АСИМПТОТИЧЕСКАЯ ЭФФЕКТИВНОСТЬ ОТКРЫТОГО СЕТЕВОГО КЛЮЧЕВОГО СОГЛАСОВАНИЯ

Синюк А. Д.[1], Потапов И. А.[2], Остроумов О. А.[3]

DOI: 10.21681/2311-3456-2024-3-96-104

Цель исследования *– поиск путей уменьшения времени восстановления сетевой криптосвязности.*

Метод исследования *– введение в теорию информации коэффициента асимптотического выигрыша по времени согласования сетевого ключа в условиях неограниченного увеличения длины передаваемой последовательности и заданных требований к открыто формируемому ключу сети связи.*

Результаты исследований *– исследуются две модели открытого формирования ключа. В первой модели первоначально поочередно формируются ключи в каждом канале сети связи, а затем один из корреспондентов выбирает один из ключей в качестве сетевого и передает его по закрытым каналам другим корреспондентам. Во второй - ключ формируется одновременно по составляющим каналам сети. Поэтому вводится коэффициент асимптотического выигрыша по времени формирования ключа трех сетевых корреспондентов определяющий показатель асимптотической эффективности открытого сетевого ключевого согласования. Выполнена оценка показателя эффективности, позволившая найти преимущественные теоретико-информационные условия использования каждой из моделей.*

Практическая ценность *– результаты могут быть полезны исследователям для анализа различных подсистем информационной безопасности телекоммуникационных систем для оценки потенциальных возможностей по уменьшению времени восстановления криптосвязности.*

Ключевые слова: *теория информации; сеть связи; нарушитель; сетевой ключ; ключевая пропускная способность; коэффициент асимптотического выигрыша по времени формирования сетевого ключа.*

ASYMPTOTIC EFFICIENCY OF OPEN NETWORK KEY CONNECTION

Sinyuk A. D.[4], Potapov I. A.[5], Ostroumov O. A.[6]

Abstract: Maintaining. *The key management subsystem main function of a telecommunication system in the key compromises context by an intruder is to ensure cryptographic connectivity timely restoration of geographically dispersed correspondents via secure channels, which is updated for network correspondents, due to the fact that the resistance of the network key to compromise is minimal.*

The study purpose *is to find ways to reduce the recovery time of network crypto-connectivity.*

The research method *is the introduction into information theory of the coefficient of asymptotic gain in time of network key agreement under conditions of an unlimited increase in the length of the transmitted sequence and specified requirements for an openly generated key of a communication network.*

Research results *– two models of open key generation are investigated. In the first model, keys are initially generated in turn in each channel of the communication network, and then one of the correspondents*

1 Синюк Александр Демьянович, доктор технических наук, доцент, профессор кафедры Общепрофессиональных дисциплин Военной орденов Жукова и Ленина краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного, Санкт-Петербург, Россия. E-mail: eentrop@rambler.ru, orcid.org/0000-0003-0608-4359.

2 Потапов Илья Александрович, кандидат технических наук, доцент, доцент кафедры Общепрофессиональных дисциплин Военной орденов Жукова и Ленина краснознаменной академии связи имени Маршала Советского Союза С.М. Буденного, Санкт-Петербург, Россия. E-mail: momento87@mail.ru

3 Остроумов Олег Александрович, кандидат технических наук, старший преподаватель кафедры Военных систем многоканальной, электропроводной и оптической связи Военной орденов Жукова и Ленина краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного, Санкт-Петербург, Россия. E-mail: oleg-26stav@mail.ru, orcid.org/0000-0003-1674-6248.

4 Alexander D. Sinyuk, Dr.Sc., Associate Professor, Professor of the Department of General Professional Disciplines of the Military Orders of Zhukov and Lenin of the Red Banner Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny, St. Petersburg, Russia. E-mail:eentrop@rambler.ru, orcid.org/0000-0003-0608-4359..

