E принял БПС u, равна

$$P(|a|=d/u,\text{принят}A)= =\frac{P(|a|=d,u,\text{принят}A)}{P(u,\text{принят}A)}=\frac{\alpha_{11}^{d}\alpha_{00}^{k-d}+\alpha_{10}^{k}}{\alpha_{11}^{d}\alpha_{00}^{k-d}+\alpha_{11}^{k-d}\alpha_{00}^{d}+2\alpha_{10}^{k}} \quad (27)$$

Используя теорему Байеса, получаем следующую вероятность наличия у E БПС u, при условии, что A принял блок a:

$$P(u/\text{принят}A)=\frac{P(u,\text{принят}A)}{P(\text{принят}A)}=\frac{\alpha_{11}^{d}\alpha_{00}^{k-d}+\alpha_{11}^{k-d}\alpha_{00}^{d}+2\alpha_{10}^{k}}{\sum_{d=0}^{k}C_{k}^{d}(\alpha_{11}^{d}\alpha_{00}^{k-d}+\alpha_{10}^{k})} \quad (28)$$

где вероятность $P(\text{ï ðèí ÿò À})$ определяется из (20).

Энтропия Шеннона принятого пользователем A информационного слова a, при условии, что нарушитель E принял БПС u, равна

$$H(u,\text{принят}A) = -\Big\langle P(|a| = d/u,\text{принят}A)\times$$
$$\times\log_2\{P(|a| = d/u,\text{принят}A)\}+$$
$$+P(|a| = k-d/u,\text{принят}A)\log_2\{P(|a| = k-d/u,\text{принят}A)\}\Big\rangle \quad (29)$$

Тогда для нарушителя E энтропия Шеннона не стертого информационного слова длиной k бит равна

$$H_E = \sum_{\forall u} P(u/\text{принят}A)H(u,\text{принят}A) \quad (30)$$

Учитывая, что двум инвертированным информационным словам с весами, равными d и $k-d$, соответствует один и тот же БПС u, выносим общие члены за знак суммирования и, производя сокращения, перепишем (30):

$$H_E = \frac{-1}{P(\text{принят}A)}\sum_{\forall u}\Big[\Big[P(a,u,\text{принят}A)\times$$
$$\times log_2\left\{\frac{P(a,u,\text{принят}A)}{P(a,u,\text{принят}A)+P(\bar{a},u,\text{принят}A)}\right\}+$$
$$+P(\bar{a},u,\text{принят}A)\times \quad (31)$$
$$\times log_2\left\{\frac{P(\bar{a},u,\text{принят}A)}{P(a,u,\text{принят}A)+P(\bar{a},u,\text{принят}A)}\right\}\Big]\Big]$$
$$=\frac{-1}{P(\text{принят}A)}\sum_{\forall a}P(a,u,\text{принят}A)\times$$
$$log_2\left\{\frac{P(a,u,\text{принят}A)}{P(a,u,\text{принят}A)+P(\bar{a},u,\text{принят}A)}\right\}$$

где $\bar{a}$ — инвертированное информационное слово a длиной k бит.

Подставим в (31) выражения (13), (20) и получим

$$H_E = \frac{-1}{\sum_{d=0}^{k} C_k^d(\alpha_{11}^d\alpha_{00}^{k-d}+\alpha_{10}^k)}\times \times\sum_{d=0}^{k} C_k^d\left(\alpha_{11}^d\alpha_{00}^{k-d}+\alpha_{10}^k\right)log_2\left\{\frac{\alpha_{11}^d\alpha_{00}^{k-d}+\alpha_{10}^k}{\alpha_{11}^d\alpha_{00}^{k-d}+\alpha_{11}^{k-d}\alpha_{00}^d+2\alpha_{10}^k}\right\} \quad (3$$

Теорема доказана.

Анализ работ [2–4] показывает что, в случае наличия у нарушителя большей неопределенности (энтропии), чем у легальных пользователей, формирование ключа возможно. Тогда выполнение необходимого условия

$$H_E - H_A > 0 \qquad (33)$$

позволяет утверждать, что если H_A определена согласно теореме 1 и H_E определена согласно теореме 2, то ключевое согласование возможно.

Оценим выполнение условия (33) для интервала $p1 \in [0.9;0.99]$. В табл. 2 сведены вероятности $p1$, значение k — длины в битах принятого информационного слова (n,k) -помехоустойчивого кода КлП, H_E — оценка энтропии Шеннона нарушителя E не стертого информационного слова и оценка разности $H_E - H_A$.

