УДК 004.056.5 DOI 10.15622/ia.22.4.1

А.Д. СИНЮК, О.А. ОСТРОУМОВ, А.А. ТАРАСОВ

ТЕОРЕТИКО-ИНФОРМАЦИОННОЕ ПРЕДСТАВЛЕНИЕ ВИРТУАЛИЗАЦИИ СЕТЕВОГО КАНАЛА ПЕРЕХВАТА

Синюк А.Д., Остроумов О.А., Тарасов А.А. **Теоретико-информационное представление виртуализации сетевого канала перехвата.**

Аннотация. Сложнейшей задачей защищенных телекоммуникационных систем, использующих симметричное шифрование, в связи с необходимостью предварительной и ресурсоемкой организации секретных каналов доставки ключей сетевым корреспондентам, является управление ключами. Альтернативой выступают методы формирования ключей по открытым каналам связи. В теории информации показано, что эти методы реализуются при условии превышения информационной скорости канала корреспондентов над скоростью канала перехвата нарушителя. Актуализируется поиск методов, обеспечивающих получение информационного преимущества корреспондентов. Цель заключается в определении теоретико-информационных условий формирования виртуальных сети и канала перехвата, для которых обеспечивается лучшее у корреспондентов отношение информационных скоростей по сравнению с отношением исходных сети и канала перехвата. В работе предлагается модель передачи информации, включающая модель связности и метод передачи информации для асимптотических длин кодовых слов. Модель включает трех корреспондентов и отличается введением идеального широковещательного канала в дополнение к широковещательному каналу с ошибками. В модели введен источник «зашумляющей» информации, которая передается по каналу с ошибками, поэтому передача кодовых слов с использованием известного метода случайного кодирования производится по каналу без ошибок. Для асимптотических длин кодовых слов все действия корреспондентов по обработке и передаче информации в модели сведены в предлагаемый метод передачи информации. Использование метода корреспондентами в рамках модели передачи позволяет одновременно сформировать для них новый виртуальный широковещательный канал с информационной скоростью, как и в первоначальном канале с ошибками, а для нарушителя новый виртуальный широковещательный канал перехвата со скоростью меньшей информационной скорости первоначального канала перехвата. Теоретико-информационные условия ухудшения канала перехвата доказывается в утверждении. Практическая значимость полученных результатов заключается в возможности использования последних для оценки информационной эффективности открытого сетевого формирования ключей в предложенной модели передачи информации, а также в развитии известных научных достижений открытого ключевого согласования. Предлагаемая модель передачи может быть полезной для проведения исследований систем управления ключами и защиты информации, передаваемой по открытым каналам. Дальнейшие исследования связаны с теоретико-информационной оценкой сетевой ключевой пропускной способности, представляющей собой потенциальную теоретико-информационную скорость формирования сетевого ключа.

Ключевые слова: модель передачи информации в сети связи, сетевой корреспондент, нарушитель, источник «шумовой» последовательности, виртуальный канал перехвата, метод передачи информации для асимптотических длин кодовых слов.

1. Введение.

Одной из сложных задач криптографических телекоммуникационных систем, использующих симметричные

шифры, является задача управления ключами, обусловленная предварительной организацией секретного для нарушителя канала доставки ключей корреспондентам [1]. В настоящее время задача решается с использованием защищенных каналов связи, что дорого, не оперативно и не всегда возможно. Обнаруженная компрометация ключа нарушителем приводит к существенным временным задержками информации. В условиях функционирования защищенных сетей связи на едином ключе вероятность компрометации увеличивается с увеличением корреспондентов, что приводит к увеличению времени простоя, связанного с большим временем организации доставки нового ключа всем корреспондентам [2].

Уменьшение информационных задержек возможно с использованием методов формирования сетевого ключа по доступным открытым каналам связи. Исследования в области теории информации [3] показали, что предпосылкой к успешной реализации метода открытого ключевого согласования является выполнение условия превышения информационной скорости канала корреспондентов над скоростью канала перехвата нарушителя. Это актуализирует поиск методов, обеспечивающих получение информационного преимущества корреспондентов. Другими словами, необходимо выполнить поиск условий, при которых обеспечивается преимущество по качеству канала(ов), который используют корреспонденты для формирования общего ключа над каналом перехвата информации, утекающей к нарушителю. Поэтому исследованию модели канала перехвата (КП) в процессе открытого ключевого согласования уделяется большое внимание. Так, например, в ходе выполнения метода распределения ключей для пары корреспондентов по квантовым каналам связи [4] применение поляризованных фотонов, позволяет получить эффект, который нельзя достичь при использовании обычных средств передачи информации. Используя принцип неопределенности Гейзенберга, можно получить канал, в котором затруднен перехват нарушителем без наличия нарушений при передаче-приеме информационного фотона корреспондентами. Одной из атак нарушителя является перехват-ретрансляция поляризованного фотона, которая может быть обнаружена корреспондентами с некоторой вероятностью. В зависимости от результатов измерения нарушений корреспонденты могут отказаться или принять сеанс формирования ключа. В другом известном методе «Модели источника» [5] формирование ключа между парой корреспондентов становится возможным, если качество одного из каналов от источника к одному из корреспондентов лучше качества КП

от источника к нарушителю. Для дискретных, в том числе двоичных, каналов связи под термином «качество канала» следует понимать вероятность ошибки в канале [3]. В качестве третьего примера выступает метод формирования сетевого ключа [6], для которого возможность формирования сетевого ключа (СКЛ) обеспечивается при выполнении условия превышения числового значения вероятности ошибки КП над числовым значением суммы вероятностей ошибок в каналах связи между сетевыми корреспондентами (СК). Ужесточение требований по качеству КП связано с необходимостью формирования СКЛ по сравнению с предшествующим примером.

Цель работы заключается в определении теоретико-информационных условий формирования виртуальных сети и канала перехвата, для которых обеспечивается лучшее для корреспондентов отношение информационных скоростей по сравнению с отношением исходных сети и канала перехвата. Круг проблем, составляющих основное содержание теории информации [7], можно охарактеризовать как исследование методов кодирования для экономного представления сообщений различных источников и для надежной передачи сообщений по каналам связи с шумом основанное на статистическом описании источников сообщений, каналов связи и измерении количества информации между сообщениями по Шеннону [3]. Тогда целевые искомые теоретико-информационные условия определяются построением модели передачи информации (МПИ) в сети связи (СС), описывающей формирование информационного преимущества корреспондентов СС. Разработка МПИ определяется задачей построения модели связности (МС) в СС, включающей источники информации и каналы связи как идеальные, так и с ошибками. Разработка только МС не позволяет достигнуть цели исследования, поэтому в качестве второй задачи представляется разработка метода передачи информации (МтПИ) для асимптотических длин кодовых слов (КС), определяющего действия корреспондентов по обработке и передаче информации в МПИ. В качестве основного метода исследования используются теория информации.