5 Ilya A. Potapov, Ph.D., Associate Professor, Associate Professor, Department of General Professional Disciplines, Military Orders of Zhukov and Lenin, Red Banner Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny, St. Petersburg, Russia. E-mail:momento87@mail.ru

6 Oleg A. Ostroumov, Ph.D., senior lecturer of the Department of Military Systems of Multichannel, Electrically Conducted and Optical Communications of the Military Orders of Zhukov and Lenin of the Red Banner Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny, St. Petersburg, Russia. E-mail: oleg-26stav@mail.ru, orcid.org/0000-0003-1674-6248.

selects one of the keys as a network key and transmits it through private channels to other correspondents. In the second, the key is formed simultaneously along the constituent channels of the network. Therefore, a coefficient of asymptotic gain in the time of key formation of three network correspondents is introduced, which is a determining indicator of open network key agreement asymptotic efficiency. An assessment of the efficiency indicator was carried out, which made it possible to find the preferential information-theoretic conditions for using each of the models.

***Practical value** – the results can be useful to researchers for analyzing various information security subsystems of telecommunication systems to assess the potential for reducing the recovery time of crypto-connectivity.*

***Discussion.** The results obtained deepen and expand the known information-theoretic assessments of various key coordination models effectiveness.*

***Keywords:** information theory; communication network; intruder; network key; open network key negotiation; key throughput; coefficient of asymptotic gain in the time of network key formation.*

Введение

Современные защищенные телекоммуникационные системы включают в своем составе подсистемы управления криптографическими ключами. Главной целью в условиях компрометаций ключей нарушителем любой подсистемы управления ключами выступает решение задачи своевременного восстановления по защищенным каналам криптосвязности территориально разнесенных корреспондентов (объектов связи), которое актуализируется для сетевых корреспондентов, ввиду того, что устойчивость сетевого ключа к компрометациям минимальна. Это актуализирует поиск путей достижения потенциальных возможностей по уменьшению времени восстановления криптографической связности объектов связи после компрометации сетевого ключа нарушителем.

В предыдущих исследованиях [1] показано, что в условиях одновременной передачи информации одновременно по составляющим каналам дискретного широковещательного канала связи без памяти (ДШКБП), может быть затрачено меньше времени на передачу, чем при поочередной передаче информации по каждому составляющему каналу ДШКБП. Этот факт определяет возможный выигрыш по времени формирования сетевого ключа (СК) объектов связи (ОС) на основе открытого сетевого ключевого согласования [2, 3]. Поэтому в работе предлагается терминология и метод оценки асимптотической эффективности открытого сетевого ключевого согласования, который позволит обоснованно выбирать преимущественные условия осуществления формирования СК по открытым каналам сети связи, обеспечивающие оперативное восстановление сетевой криптосвязности. Вводится коэффициент асимптотического выигрыша по времени формирования СК в условиях неограниченного увеличения длины передаваемого открытого сообщения (кодового слова) [4] и заданных требований к СК [2].

Полученные результаты расширяют область известных исследований открытого ключевого согласования и могут быть использованы для оценки потенциальных возможностей и анализа предлагаемых современных криптографических подсистем защиты информации телекоммуникационных систем [5], включающих подсистемы управления ключами.

Предварительные результаты

В источниках [2] исследована модель формирования ключа для трех сетевых объектов связи (ОС). Рассмотрено следующее общее описание ситуации передачи информации в сети связи (по широковещательному каналу связи), показанной на рис. Имеется один передатчик (кодер) у ОС $\boldsymbol{A}$ и три независимо работающих приемника (декодера) у ОС $\boldsymbol{B}$, $\boldsymbol{C}$ и нарушителя $\boldsymbol{E}$, на входы которых поступают выходные сигналы разных каналов.