Таблица 2. **Характеристика иртервала вероятностей**

$p1$	k	H_E	$H_E - H_A$
0,9	8	$2{,}459 \cdot 10^{-5}$	$2{,}617 \cdot 10^{-16}$
0,95	6	$6{,}837 \cdot 10^{-6}$	$3{,}177 \cdot 10^{-16}$
0,99	2	$1{,}907 \cdot 10^{-3}$	$2{,}168 \cdot 10^{-19}$

3. Выводы. Анализ табл. 2 показывает, что в исследуемом интервале вероятностей $p1$ формирование ключа возможно при использовании нарушителем канала перехвата без ошибок. Выполнение условия (33) с точки зрения информационно-теоретического подхода определяется наличием у пользователя дополнительного условия, уменьшающего его неопределенность по сравнению с нарушителем. Это знание самим пользователем своего сохраненного (не стертого) кодового слова. В то время когда проверочные биты к нему знают как пользователь, так и нарушитель. При более низких значениях вероятностей $p1$ ключевое согласование возможно при больших длинах k принятого информационного слова (n,k) -помехоустойчивого кода, так как требования по достоверности (совпадению) КлП здесь обеспечить сложнее, чем при более высоких значениях вероятностей $p1$. С увеличением $p1$ разница $H_E - H_A$ увеличивается и уменьшается на несколько порядков при $p1 = 0{,}99$, энтропия нарушителя H_E почти сравнима с энтропией пользователей, так как вероятностное распределение КлП приобретает почти детерминированный характер. Поэтому

разница $H_E - H_A$ достаточно мала. Малая разница $H_E - H_A$ потребует обмена последовательностями большой длины, так, например, для формирования ключа длиной 100 бит при $p1 = 0{,}95$ потребуется передать последовательность длиной порядка $3.147 \cdot 10^{17}$ бит. С точки зрения информационно-теоретического подхода оценки стойкости криптографических систем защиты информации [2–4], построение протокола формирования ключа в таких условиях затруднительно и неконструктивно. Для синтеза протокола необходимы дополнительные предположения, например, об ограниченной вычислительной способности (или емкости запоминающих устройств) нарушителя в рамках сложностно-теоретического подхода или построение модели нарушителя, что характерно для системного подхода [1]. По мнению авторов, цель работы достигнута.

Литература

1. *Молдовян Н. А., Молдовян А. А., Еремеев М. А.* Криптография: от примитивов к синтезу алгоритмов. СПб.: БХВ-Петербург, 2004. 448 с: ил.
2. *Maurer U.* Secret Key Agreement by Public Discussion Based on Common Information // IEEE Trans. on IT. 1993. Vol. 39. P. 733–742.
3. *Csisar I., Korner J.* Broadcast channels with confidential messages// IEEE Trans. on IT. 1978. Vol. 24, N 3. P. 339–348,
4. *Wyner A.* The wire-tap channel // Bell Syst. Techn. J. 1975, Vol. 54, N 8. P. 1355–1387.

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, д. 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.

Козленко Андрей Владимирович — адъюнкт Военной академии связи. Область научных интересов: оценивание и контроль защищенности информации в условиях различного рода неопределенности информации о состоянии защиты, программирование, разработка комплексов программ. Число научных публикаций — 11. et-ak@yandex.ru; Военная академия связи, Тихорецкий проспект, 3, Санкт-Петербург, 194064, РФ; р.т. +7(812)247-9842. Научный руководитель — В.С. Авраменко.

Kozlenko Andrei Vladimirovich — post-graduate student, Military academy of signal communication. Research interests: the information security estimation and control in the various sort of uncertainty information security conditions, programming, complex software development. The number of publications — 11. et-ak@yandex.ru; Military academy of signal com-

munication, Tihoretskiy broad street, 3, St. Petersburg, 194064, Russia; office phone +7(812)247-9842. Scientific adviser — V.S. Avramenko.

Чирушкин Константин Анатольевич — адъюнкт Военной академии связи. Область научных интересов: автоматизация контроля уровня знаний. Число научных публикаций — 6. cka83@yandex.ru; Военная академия связи, Тихорецкий проспект, 3, Санкт-Петербург, 194064, РФ; р.т. +7(812)247-9842. Научный руководитель — В.Ф. Щетка.