В результате исследований построена новая МПИ включающая МС и МтПИ. Первая компонента включает трех СК и нарушителя (Нр). В рамках МС производится передача информации по совокупности широковещательных каналов связи [8] с ошибками и без ошибок таким образом, что в результате для корреспондентов формируются новый виртуальный широковещательный канал (ШВК) с качеством равным первоначальному каналу. Для нарушителя формируется новый виртуальный канал перехвата, значительно

уступающий своему первоначальному образу по количеству информации на своем выходе. Произведена постановка задачи. Обмен информацией основан на известных моделях случайного кодера и детерминированного декодера [6], функционирующих в новых условиях взаимосвязи с введенным источником «зашумляющей» информации. Разработан асимптотический МтПИ. Математически строго доказано утверждение об отсутствии информационных потерь в виртуальном широковещательном канале корреспондентов и их наличии в виртуальном канале перехвата. Для СС описываемой моделью двоичного ШВК показано условие по качеству каналов, выполнение которого обеспечивает достижение цели исследования.

Научная новизна полученных результатов определяется построением новой МПИ в СС, определяющей теоретико-информационные условия формирования виртуальных ШВК и КП, для которых обеспечивается информационный выигрыш для корреспондентов.

Практическая значимость результатов определяется предметом теории информации [3], сущность которого заключается в доказательстве теорем, устанавливающих предельные возможности различных методов обработки и передачи сообщений.

Практическая значимость заключается в создании условий для оценки предельного значения информационной эффективности открытого сетевого формирования ключей в предложенной МПИ СС, а также в развитии известных научных достижений открытого ключевого согласования [1, 4, 5, 6]. Кроме этого, МПИ может быть полезной для проведения исследований систем управления ключами и защиты информации, передаваемой по открытым каналам. Дальнейшие исследования связаны с теоретико-информационной оценкой сетевой ключевой пропускной способности, представляющей собой потенциальную теоретико-информационную скорость формирования сетевого ключа.

Логика проведенного исследования определяет структуру статьи. В постановке задачи предлагается МПИ в СС, которая декомпозируется на новые МС и МтПИ. Для описания передачи информационных последовательностей асимптотических длин в теории информации используется случайное кодирование [9], поэтому предлагаются известные модели случайного кодера и детерминированного декодера [6] с описанием особенностей использования. Для вышеописанных условий предлагается МтПИ определяющий порядок передачи и обработки информационных последовательностей асимптотических длин. Особенность модели нарушителя [6] заключается в наличии

дополнительного КП без ошибок в целях контроля идеального ШВК. В дальнейшем на основе анализа предложенной МПИ описывается процесс формирования виртуальных ШВК и КП. Формулируется и доказывается утверждение о формировании информационного преимущества виртуального ШВК над виртуальным КП. Произведенный анализ результатов доказательства утверждения позволяет определить требуемое условие по качеству исходных ШВК и КП. Обобщение полученных результатов, их значимость, а также направления дальнейших исследований приведены в заключении.

2. Постановка задачи. Требуется разработать модель передачи информации по открытым каналам сети связи, в которой относительно передаваемой информационной последовательности асимптотической длины качество формируемого в процессе передачи виртуального КП ухудшается относительно качества канала перехвата нарушителя до передачи информации, а качество одновременно формируемых виртуальных открытых каналов сетевых корреспондентов остается неизменным относительно качества открытых каналов СС до передачи информации. С другой точки зрения теории информации реализация этого требования определяет формирование виртуальных сети и КП, для которых обеспечивается лучшее для корреспондентов отношение информационных скоростей по сравнению с отношением исходных сети и канала перехвата.

Для этого предлагается новая МПИ в СС включающая ряд компонент, основными из которых являются МС и МтПИ. Опишем связности предлагаемой МС сети связи, показанной на рисунке 1.

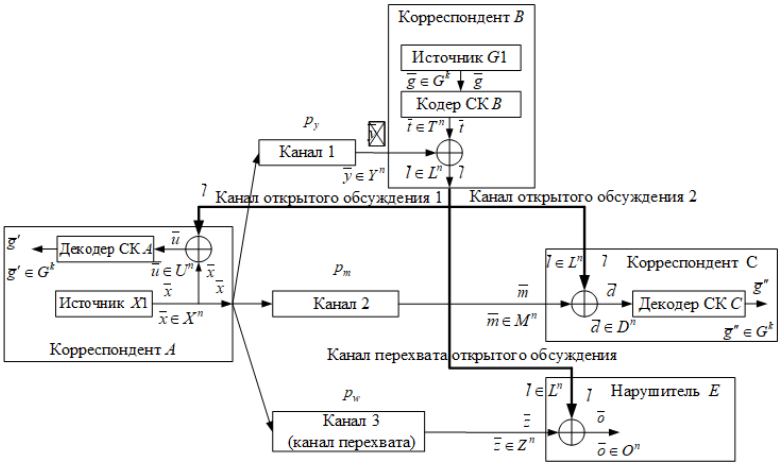

Рис. 1. Модель связности СК *A, B, C* и нарушителя *E*

Корреспондент *A* имеет источник «шумовой» последовательности. Выход источника связан с первым входом сумматора по модулю 2 (СМ2) и входом ШВК (входами двух независимых составляющих каналов ШВК, описываемых моделями двоичных симметричных каналов связи (ДСК) с ошибками [3]). Канальная связность сетевых корреспондентов в СС описывается моделью двухсоставного широковещательного канала связи [10]. С выходов составляющих каналов сигналы поступают на первые входы СМ2 СК *B*, *C*. Выход ШВК контролируется нарушителем *E* посредством КП, описываемого моделью ДСК. Выход КП связан с первым входом СМ2 нарушителя. У корреспондента *B* имеется источник сообщений *G1*. Выход *G1* связан с входом случайного кодера (СлК). Выход СлК связан со вторым входом СМ2 СК *B*. Выход СМ2 СК *B* с входом безошибочного ШВК (ШВКбо). В направлении от СК *B* к СК *A* и *C* имеется ШВКбо, включающий два составных канала, описываемых моделями ДСК без памяти [3], в которых отсутствуют ошибки. Назовем эти каналы – каналами открытого обсуждения (КОО) и обозначим КОО-1, КОО-2, соответственно. Выход КОО-1 связан со вторым входом СМ2, а выход СМ2 связан входом детерминированного декодера (ДД) СК *A*. Выход КОО-2 связан с вторым входом СМ2, а выход СМ2 связан входом ДД СК *C*. Выход ШВКбо контролируется Нр *E* посредством канала утечки информации, который описывается моделью ДСК без ошибок. Назовем его каналом перехвата открытого обсуждения (КПОО). Выход КПОО связан со вторым входом СМ2 нарушителя.

Кратко опишем элементы МС. Пусть первая компонента – источник «шумовой» последовательности $X1$ описывается моделью двоичного стационарного источника без памяти [11] и задается ансамблем $\{X, p(x)\}$. Алфавит задается множеством X и состоит символов $X = \{0,1\}$, и в каждую единицу времени независимо выбирает i -ю букву x_i из алфавита с одинаковой вероятностью $p(x_i) = 0,5$. Источник генерирует сообщение $\overline{x}$, представляющее двоичную последовательность длиной n, причем $\overline{x} \in X^n$, где X^n – декартова n -я степень множества X [11].

Второй элемент МС – совокупность, состоящая из двух каналов с общим входом (выход источника $X1$, который находится у СК *A*) и выходами (входы сумматоров СК *B* и *C*), описывается моделью двоичного ШВК с двумя составляющими каналами связи с ошибками. Передача символов по ШВК определяется общим алфавитом X, выходными двоичными алфавитами Y и M и матрицами переходных

вероятностей $P_1 = \{p(y/x)\}, P_2 = \{p(m/x)\}, x \in X, \quad y \in Y, m \in M.$ Первый составляющий канал (СтК1) описывается моделью ДСК с вероятностью ошибки p_y, а второй (СтК2) – ДСК с p_m.