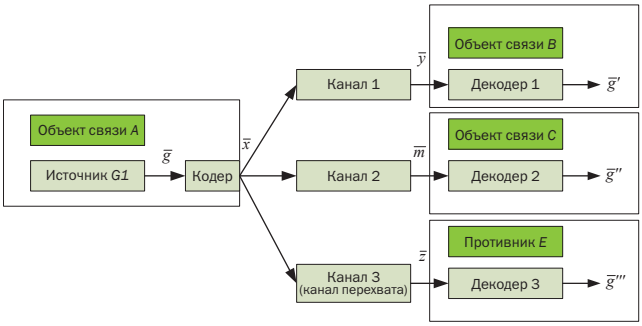

Рис. 1. Модель сетевой канальной связности ОС A, B, C и нарушителя E

На передатчик поступают сообщения $\bar{g}$ от источника $G1$ (который находится у ОС A), которые он должен передать в одно и то же время приемникам 1, 2 и 3 (ОС B, C и нарушителю E, соответственно) так, чтобы приемники 1 и 2 могли восстановить с произвольно малой вероятностью ошибки сообщения источника $G1$, а нарушитель не был в состоянии восстановить с произвольно малой вероятностью ошибки сообщения источника $G1$. Совокупность, состоящая из источника сообщений $G1$ и кодера, приемников, каналов связи образует модель канальной связности (МКС).

Пусть ОС A использует для генерации сетевого ключа (СК) дискретный источник без памяти $G1$ [6] модели канальной связности трех сетевых ОС и нарушителя с равномерным законом распределения вероятностей сообщений [7].

Все каналы связи в МКС описываются моделями дискретных симметричных каналов связи без памяти (ДСК) [8]. Совокупность, состоящая из двух каналов с общим входом (выход кодера, который находится у ОС A) и выходами (входы приемников 1, 2, которые находятся у ОС B, C, соответственно) описывается моделью дискретного широковещательного канала без памяти (ДШКБП), который был исследован [9].

Передача сигналов по ДШКБП определяется двумя каналами с общим входным алфавитом X, выходными алфавитами Y и M и матрицами переходных вероятностей $P_1 = \{p(y/x)\}$, $P_2 = \{p(m/x)\}$, $x \in X$, $y \in Y$, $m \in M$. Алфавиты X, Y и M конечны и для любых последовательностей $\bar{x} \in X^n$, $\bar{y} \in Y^n$, $\bar{m} \in M^n$, где X^n – декартова n-я степень множества X [6], а Y^n и M^n определяются аналогично. Дискретный широковещательный канал без памяти обозначим символом $\{X,Y,M;p(y/x),p(m/x)\}$, при этом каналы $\{X,Y;p(y/x)\}$ и $\{X,M;p(m/x)\}$ являются составляющими ДШКБП. Канал связи с входом на выходе кодера, который находится у ОС A, и с выходом на входе приемника 3, который находятся у нарушителя E определен в [2] как канал перехвата (КП). Передача сигналов по КП (описывается моделью дискретного симметричного канала связи без памяти) определяется входным алфавитом X, выходным алфавитом Z и матрицей переходных вероятностей $P_3 = \{p(z/x)\}$, $x \in X$, $z \in Z$. Для КП алфавиты X, Z конечны и для любых последовательностей $\bar{x} \in X^n$, $\bar{z} \in Z^n$, где X^n – декартова n-я степень множества X и Z^n – декартова n-я степень множества Z. КП обозначим символом $\{X,Z;p(z/x)\}$.

Составляющие ДШКБП и КП являются независимыми каналами [8]. Алфавиты (объемы алфавитов) источника $G1$, алфавит, описывающий вход ДШКБП и КП, выходные алфавиты составляющих ДШКБП и КП совпадают, т. е. $|G| = |X| = |Y| = |M| = |Z| = t$.

Для передачи информации используется случайный кодер, математическое описание которого представлено в [2]. Нарушитель E при использовании случайного кодера представляется случайным выбором сообщения источника $G1$ (это соответствует случайному выбору кодового подмножества) и равномерным распределением входной последовательности на входе КП при условии известного выбора сообщения источника $G1$.