Chirushkin Konstantin Anatol'evich — post-graduate student, Military academy of signal communication. Research interests: Automation of the knowledge level control. The number of publications — 6. cka83@yandex.ru; Military academy of signal communication, Tihoretskiy broad street, 3, St. Petersburg, 194064, Russia; office phone +7(812)247-9842. Scientific adviser — V.F. Schetka.

Рекомендовано лабораторией проблем компьютерной безопасности, заведующий лабораторией д-р техн.наук, проф. И.В. Котенко.
Статья поступила в редакцию 22.11.2010.

РЕФЕРАТ

Синюк А.Д., Козленко А.В., Чирушкин К.А. **Информационно-теоретическая модель формирования ключа по открытым каналам без ошибок.**

В статье предлагается информационно-теоретическая модель формирования неопределенностей легальных пользователей и нарушителя.

Общая постановка задачи сводится к следующему: необходимо сформировать ключевые последовательности (КлП) (из которых затем вырабатывается общий ключ) для легальных пользователей, осуществляя обмен данными между ними по двунаправленному каналу без ошибок доступному нарушителю по безошибочному каналу перехвата. При этом требуется обеспечить формирование КлП с высокой достоверностью для пользователей (минимальную неопределенность для пользователей) и обеспечить заданное малое количество информации о КлП для нарушителя (максимальную неопределенность для нарушителя). Предполагается, что нарушитель пассивен.

Предложенная информационно-теоретическая модель включает в себя: модель канальной связности легальных пользователей и нарушителя, алгоритм генерирования ПП легальных пользователей, код с обнаружением ошибок. Модель канальной связности легальных пользователей и нарушителя всеобъемлюще описывает легальных пользователей, нарушителя и каналы связи между ними. Алгоритм генерирования ПП легальных пользователей позволяет сформировать их без передачи по каналу связи. Код с обнаружением ошибок используется для устранения несовпадений ПП.

Анализ известных работ в области ключевого согласования показывает, что, в случае наличия у нарушителя большей неопределенности (энтропии), чем у легальных пользователей, формирование ключа возможно. Однако в исследуемой модели получено малое преимущество в неопределенности легальных пользователей по сравнению с нарушителем, что потребует обмена последовательностями большой длины. С точки зрения информационно-теоретического подхода оценки стойкости криптографических систем защиты информации, построение протокола формирования ключа в таких условиях затруднительно и неконструктивно. Для синтеза протокола необходимы дополнительные предположения, например, об ограниченной вычислительной способности (или емкости запоминающих устройств) нарушителя в рамках сложностно-теоретического подхода или построение модели нарушителя, что характерно для системного подхода.

SUMMARY

Sinjuk A.D., Kozlenko A.V., Chirushkin K.A. **Informational-theoretical model of key sharing based on noiseless public channels.**

In paper the informational-theoretical model of formation uncertainty legal users and eavesdropper is offered.

Common setting of the task is reduced to the following: it is necessary to generate key sequences (KS) (from which the common key is worked out then) for legal users, realizing data exchange between them on the bidirectional noiseless channel, which is accessible to eavesdropper on the faultless channel of interception. Thus it is required to ensure creation KS with high reliability for users (minimum ambiguity for users) and to ensure a preset small information content about KS for the eavesdropper (maximum ambiguity for the eavesdropper). It is supposed, that the eavesdropper is passive.

The offered informational-theoretical model includes: model of channel connectivity of legal users and the eavesdropper, algorithm of a primary sequences generating for legal users, an error-detecting code. The model of channel connectivity of legal users and the eavesdropper comprehensively describes legal users, the eavesdropper and data links between them. The algorithm of a primary sequences generating for legal users allows to generate them without transmission on a data link. The error-detecting code uses for incongruities elimination of primary sequences.

The analysis of known operations in the field of the key matching shows that, in case of presence for the eavesdropper greater ambiguity (entropy), than for legal users, key creation probably. However in researched model small advantage is got in ambiguity of legal users in comparison with the eavesdropper that will demand an sequences interchanging of larger length. From the point of view of the informational-theoretical approach of cryptography information security systems firmness estimation, construction of the key creation protocol a in such conditions inconveniently and was not constructively. Additional suppositions are necessary for protocol synthesis, for example, about the limited computing ability (or sizes of storage devices) the eavesdropper within the limits of the complexity-theoretical approach or construction of eavesdropper model that is characteristic of a system approach.