Третья компонента – канал перехвата, который представляет собой канал связи от выхода источника $X1$ СК A и выходом на входе СМ2 нарушителя E. Передача сигналов по КП определяется двоичными входным алфавитом X, выходным алфавитом Z и матрицей переходных вероятностей $P_3 = \{p(z/x)\}, x \in X, z \in Z$. КП описывается моделью ДСК с вероятностью ошибки p_w. Составляющие каналы ШВК и КП являются каналами с независимыми ошибками [3].

Четвертый элемент – источник сообщений $G1$ СК B описывается моделью двоичного стационарного источника без памяти. Алфавит источника задается множеством G и состоит из двух букв $G = \{0,1\}$. Пусть источник в каждую единицу времени независимо выбирает i-ю букву из алфавита с равной вероятностью $p(g_i) = 0,5$. Источник задается ансамблем $\{G, p(g)\}$. Источник генерирует сообщение $\overline{g}$, представляющее собой случайную двоичную последовательность длиной k символов источника, причем $\overline{g} \in G^k$.

Пятая составляющая МС – ШВКбо. Пусть вход ШВКбо СК B описывается множеством L^n, где L – двоичный алфавит входа. Пусть выход первого составляющего канала КОО-1 у СК A описывается множеством U^n, где U – двоичный алфавит выхода КОО-1. Пусть выход второго составляющего КОО-2 СК C описывается множеством D^n, где D – двоичный алфавит выхода второго составляющего канала КОО-2. Определим последовательности на входе ШВКбо $\overline{l}$, причем $\overline{l} \in L^n$, и выходе КОО-1 – $\overline{u}$, причем $\overline{u} \in U^n$, и выходе КОО-2 – $\overline{d}$, причем $\overline{d} \in D^n$.

Дополнительно у СК и Нр имеются СМ2 [3]. Выход СМ2 равен символу «1», если на его вход поступают различающие символы, иначе равен «0». Описание моделей СлК и ДД приведено ниже. В отличие от известных [6] в предлагаемой МС используется расположение СлК у СК B и ДД у СК A, поэтому введены модели ШВКбо и КПОО.

Общая постановка задачи: необходимо синтезировать и исследовать условия и порядок действий СК в процессе передачи

информации с постоянной скоростью по открытым каналам СС, описываемой совокупностью моделей ШВК и ШВКбо, обеспечивающие уменьшение информационной скорости передачи на выходе виртуального канала перехвата нарушителя, формируемого в процессе передачи.

Особенности моделей случайного кодера и детерминированного декодера. Информационная последовательность $\overline{g}, \overline{g} \in G^k$, переданная по ШВК, не может быть использована СК, т.к. может содержать ошибочно принятые символы. Это требует коррекции (отображения) принятых последовательностей в декодированные информационные последовательности: $\overline{u} \mapsto \overline{g}'$, где $\overline{g}' \in G^k$ для СК A и $\overline{d} \mapsto \overline{g}''$, где $\overline{g}'' \in G^k$ для СК C. Методология теории информации определяет, что при построении кода рассматриваются только такие коды, для которых кодер является тождественным отображением на множестве кодовых слов [5]. В таком случае коды задаются множествами кодовых слов и декодирующими отображениями, а не кодерами и декодерами, как это использовалось в [12]. Пусть задано достаточно большое n ($n \to \infty$). Необходимо выбрать код, с помощью которого производится передача информации. Для передачи информации используем модель случайного кодера, предложенного в [6] с особенностью его использования заключающуюся в том, что для формирования «виртуальных» каналов выход его связан не с входом ШВК с ошибками, как показано в [6], а с входом ШВК без ошибок у СК B и расположения ДД у СК A. Другая особенность связана с тем, что случайный кодер использует «двоичный вектор ошибок» длиной n [3] ШВК для формирования зашумленного кодового слова, а ДД у СК A и C сначала снимают «зашумление» и только потом декодируют принятые сообщения.

Кратко опишем модель СлК. Выберем из T^n множество кодовых слов V, причем V представляет высоковероятное множество типичных последовательностей [3] и задает на T^n некоторый (n, ε_1) код со скоростью R [13] удовлетворяющей условию для $\tau, \tau > 0$:

$$R < F(X;Y;M) - \tau, \tag{1}$$

где $F(X;Y;M)$ – совместная информация (СИ) ШВК [14].

С учетом (1) мощность J множества V не превышает 2^{nR}.

В соответствии с прямой теоремой кодирования ШВК [14] для (n, ε_1) кода обеспечивается средняя вероятность ошибочного декодирования не более ε_1, причем $\varepsilon_1 > 0$. Разделим V на M_0 непересекающихся подмножеств C_i (кодовых множеств), где $i = 1, 2, ..., \mathrm{M}_0$, равной мощности $D1$:

$$D1 = \frac{J}{\mathrm{M}_0}, \tag{2}$$

где M_0 – число последовательностей $G1$:

$$\mathrm{M}_0 = 2^k. \tag{3}$$

В соответствии теоремой о высоковероятных множествах [3] для $n \to \infty$ вероятности элементов V почти равны. Вероятность V близка к 1, т.е. для малого ρ, где $\rho > 0$, $P(V)$ удовлетворяет условию:

$$P(V) > 1 - \rho. \tag{4}$$

Тогда вероятности элементов C_i также близки друг к другу. Выражение (4) означает, что для любой $\overline{t}$, где $\overline{t} \in T^n$, с вероятностью:

$$p(\overline{t} \in C_i) \geq \rho, \tag{5}$$

найдется C_i, причем $\overline{t} \in C_i$. Тогда $\overline{g}_i \mapsto C_i$.

Кодирование. Пусть на выходе $G1$ появляется $\overline{g}_i$. Кодер с вероятностью (5) выбирает C_i. Затем с равной вероятностью выбирает кодовое слово $\overline{t}$, где $\overline{t} \in C_i$, и отправляет $\overline{t}$ на вход ШВКбо. Кодирование задает распределение на T^n:

$$p(\overline{t}) = \begin{cases} \dfrac{p(\overline{g}_i)}{D1}, \ \forall\ \overline{t} \in C_i; \\ 0, \ \forall\ \overline{t} \notin \bigcup\limits_{i=1}^{\mathrm{M}_0} C_i, \end{cases}, \tag{6}$$

где $D1$ определяется из (2), а M_0 из (3).

Особенность схем декодирования заключается в том, что ДД своим входом связаны через СМ2, в котором суммируются выход ШВКбо с выходом ШВК.