Общая постановка задачи формирования общего ключа (СК) трех сетевых объектов связи по открытым каналам связи с ошибками сводится к необходимости выработать общий ключ (СК) для сети из трех сетевых ОС, передавая данные по ДШКБП и КП. Требуется обеспечить формирование общего СК с высокой надежностью для ОС и обеспечить наперед заданный низкий уровень информации об этом СК со стороны нарушителя. Предполагается, что нарушитель использует пассивную стратегию [2, 10]. Особенности активного нарушителя показаны в [11, 12]. После передачи информации ОС обладают некоторой информацией в виде последовательностей на входе ДШКБП и двух его выходах в виде кодового слова $\bar{x}$, $\bar{x} \in V$ для ОС A и принятых последовательностей $\bar{y}$, $\bar{y} \in Y^n$ для ОС B и $\bar{m}$, $\bar{m} \in M^n$ для ОС C. Эти последовательности могут быть коррелированы между собой [13], а также с начальными данными нарушителя в виде последовательности $\bar{z}$, $\bar{z} \in Z^n$. Предполагается, что нарушитель E знает полное описание всех действий выполняемых ОС, выбранного кода (n,ε_1) и источника $G1$, как и в модели [2, 14]. Первоначально распределенные (переданные) последовательности не могут быть использованы для формирования СК, т.к. в ДШКБП (в составляющих ДШКБП) могут возникать ошибки. Тогда они требуют коррекции с использованием метода декодирования полученных на выходах ДШКБП последовательностей. После чего декодированные последовательности и первоначально выбранная последовательность источника $G1$ могут быть выбраны в качестве СК для ОС B, C и A. Эти условия определяют построение для достаточно большого n протокола формирования общего СК, который приведен в [2].

Основные показатели качества, сформированного (переданного) СК после использования ОС протокола формирования общего СК для достаточно большого n приведены в [2]. Качественно они сводятся к надежной передаче большого количества бит «хорошего» СК при малой утечке информации к нарушителю E. «Информационная» скорость формирования СК по отношению к длине кодового слова (КС) n характеризует оперативность установления криптосвязности между ОС. СК удовлетворяет ряду требований, показанных в [2].

Определена ключевая пропускная способность для трех сетевых ОС C_3 [2] как максимально достижимая величина скорости формирования ключа для трех сетевых ОС H_3. Разработанная модель канальной связности сетевых ОС и нарушителя, приведенная на рис. 1, выполнение во времени ОС шагов протокола формирования СК для формирования общего СК трех сетевых ОС представляется как процесс формирования СК для трех объектов связи во времени.

Основным параметром, характеризующим быстротечность процесса формирования СК для сетевых объектов связи (ПФСК), является C_3 – ключевая

пропускная способность для трех сетевых ОС, которая достигается при $n \to \infty$ и равномерном распределении на входе ДШКБП и КП в силу свойств информационных мер дискретных симметричных каналов, приведенных в [5, 8], и совсем не зависит от модели, описывающей источник $G1$. Показатель C_3 зависит от потенциальных возможностей ДШКБП и КП. Пропускная способность ДШКБП $C_{ДШКБП}$ определяет (измеряет) потенциальное (предельное) количество информации источника, которое может нести один символ кодового слова [15]. Это же можно утверждать относительно пропускной способности КП C_w. А так как теория информации [16] только измеряет количество информации, то только превышение $C_{ДШКБП}$ над C_w гарантирует передачу по ДШКБП по сравнению с КП той положительной разницы в количестве информации, которая в последующем может быть использована для формирования СК.

Если один из составляющих каналов ДШКБП не подвержен влиянию ошибок (помех), то C_3 определяется как секретная пропускная способность с каналом перехвата C_S для двух ОС, в МКС, предложенной Чисаром и Кернером [5], в которой основной канал (канал между ОС) и канал перехвата имеют общий вход и являются независимыми каналами [9, 17].

Постановка задачи

В [1] показано, что один из возможных методов передачи по ДШКБП состоит в разделении времени, когда в течение некоторого отрезка времени осуществляется передача одному приемнику, а в течение другого отрезка времени – второму. Другая возможность состоит в том, чтобы вести передачу обоим приемникам в одно и то же время. Первый случай широко исследован в [18]. В статье исследуется последний случай. Процесс формирования СК основан на передаче сообщений. Тогда в рамках МКС возможны 2 варианта формирования СК. В первом случае СК может формироваться при поочередной передаче информации по каждому составляющему каналу ДШКБП, который соответствует случаю разделения времени и формированию СК в модели Чисара и Кернера [5]. После формирования ОС A СК с ОС B и C разных парных ключей (вероятность совпадения парных ключей (ПК) очень мала и стремится к нулю при неограниченном увеличении формируемого СК) ОС A формирует 2 закрытых (защищенных) канала, выбирает один из ПК за общий СК и передает его по закрытому каналу тому ОС, у которого другой ПК. Второй случай связан с формированием СК, когда ведется передача информации одновременно по обоим составляющим каналам ДШКБП. Для краткости модель, описывающую первый случай процесса формирования СК, назовем моделью формирования СК № 1 (МФШК-1), а модель, описывающую второй случай процесса формирования СК, назовем моделью формирования СК № 2 (МФШК-2).

В [1] показано, что в условиях одновременной передачи информации одновременно по обоим составляющим каналам ДШКБП, может быть затрачено меньше времени на передачу, чем при поочередной передаче информации по каждому составляющему каналу ДШКБП. Это определяет возможный выигрыш по времени формирования СК в МФШК-2 по сравнению с МФШК-1.

Одним из важнейших аспектов синтеза систем формирования СК является время формирования СК (или «информационная» скорость его формирования), т.к. это связано с информационными потерями, связанными с задержкой конфиденциальной информации при компрометации СК и необходимости временных затрат на установление криптосвязности на новом (не скомпрометированном) СК [19].

Показатель эффективности

Эффективность МФШК-1 и МФШК-2 предлагается в разрабатываемой модели оценки асимптотической эффективности открытого сетевого ключевого согласования оценивать показателем временной эффективности, т.е. исследовать соотношение временных показателей ПФСК с поочередной передачей информации, которая соответствует случаю разделения времени и ПФСК с одновременной передачей информации по ДШКБП. Считаем, что все процессы обработки информации у ОС не оказывают существенного влияния на время формирования СК (т.е. выполняются мгновенно) за исключением самого процесса передачи сообщений по каналам связи. Определим этот показатель и опишем модель оценивания этого показателя.

Пусть в модели МФШК-1 скорость формирования СК для двух ОС R_{11} [5, 7] с использованием канала от ОС A к ОС B равна

$$R_{11} = \frac{H(G^k)}{n_{11}}, \quad (1)$$

где $H(G^k)$ – информация ансамбля СК (сообщений), n_{11} – длина последовательности, передаваемой по каналу от ОС A к ОС B (первому составляющему каналу ДШКБП) [2, 17].

Пусть в модели МФШК-1 скорость формирования СК для двух ОС R_{12} с использованием канала от ОС A к ОС C равна

$$R_{12} = \frac{H(G^k)}{n_{12}}, \quad (2)$$

где n_{12} – длина последовательности передаваемой по каналу от ОС A к ОС C (второму составляющему каналу ДШКБП).

Пусть в модели МФШК-2 скорость формирования СК для трех сетевых ОС H_3 с использованием составляющих каналов ДШКБП от ОС A к ОС B и C равна

$$H_3 = \frac{H(G^k)}{n_3}, \quad (3)$$

где n_3 – длина последовательности передаваемой по составляющим каналам ДШКБП от ОС A к ОС B и C.

Пусть техническая скорость передачи информации [7, 16] в МФШК-1 и МФШК-2 одинакова и равна ν бит/с.

Пусть для обеих моделей заданы требования к формируемому СК [2], которые совпадают.