Декодирование. СК A и C известны C_i, которые выбирают в качестве соответствующих решающих областей $S_i \subseteq U^n, Q_i \subseteq D^n, i = 1,...,\mathrm{M}_0$. Пусть $V1$ – ансамбль решений ДД СК A. Каждая $\overline{u} \in U^n$ определяет решение $v \in V1$ по правилу:

$$v = \begin{cases} v_i, \ \forall \ \overline{u} \in S_i; \\ v_{\mathrm{M}_0+1}, \ \forall \ \overline{u} \notin \bigcup\limits_{i=1}^{\mathrm{M}_0} S_i. \end{cases} \quad (7)$$

Решение v_i в (7) принимается с вероятностью (4). Решение v_{M_0+1} связано с отказом от декодирования. По аналогии пусть W – ансамбль решений ДД СК B. Каждая $\overline{d} \in D^n$ определяет решение $w \in W$ по правилу:

$$w = \begin{cases} w_i, \forall \overline{d} \in Q_i, ; \\ w_{\mathrm{M}_0+1}, \forall \overline{d} \notin \bigcup\limits_{i=1}^{\mathrm{M}_0} Q_i. \end{cases} \quad (8)$$

Решение w_i в (8) принимается с вероятностью (4), которая больше $(1-\rho)$. Решение w_{M_0+1} определяет отказ от декодирования.

Вероятность одновременного правильного декодирования $\overline{u}$ и $\overline{d}$ превышает величину $(1-\rho)^2 - \varepsilon_1$.

Метод передачи информации для асимптотических длин кодовых слов. Введем символ $\overline{\oplus}$, который обозначает поразрядное суммирование по модулю 2 двух двоичных последовательностей одинаковой длины. В общем виде метод для достаточно большого n представляет следующую последовательность действий:

1. СК A с использованием $X1$ случайно выбирает «шумовую» $\overline{x}$. асимптотической длины n, причем $\overline{x} \in X^n$, $n \to \infty$.
2. СК A подает $\overline{x}$ на вход ШВК и передает СК B, C.

3. СК *B* принимает на выходе СтК1 ШВК $\overline{y}$ длины *n*, причем $\overline{y} \in Y^n$. СК *C* принимает на выходе СтК2 – $\overline{m}$ длины *n*, причем $\overline{m} \in M^n$.

4. СК *B* с использованием *G*1 случайно выбирает информационную последовательность $\overline{g}_i$ асимптотической длины *k*, причем $k \to \infty$, $\overline{g}_i \in G^k$, $i = 1,..., \mathrm{M}_0$.

5. СК *B* кодирует (n, ε_1) кодом со скоростью *R*, определенной в (1) $\overline{g}_i$ и формирует по закону (6) кодовое слово $\overline{t}$ длины *n*, причем $\overline{t} \in V$.

6. СК *B* поразрядно суммирует по модулю 2 в сумматоре $\overline{t}$ и $\overline{y}$ и получает последовательность «зашумленного» кодового слова $\overline{l}$ длины *n*:

$$\overline{l} = \overline{y} \oplus \overline{t}. \tag{9}$$

7. СК *B* подает $\overline{l}$ на вход ШВКбо и передает к СК *A*, *C*.

8. СК *A* принимает на выходе КОО-1, а СК *C* на выходе КОО-2 «зашумленное» кодовое слово $\overline{l}$.

9. СК *A* снимает зашумление с $\overline{l}$ путем поразрядного суммирования $\overline{l}$ с $\overline{x}$ и получает двоичную принятую последовательность $\overline{u}$ длины *n*, причем $\overline{u} \in U^n$:

$$\overline{u} = \overline{x} \oplus \overline{l}. \tag{10}$$

По аналогии СК *C* снимает зашумление с $\overline{l}$ посредством $\overline{m}$ и получает двоичную принятую последовательность $\overline{d}$ длины *n*, причем $\overline{d} \in D^n$:

$$\overline{d} = \overline{m} \oplus \overline{l}. \tag{11}$$

10. По правилу декодирования (7) СК *A* с вероятностью более, чем $1 - \rho$ выносит решение о сообщении $\overline{g}'$ длины *k*, причем $\overline{g}' \in G^k$. В противном случае выносит решение об отказе от декодирования. СК *C* по аналогии с вероятностью более $1 - \rho$ по правилу (8) выносит

решение о сообщении $\overline{g}''$ длины k, причем $\overline{g}'' \in G^k$. Иначе выносит решение об отказе от декодирования.

Модель нарушителя. Выше показано, что перехват информационного обмена в СС производится Нр посредством моделей КП и КПОО. Предполагается, что, как и в [6], нарушитель придерживается пассивной стратегии и может только контролировать информацию на выходах КП и КПОО. Использование Нр активной стратегии, когда он создает информацию и может обмениваться ею с СК описаны в [15]. Дополнительно предполагается, что нарушитель знает полное описание выбранного кода (n, ε_1) и источников $X1$ и $G1$, последовательность и содержание всех действий, выполняемых СК по передаче информации в СС.

Рассмотрим перехватываемую информацию Нр на основе анализа шагов вышеописанного метода передачи. На втором и третьем шагах Нр E наблюдает версию «шумовой» последовательности $\overline{x}$ на выходе КП и принимает на выходе КП последовательность $\overline{z}$, причем $\overline{z} \in Z^n$. На седьмом и восьмом шагах Нр E наблюдает и принимает «зашумленное» кодовое слово $\overline{l}$ на выходе КПОО. Зашумленная передача информации, используемая СК посредством предлагаемого метода передачи информации в СС, создает условия для формирования виртуального канала перехвата Нр [16]. Знание Нр $\overline{z}$ не увеличивает его информацию о передаваемой СК B информационной последовательности $\overline{g}$, т.к. они формируются и передаются независимо разными СК. Знание нарушителем «зашумленного» кодового слова $\overline{l}$ оставляет его информацию о переданном кодовом слове на нулевом уровне, т.к. согласно (9) $\overline{l}$ представляет собой сумму $\overline{t}$ и $\overline{y}$, причем слагаемое $\overline{y}$ в сумме играет роль шума с максимальной собственной энтропией [17]. Это с точки зрения теории информации максимально зашумляет кодовое слово $\overline{t}$ длины n. В [18] доказано, что при таких условиях оптимальной обработкой нарушителя E будет суммирование $\overline{l}$ с $\overline{z}$ для снятия случайного «зашумления» с переданного кодового слова:

$$\overline{o} = \overline{z} \oplus \overline{l} . \qquad (12)$$

В результате E получает принятую последовательность $\overline{o}$, причем $\overline{o} \in O^n$. После выполнения СК предлагаемого МтПИ и Нр вышеописанной обработки имеющейся у него информации действий

из первоначальной модели связности формируется модель «виртуальной» связности, соединяющей выход источника сообщений *G1* СК *B* с входами декодеров СК *A*, *C* (и нарушителя *E*), посредством «виртуальных» ШВК и КП с «виртуальными ошибками».