Тогда в рамках МФШК-1 для модели Чисара и Кернера можно сформировать СК, удовлетворяющий требованиям [2] с использованием дискретного канала без памяти от ОС A к ОС B, причем скорость формирования СК R_{11}, $R_{11} < C_{11}$, где C_{11} – значение ключевой пропускной способности двух ОС [10] для дискретного канала без памяти от ОС A к ОС B. Это можно сказать о процессе формирования СК с использованием дискретного канала без памяти от ОС A к ОС C, т.е. $R_{12} < C_{12}$, где C_{12} – значение ключевой пропускной способности двух ОС для дискретного канала без памяти от ОС A к ОС C. Для МФШК-2 в соответствии с теоремой о ключевой пропускной способности процесса формирования ключа для трех объектов связи доказанной в [2], можно сформировать СК, удовлетворяющий требованиям с использованием составляющих каналов связи ДШКБП от ОС A к ОС B и C, причем скорость формирования СК для трех сетевых ОС $H_3 < C_3$, где C_3 – значение сетевой ключевой пропускной способности трех сетевых ОС для ДШКБП [2] от ОС A к ОС B и C.

Определим T_1 – время формирования общего СК в МФШК-1.

$$T_1 = \nu n_{11} + \nu n_{12} + \nu H(G^k) = \nu H(G^k)\left(\frac{1}{R_{11}} + \frac{1}{R_{12}} + 1\right). \quad (4)$$

Подобным образом определим T_2 – время формирования общего СК в МФШК-2.

$$T_2 = \nu n_3 = \nu H(G^k)\frac{1}{H_3}. \quad (5)$$

Определение 1. Пусть ОС A, B и C для формирования общего СК используют модель МФШК-1 и МФШК-2. Пусть техническая скорость передачи информации в МФШК-1 и МФШК-2 одинакова и равна ν бит/с. *Временной эффективностью процесса формирования СК* для трех сетевых ОС χ называется коэффициент равный отношению времени формирования СК в МФШК-1 к времени формирования СК в МФШК-2, при котором обеспечивается выполнение заданных требований к формируемому СК [2]

$$\chi = \frac{T_1}{T_2} = \frac{H_3\,(R_{11}+R_{12}+R_{11}\,R_{12})}{R_{11}\,R_{12}}. \quad (6)$$

Найдем потенциально достижимый коэффициент выигрыша по времени формирования СК χ_0, если для формирования (передачи) СК используются коды неограниченной длины, т.е. в случае, если $n_{11} \to \infty$, $n_{12} \to \infty$ и $n_3 \to \infty$. В соответствии с (6), приведенными результатами в [5, 10] для модели Чисара и Кернера и с теоремой о ключевой пропускной способности процесса формирования ключа для трех объектов связи [2] и χ_0 вычисляется из формулы

$$\chi_0 = \frac{C_3\,(C_{11}+C_{12}+C_{11}\,C_{12})}{C_{11}\,C_{12}}, \quad (7)$$

где в рамках МФШК-1 C_{11} – значение ключевой пропускной способности двух ОС для дискретного канала без памяти от ОС A к ОС B, C_{12} – значение ключевой пропускной способности двух ОС для дискретного канала без памяти от ОС A к ОС C и в рамках МФШК-2 C_3 – значение ключевой пропускной способности трех сетевых ОС для ДШКБП от ОС A к ОС B и C.

Определение 2. Временная эффективность процесса формирования СК для трех сетевых ОС при использовании для формирования (передачи) СК кодов неограниченной длины называется *коэффициентом асимптотического выигрыша по времени формирования СК* для трех сетевых ОС, обозначается через χ_0 и определяется согласно (7).