3. Формирование виртуальных каналов. Исследуем, к каким преобразованиям в МС привело использование вышеописанного МтПИ. Для описания передачи в ШВК обозначим $\overline{e}_y$ – вектор ошибок [3] (длиной n двоичных символов) в СтК1 ШВК, причем e_y – двоичный символ ошибки $\overline{e}_y$, который равен «1» с вероятностью $p\left(e_y = 1\right) = p_y$. Для СтК2 обозначим $\overline{e}_m$ как вектор ошибок длиной n, причем e_m – двоичный символ ошибки $\overline{e}_m$, который равен «1» с вероятностью $p\left(e_m = 1\right) = p_m$. Для описания перехвата в КП по аналогии обозначим $\overline{e}_w$ как вектор ошибок длиной n, причем e_w – двоичный символ ошибки $\overline{e}_w$, который равен «1» с вероятностью $p\left(e_w = 1\right) = p_w$. Определим взаимосвязь входа ШВК с его выходами и выходом КП на третьем шаге предлагаемого МтПИ:

$$\overline{y} = \overline{x} \,\overline{\oplus}\, \overline{e}_y,$$

$$\overline{m} = \overline{x} \,\overline{\oplus}\, \overline{e}_m, \tag{13}$$

$$\overline{z} = \overline{x} \,\overline{\oplus}\, \overline{e}_w.$$

Исходя из (13), можно определить, как связаны $\overline{y}$ и $\overline{m}$:

$$\overline{m} = \overline{y} \,\overline{\oplus}\, \overline{e}_y \,\overline{\oplus}\, \overline{e}_m. \tag{14}$$

На шестом шаге МтПИ СК *B* формирует $\overline{l}$, для которого с использованием (9) и (13) запишем:

$$\overline{l} = \overline{x} \,\overline{\oplus}\, \overline{e}_y \,\overline{\oplus}\, \overline{t}. \tag{15}$$

На девятом шаге СК *A* формирует $\overline{u}$, для которой на основе (10) и (15) получаем:

$$\overline{u} = \overline{t} \oplus \overline{e}_y . \tag{16}$$

СК *C* формирует $\overline{d}$, для которой из (11), (13) и (15) получаем:

$$\overline{d} = \overline{t} \oplus \overline{e}_y \oplus \overline{e}_m . \tag{17}$$

Нарушитель *E* формирует $\overline{o}$, для которой из (12), (13) и (15) получаем:

$$\overline{o} = \overline{t} \oplus \overline{e}_y \oplus \overline{e}_w . \tag{18}$$

Анализ преобразований (14), (15), (16), (17), (18) в процессе передачи информации в СС показывает, что исходные ШВК и КП в МС, представленные на рисунке 2(а), преобразуется использованием ШВКбо и КПОО к виртуальным ШВК и КП, которые показаны на рисунке 2(б). В итоге формируется виртуальная МС.

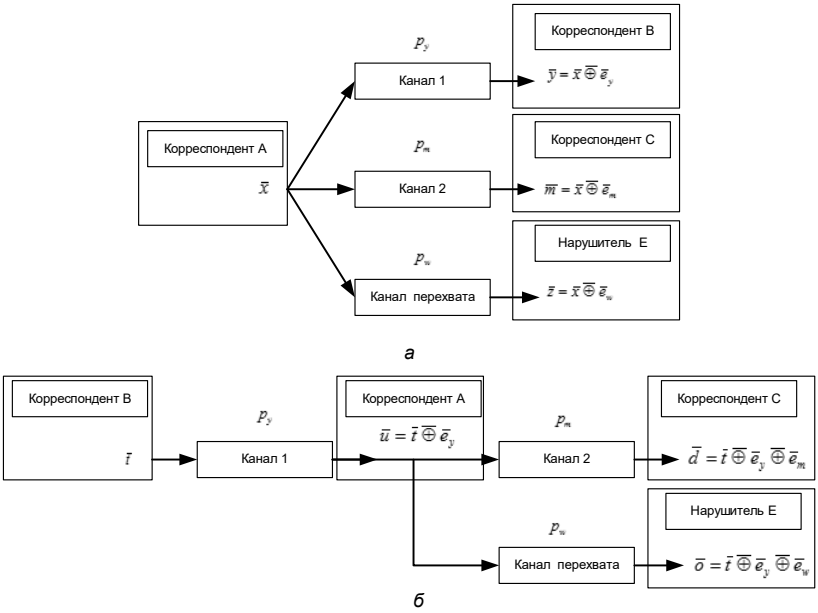

Рис. 2. Переход: а) исходных ШВК и КП; б) к «виртуальным» ШВК и КП

Анализ виртуальной модели связности на рисунке 2 показывает, что в ней, как и в первоначальной МС, имеется ШВК с ошибками, связывающий СК. Такой ШВК описывается моделью ухудшающимся широковещательным каналом (УШВК) [19]. В модели УШВК и в первоначальной модели ШВК первые составляющие ДСК каналы совпадают, а вот второй составляющий канал УШВК (между СК *B* и *C*) является ухудшенным вариантом первого составляющего канала УШВК, т.к. в его состав дополнительно входит второй составляющий канал ШВК. Ниже показано, что формирование виртуального ШВК не приводит к потере информации в процессе передачи меду СК. В отношении виртуального КП можно сказать, что в нем произошли изменения по сравнению с его первоначальным вариантом. Теперь виртуальный КП (ВКП) описывается моделью УШВК, у которого первым составляющим каналом является первый составляющий канал ШВК, а второй составляющий канал является ухудшенным вариантом первоначального КП. Ниже, в Утверждении, показано, что использование СК МтПИ приводит к потере передаваемой информации между СК *B* и нарушителем *E* по сравнению с первоначальным количеством передаваемой информации между СК *A* и *E* (если дополнительно не использовать ШВКбо, как ранее показано в [6]). Это определяет целесообразность использования предлагаемого МтПИ в МС.

Утверждение. Пусть СК используют для передачи информации вышеописанный МтПИ в рамках МС с равномерным распределением символов на совмещенном входе формируемых УШВК и ВКП, тогда между информационными мерами до использования МтПИ и после его использования устанавливаются следующие соотношения:

$$\max_{\{p(t)\}} \; I\left(T;D\right) = \max_{\{p(x)\}} \; F\left(X;Y;M\right), \tag{19}$$

$$\max_{\{p(t)\}} \; I\left(T;O\right) \le \max_{\{p(x)\}} \; I\left(X;Z\right), \tag{20}$$

причем равенство в (20) достигается при $p_y = 0$ и где $F\left(X;Y;M\right)$ – совместная информация между входом и выходами канала ШВК [14], $I\left(T;D\right)$ – взаимная информация между входом и выходом второго составляющего канала УШВК [20], $I\left(X;Z\right)$ – взаимная информация между входом и выходом первоначального КП, $I\left(T;O\right)$ – взаимная

информация между входом и выходом ВКП нарушителя.

Доказательство.

Совместная информация $F(X;Y;M)$ ШВК [14] равна:

$$F(X;Y;M) = I(Y;M), \tag{21}$$

где $I(Y;M)$ – взаимная информация между ансамблями Y и M.

Используя (14) и (21) учитывая равномерный закон распределения вероятностей на входе ШВК с ошибками можно записать для $F(X;Y;M)$:

$$F(X;Y;M) = H(Y) - H(Y/M) = 1 - h\left(p_y + p_m - 2p_y p_m\right), \tag{22}$$

где $h(q) = -q\log_2 q - (1-q)\log_2(1-q)$ – энтропийная функция ДСК [3].

Равенство в (22) энтропии выходного ансамбля СтК1 ШВК максимально и $H(Y) = 1$, т.к. максимальна энтропия его входного ансамбля $H(X) = 1$ [3]. Условная энтропия $H(Y/M) = h\left(p_y + p_m - 2p_y p_m\right)$, т.к. она зависит от сочетания вероятностей ошибок в составляющих ШВК, обусловленных «сверткой» вероятностей в соответствии с зависимостью между $\overline{y}$ и $\overline{m}$ определенной в (14).

Для взаимной информации $I(T;D)$ и любых t на входе второго составляющего канала УШВК и d на его выходе в соответствии с зависимостью между $\overline{y}$ и $\overline{o}$ определенной в (18) можно записать:

$$I(T;D) = H(D) - H(D/T) = 1 - h\left(p_y + p_m - 2p_y p_m\right), \tag{23}$$

причем $H(D) = 1$, если $H(T) = 1$. Последнее достигается при равномерном распределении на входе второго составляющего канала УШВК [3]. Тогда (22) и (23) равны, что доказывает (19) первой части Утверждения. На основе (13) и с учетом равномерного закона распределения вероятностей на входе ШВК можно записать для

$I(X;Z)$ [3]:

$$I(X;Z) = H(Z) - H(Z/X) = 1 - h(p_w). \quad (24)$$

Равенство энтропии выходного ансамбля КП $H(Z)$ в (24) максимально, т.к. максимальна энтропия его входного ансамбля $H(X) = 1$ для ДСК канала [3]. Для оценки $I(T;O)$ и любых t на входе ВКП и символов o на его выходе с использованием (18) и на основе анализа модели нарушителя можно записать:

$$I(T;O) = H(O) - H(O/T) = 1 - h(p_y + p_w - 2p_y p_w), \quad (25)$$

причем $H(O) = 1$, если $H(T) = 1$, что достигается при равномерном распределении на входе ВКП. Сравнение (24) и (25) показывает, что $I(X;Z) \geq I(T;O)$, в силу того, что энтропийная функция канала является возрастающей функцией [3] в области определения, принадлежащей отрезку [0;0,5]. Это доказывает неравенство (20) во второй части Утверждения со знаком равенства в случае, если $p_y = 0$ в первом составляющем канале ШВК.

Утверждение доказано.

Анализ результатов утверждения показывает, что передаваемое СК *B* кодовое слово является общей информацией УШВК для СК и, следовательно, при выполнении МтПИ и условия (19) «качественная» информационные мера $F(X;Y;M)$ ШВК до выполнения МтПИ и информационная мера, характеризующая «качество» виртуального УШВК, после выполнения МтПИ равны. Это говорит о том, что использование МтПИ не ухудшает «качества» передачи общей информации сети связи. Этого нельзя сказать о виртуальном КП, формируемом после выполнения СК МтПИ и условия (20) Утверждения. «Качественная» информационная мера $I(X;Z)$ КП до выполнения МтПИ больше $I(T;O)$ – информационной меры, характеризующей «качество» «виртуального» КП после выполнения МтПИ. Это говорит о том, что использование МтПИ ухудшает «качество» формируемого ВКП. «Качество» формируемых виртуальных УШВК и КП связано с вероятностями ошибок. Анализ (22) и (23) показывает, что вероятности ошибок в ШВК и виртуального УШВК одинаковы и равны оценке $p1$:

$$p1 = p_y + p_m - 2p_y p_m . \quad (26)$$

В то же время вероятность ошибки формируемого ВКП $p2$ равна:

$$p2 = p_y + p_w - 2p_y p_w . \quad (27)$$

Анализ (27) показывает, что $p2 \geq p_w$. Это подтверждает факт того, что использование МтПИ ухудшает «качество» ВКП.

С другой стороны, взаимные информации $I(T;D)$, $I(T;O)$, $I(X;Z)$ определяется как информационная скорости соответствующих каналов связи [3]. Совместная информация $F(X;Y;M)$ является информационной скоростью ШВК [21]. В соответствии с результатами Утверждения, после виртуализации каналов информационная скорость в виртуальном УШВК остается прежней, а информационная скорость в ВКП уменьшается.

Заметим, что для того, чтобы в предлагаемой модели МПИ было возможно формирование сетевого ключа необходимо, чтобы информационная скорость в виртуальном УШВК была больше информационной скорости в ВКП [6]. Для этого необходимо выполнение условия: $p2 > p1$. Анализ (26) и (27) показывает, что это становится возможным в случае выполнения условия: $p_w > p_m$. Выполнение этого условия значительно легче для реализации, чем условие: $p_w > p_m + p_y$ для модели формирование сетевого ключа [6].

4. Заключение. В работе содержатся новые научные результаты теоретико-информационного представления виртуализации сетевого канала перехвата сети связи, включающей трех корреспондентов, связанных совокупностью ШВК с ошибками и ШВК без ошибок. Описана постановка задачи, в которой предлагается МПИ в СС, которая декомпозируется на новые МС и МтПИ. Особенностью предлагаемой МС является использование СК для передачи информации в дополнение к ШВК еще и ШВКбо. Это предопределило разработку нового МтПИ включающего 10 шагов и определяющего порядок передачи и обработки информационных последовательностей асимптотических длин. Особенностью предложенной модели нарушителя является использование им КПОО без ошибок в дополнение к КП. В целом исследуемая МПИ описывает процесс

формирования виртуальных ШВК и КП.

Методом теории информации доказано Утверждение о получении информационного преимущества виртуального ШВК над виртуальным КП, которые формируются в МПИ. Произведен анализ Утверждения как на уровне «качества» виртуальных каналов, так и на уровне информационных скоростей в формируемых каналах связи. Дальнейший анализ позволил найти условие, обеспечивающее получение информационного преимущества СК над Нр, связанное с качеством исходных ШВК и КП. Определенное условие создает предпосылки для разработки ключа с увеличенной информационной скоростью формирования ключа.

Направления дальнейших исследований связаны с теоретико-информационной оценкой в предлагаемой МПИ ключевой пропускной способности сети как оценкой потенциальной информационной скорости формирования сетевого ключа.

Полученные результаты могут быть полезны исследователям для анализа различных систем управления ключами и криптографических систем защиты информации в поиске ответов на вопросы о предельных возможностях перечисленных систем, определения, в какой мере проектируемая система уступает теоретически возможной. Кроме этого, логика вывода, используемая в теоретико-информационном исследовании подобных систем информации, может подсказать исследователям путь, на котором возможно будет найдено конструктивное решение для построения реальной системы.

Литература

1. Zhou H., El Gamal A. Network Information Theoretic Security with Omnipresent Eavesdropping // IEEE Transactions on Information Theory. 2021. vol. 67(12). pp. 8280–8299. DOI: 10.1109/TIT.2021.3116962.
2. Mitsugu I., Kazuo O, Junji S. Security Formalizations and their Relationships for Encryption and Key Agreement in Information-Theoretic Cryptography // IEEE Transactions on Information Theory. 2018. vol. 64(1). pp. 654–685. DOI: 10.1109/TIT.2017.2744650.
3. Csiszar I., Korner J. Information theory: coding theorems for discrete memoryless systems // Cambridge University Press. 2011. 523 p.
4. Chitambar E., Fortescue B., Hsieh M.-H. The Conditional Common Information in Classical and Quantum Secret Key Distillation // IEEE Transactions on Information Theory. 2018. vol. 64(11). pp. 7381–7394. DOI: 10.1109/TIT.2018.2851564.
5. Gohari A., Günlü O., Kramer G. Coding for Positive Rate in the Source Model Key Agreement Problem // IEEE Transactions on Information Theory. 2020. vol. 66(10). pp. 6303–6323. DOI: 10.1109/TIT.2020.2990750.
6. Синюк А.Д., Остроумов О.А. Теорема о ключевой пропускной способности сети связи // Информационно-управляющие системы. 2018. № 5(96). С. 79–87. DOI: 10.31799/1684-8853-2018-5-79-87.

7. Bloch M., Günlü O., Yener A., Oggier F., Poor H.V., Sankar L., Schaefer R.F. An Overview of Information-Theoretic Security and Privacy: Metrics, Limits and Applications // IEEE Journal on Selected Areas in Information Theory. 2021. vol. 2(1). pp. 5–22. DOI: 10.1109/JSAIT.2021.3062755.
8. Pappas N., Kountouris M., Ephremides A., Angelakis V. Stable Throughput Region of the Two-User Broadcast Channel // IEEE Transactions on Communications. 2018. vol. 66(10). pp. 4611–4621. DOI: 10.1109/TCOMM.2018.2834943.
9. Averbuch R., Merhav N. Exact Random Coding Exponents and Universal Decoders for the Asymmetric Broadcast Channel // IEEE Transactions on Information Theory. 2018. vol. 64(7). pp. 5070–5086. DOI: 10.1109/TIT.2018.2836668.
10. Mohapatra P., Pappas N., Lee J., Quek T.Q.S., Angelakis V. Secure Communications for the Two-User Broadcast Channel with Random Traffic // IEEE Transactions on Information Forensics and Security. vol. 13(9). 2018. pp. 2294–2309. DOI: 10.1109/TIFS.2018.2818076.
11. Yu L., Li H., Li W. Distortion Bounds for Source Broadcast Problems // IEEE Transactions on Information Theory. 2018. vol. 64. no. 9. pp. 6034–6053. DOI: 10.1109/TIT.2018.2854547.
12. Choi J. A Coding Approach with Key-Channel Randomization for Physical-Layer Authentication // IEEE Transactions on Information Forensics and Security. 2019. vol. 14(1). pp. 175–185. DOI: 10.1109/TIFS.2018.2847659.
13. Padakandla A., Sandeep Pradhan S. Achievable Rate Region for Three User Discrete Broadcast Channel Based on Coset Codes // IEEE Transactions on Information Theory. 2018. vol. 64(4). pp. 2267–2297. DOI: 10.1109/TIT.2018.2798669.
14. Остроумов О.А., Синюк А.Д. Пропускная способность широковещательного канала связи // Вестник компьютерных и информационных технологий. 2019. № 9(183). С. 33–42.
15. Qikun Z., Yongjiao L., Yong G., Chuanyang Z., Xiangyang L., Jun Z. Group Key Agreement Protocol Based on Privacy Protection and Attribute Authentication // IEEE Access. 2019. vol. 7. pp. 87085–87096. DOI: 10.1109/ACCESS.2019.2926404.
16. Ghosh S., Natarajan L. Linear Codes for Broadcasting with Noisy Side Information: Bounds and Code Constructions // IEEE Transactions on Information Theory. vol. 65(7). 2019. pp. 4207–4226. DOI: 10.1109/TIT.2019.2893617.
17. De Palma G. New lower bounds to the output entropy of multi-mode quantum Gaussian channels // IEEE Transactions on Information Theory. 2019. vol. 65. no. 9. pp. 5959–5968. DOI: 10.1109/TIT.2019.2914434.
18. Günlü O., Schaefer R.F. Controllable Key Agreement with Correlated Noise // IEEE Journal on Selected Areas in Information Theory. 2021. vol. 2(1). pp. 82–94. DOI: 10.1109/JSAIT.2021.3054035.
19. Zou S., Liang Y., La L., Poor H.V., Shamai S. Degraded Broadcast Channel with Secrecy Outside a Bounded Range // IEEE Transactions on Information Theory. 2018. vol. 64(3). pp. 2104–2120. DOI: 10.1109/TIT.2018.2791995.
20. Li C.T., Anantharam V. One-Shot Variable-Length Secret Key Agreement Approaching Mutual Information // IEEE Transactions on Information Theory. 2021. vol. 67(8). pp. 5509–5525. DOI: 10.1109/TIT.2021.3087963.
21. Синюк А.Д., Остроумов О.А. Информационная емкость и неопределенность дискретного широковещательного канала связи // Вестник компьютерных и информационных технологий. 2018. № 8(170). С. 36–45.

Синюк Александр Демьянович — д-р техн. наук, доцент, профессор кафедры, кафедра «общепрофессиональных дисциплин», Военная орденов Жукова и Ленина краснознаменная академия связи имени Маршала Советского Союза С.М. Буденного (ВАС). Область научных интересов: криптографическая защита информации,

передаваемая по открытым каналам связи. Число научных публикаций — 250. eentrop@rambler.ru; Тихорецкий проспект, 3, 194064, Санкт-Петербург, Россия; р.т.: +7(812)247-9481.

Остроумов Олег Александрович — канд. техн. наук, докторант кафедры, кафедра «защиты инфотелекоммуникационных систем специального назначения», Военная орденов Жукова и Ленина краснознаменная академия связи имени Маршала Советского Союза С.М. Буденного (ВАС). Область научных интересов: криптографическая защита информации, передаваемая по открытым каналам связи, обеспечение безопасности критически важных объектов систем вязи и управления. Число научных публикаций — 134. oleg-26stav@mail.ru; Тихорецкий проспект, 3, 194064, Санкт-Петербург, Россия; р.т.: +7(812)247-9832.

Тарасов Александр Алексеевич — адъюнкт кафедры, кафедра «общепрофессиональных дисциплин», Военная орденов Жукова и Ленина краснознаменная академия связи имени Маршала Советского Союза С.М. Буденного (ВАС). Область научных интересов: криптографическая защита информации, передаваемая по открытым каналам связи. Число научных публикаций — 10. taras4912@mail.ru; Тихорецкий проспект, 3, 194064, Санкт-Петербург, Россия; р.т.: +7(812)247-9481.

DOI 10.15622/ia.22.4.1

A. SINYUK, O. OSTROUMOV, A. TARASOV

INFORMATION-THEORETIC REPRESENTATION OF INTERCEPTION NETWORK CHANNEL VIRTUALIZATION

Sinyuk A., Ostroumov O., Tarasov A. **Information-Theoretic Representation of Interception Network Channel Virtualization.**

Abstract. The most difficult task of secure telecommunication systems using symmetric encryption, due to the need for preliminary and resource-intensive organization of secret channels for delivering keys to network correspondents, is key management. An alternative is the generating keys methods through open communication channels. In information theory, it is shown that these methods are implemented under the condition that the channel information rate of correspondents exceeds the rate of the intruder interception channel. The search for methods that provide the informational advantage of correspondents is being updated. The goal is to determine the information-theoretical conditions for the formation of a virtual network and an interception channel, for which the best ratio of information speeds for correspondents is provided compared to the ratio of the original network and interception channel. The paper proposes an information transfer model that includes a connectivity model and an information transfer method for asymptotic lengths of code words. The model includes three correspondents and is characterized by the introduction of an ideal broadcast channel in addition to an errored broadcast channel. The model introduces a source of "noisy" information, which is transmitted over the channel with errors, so the transmission of code words using the known method of random coding is carried out over the channel without errors. For asymptotic lengths of code words, all actions of correspondents in processing and transmitting information in the model are reduced to the proposed method of transmitting information. The use of the method by correspondents within the framework of the transmission model makes it possible to simultaneously form for them a new virtual broadcast channel with information rate as in the original channel with errors, and for the intruder a new virtual broadcast interception channel with a rate lower than the information rate of the initial interception channel. The information-theoretic conditions for deterioration of the interception channel are proved in the statement. The practical significance of the results obtained lies in the possibility of using the latter to assess the information efficiency of open network key formation in the proposed information transfer model, as well as in the development of well-known scientific achievements of open key agreement. The proposed transmission model can be useful for researching key management systems and protecting information transmitted over open channels. Further research is related to the information-theoretic assessment of the network key throughput, which is the potential information-theoretic speed of network key formation.

Keywords: information transmission model in a communication network, network correspondent, intruder, source of «noise» sequence, virtual interception channel, information transmission method for asymptotic lengths of code words.

References

1. Zhou H., El Gamal A. Network Information Theoretic Security with Omnipresent Eavesdropping. IEEE Transactions on Information Theory. 2021. vol. 67(12). pp. 8280–8299. DOI: 10.1109/TIT.2021.3116962.
2. Mitsugu I., Kazuo O, Junji S. Security Formalizations and their Relationships for Encryption and Key Agreement in Information-Theoretic Cryptography. IEEE

Transactions on Information Theory. 2018. vol. 64(1). pp. 654–685. DOI: 10.1109/TIT.2017.2744650.
3. Csiszar I., Korner J. Information theory: coding theorems for discrete memoryless systems. Cambridge University Press. 2011. 523 p.
4. Chitambar E., Fortescue B., Hsieh M.-H. The Conditional Common Information in Classical and Quantum Secret Key Distillation. IEEE Transactions on Information Theory. 2018. vol. 64(11). pp. 7381–7394. DOI: 10.1109/TIT.2018.2851564.
5. Gohari A., Günlü O., Kramer G. Coding for Positive Rate in the Source Model Key Agreement Problem. IEEE Transactions on Information Theory. 2020. vol. 66(10). pp. 6303–6323. DOI: 10.1109/TIT.2020.2990750.
6. Sinyuk A.D., Ostroumov O.A. [Theorem about key capacity of a communication network]. Informatsionno-upravliaiushchie sistemy – Information and Control Systems. 2018. no. 5(96). pp. 79–87. DOI: 10.31799/1684-8853-2018-5-79-87. (In Russ.).
7. Bloch M., Günlü O., Yener A., Oggier F., Poor H.V., Sankar L., Schaefer R.F. An Overview of Information-Theoretic Security and Privacy: Metrics, Limits and Applications. IEEE Journal on Selected Areas in Information Theory. 2021. vol. 2(1). pp. 5–22. DOI: 10.1109/JSAIT.2021.3062755.
8. Pappas N., Kountouris M., Ephremides A., Angelakis V. Stable Throughput Region of the Two-User Broadcast Channel. IEEE Transactions on Communications. 2018. vol. 66(10). pp. 4611–4621. DOI: 10.1109/TCOMM.2018.2834943.
9. Averbuch R., Merhav N. Exact Random Coding Exponents and Universal Decoders for the Asymmetric Broadcast Channel. IEEE Transactions on Information Theory. 2018. vol. 64(7). pp. 5070–5086. DOI: 10.1109/TIT.2018.2836668.
10. Mohapatra P., Pappas N., Lee J., Quek T.Q.S., Angelakis V. Secure Communications for the Two-User Broadcast Channel with Random Traffic. IEEE Transactions on Information Forensics and Security. vol. 13(9). 2018. pp. 2294–2309. DOI: 10.1109/TIFS.2018.2818076.
11. Yu L., Li H., Li W. Distortion Bounds for Source Broadcast Problems. IEEE Transactions on Information Theory. 2018. vol. 64. no. 9. pp. 6034–6053. DOI: 10.1109/TIT.2018.2854547.
12. Choi J. A Coding Approach with Key-Channel Randomization for Physical-Layer Authentication. IEEE Transactions on Information Forensics and Security. 2019. vol. 14(1). pp. 175–185. DOI: 10.1109/TIFS.2018.2847659.
13. Padakandla A., Sandeep Pradhan S. Achievable Rate Region for Three User Discrete Broadcast Channel Based on Coset Codes. IEEE Transactions on Information Theory. 2018. vol. 64(4). pp. 2267–2297. DOI: 10.1109/TIT.2018.2798669.
14. Ostroumov O.A., Sinyuk A.D. [Broadcast communication channel bandwidth]. Vestnik komp'yuternyh i informacionnyh tekhnologij – Bulletin of computer and information technologies. 2019. №. 9 (183). pp. 33–42. (In Russ.).
15. Qikun Z., Yongjiao L., Yong G., Chuanyang Z., Xiangyang L., Jun Z. Group Key Agreement Protocol Based on Privacy Protection and Attribute Authentication. IEEE Access. 2019. vol. 7. pp. 87085–87096. DOI: 10.1109/ACCESS.2019.2926404.
16. Ghosh S., Natarajan L. Linear Codes for Broadcasting with Noisy Side Information: Bounds and Code Constructions. IEEE Transactions on Information Theory. vol. 65(7). 2019. pp. 4207–4226. DOI: 10.1109/TIT.2019.2893617.
17. De Palma G. New lower bounds to the output entropy of multi-mode quantum Gaussian channels. IEEE Transactions on Information Theory. 2019. vol. 65. no. 9. pp. 5959–5968. DOI: 10.1109/TIT.2019.2914434.
18. Günlü O., Schaefer R.F. Controllable Key Agreement with Correlated Noise. IEEE Journal on Selected Areas in Information Theory. 2021. vol. 2(1). pp. 82–94. DOI: 10.1109/JSAIT.2021.3054035.

19. Zou S., Liang Y., La L., Poor H.V., Shamai S. Degraded Broadcast Channel with Secrecy Outside a Bounded Range. IEEE Transactions on Information Theory. 2018. vol. 64(3). pp. 2104–2120. DOI: 10.1109/TIT.2018.2791995.
20. Li C.T., Anantharam V. One-Shot Variable-Length Secret Key Agreement Approaching Mutual Information. IEEE Transactions on Information Theory. 2021. vol. 67(8). pp. 5509–5525. DOI: 10.1109/TIT.2021.3087963.
21. Sinyuk A.D., Ostroumov O.A. [Information capacity and uncertainty of a discrete broadcast communication channel]. Vestnik komp'yuternyh i informacionnyh tekhnologij – Bulletin of computer and information technologies. 2018. no. 8(170). pp. 36–45. (In Russ.).

Sinyuk Alexander — Ph.D., Dr.Sci., Associate Professor, Professor of the department, General professional disciplines department, Military communications academy. Research interests: cryptographic protection of information transmitted through open communication channels. The number of publications — 250. eentrop@rambler.ru; 3, Tikhoretsky Av., 194064, St. Petersburg, Russia; office phone: +7(812)247-9481.

Ostroumov Oleg — Ph.D., Doctoral student of the department, Information protection department and telecommunication systems of special purpose, Military communications academy. Research interests: cryptographic protection of information transmitted through open communication channels, ensuring the security of communication and control systems critical objects. The number of publications — 134. oleg-26stav@mail.ru; 3, Tikhoretsky Av., 194064, St. Petersburg, Russia; office phone: +7(812)247-9832.

Tarasov Alexander — Adjunct of the department, General professional disciplines department, Military communications academy. Research interests: cryptographic protection of information transmitted through open communication channels. The number of publications — 10. taras4912@mail.ru; 3, Tikhoretsky Av., 194064, St. Petersburg, Russia; office phone: +7(812)247-9481.