Методика оценки асимптотической эффективности открытого сетевого ключевого согласования, т.е. оценки χ_0 сводится к определению ключевых пропускных способностей дискретных симметричных каналов без памяти для двух ОС в модели Чисара и Кернера и ключевой пропускной способности ПФСК с использованием ДШКБП для трех сетевых ОС. На первом шаге определяются ключевые пропускные способности дискретных симметричных каналов без памяти для двух ОС. Ключевая пропускная способность дискретного симметричного канала без памяти C_K определяется согласно выражению из [5]

$$C_K = C - C_w, \quad (8)$$

где C – пропускная способность дискретного симметричного канала без памяти между двумя ОС [8] и C_w – пропускная способность КП (дискретного симметричного канала без памяти между ОС A и нарушителем E).

На втором шаге методики находится значение ключевой пропускной способности процесса формирования ключа для трех объектов связи [2].

На завершающем шаге оценивается асимптотический выигрыш по времени формирования СК для трех сетевых ОС с использованием формулы (7).

Оценка коэффициента асимптотического выигрыша по времени формирования сетевого ключа

Из определения 2, оценки пропускной способности двоичного ДСК (ДСКБП) [16, 17] для общего двоичного алфавита ($t = 2$) вытекает следующее следствие.

Следствие. Пусть каналы связи МФШК-1 и МФШК-2 описываются с помощью моделей ДСКБП. Тогда коэффициент асимптотического выигрыша по времени формирования СК для трех сетевых ОС равен

$$\chi_0 = \frac{(h(p_w) - h(p))(2h(p_w) + h(p_w)^2 + h(p_y)h(p_m) - (h(p_y) + h(p_m))(1+ h(p_w)))}{(h(p_w)^2 + h(p_y)h(p_m) - h(p_w)(h(p_y) + h(p_m))}. \quad (9)$$

где $h(l) = -l\,logl - (1-l)\,log(1-l)$ – энтропийная функция ДСКБП [5, 9], p_w – вероятность ошибки в КП, который описывается моделью ДСКБП, вероятность p равна

$$p = p_y(1 - p_m) + (1 - p_y)p_m, \quad (10)$$

где p_y - вероятность ошибки в первом ДСКБП канале в МФШК-1 и первом составляющем ДСКБП канале двоичного широковещательного канала без памяти (ДвШКБП), p_w – вероятность ошибки во втором ДСКБП канале в МФШК-1 и втором составляющем ДСКБП канале ДвШКБП.

В таблице 1 приведены оценки значений коэффициента асимптотического выигрыша по времени формирования СК для трех сетевых ОС и фиксированной вероятности ошибки в КП $p_w = 0{,}3$ для интервала изменения вероятностей ошибок в составляющих ДСКБП от 0 до 0,3.

В таблице 2 приведены оценки значений коэффициента асимптотического выигрыша по времени формирования СК для трех сетевых ОС и фиксированной вероятности ошибки в КП $p_w = 0{,}1$ для интервала изменения вероятностей ошибок в составляющих ДСКБП от 0 до 0,3.

Анализ таблиц 1 и 2 показывает, что улучшение качества КП приводит к уменьшению области эффективного использования МФШК-2, где $\chi_0 > 1$. Оценка коэффициента ограничена значениями

$$0 \le \chi_0 < 3. \quad (11)$$

Таблица 1

Оценки значений χ_0 для общего двоичного алфавита при $p_w = 0{,}3$

		p_m						
		0	**0.05**	**0.1**	**0.15**	**0.2**	**0.25**	**0.3**
p_y	0	2.8813	2.2699	1.8801	1.5795	1.3402	1.1495	0
	0.05	2.2699	1.8684	1.5169	1.2119	0.925	0.5555	0
	0.1	1.8801	1.5169	1.1773	0.8611	0.5291	0	0
	0.15	1.5795	1.2119	0.8611	0.5203	0.1377	0	0
	0.2	1.3402	0.925	0.5291	0.1377	0	0	0
	0.25	1.1495	0.5555	0	0	0	0	0
	0.3	0	0	0	0	0	0	0

Таблица 2

Оценки значений χ_0 для общего двоичного алфавита при $p_w = 0{,}1$

		p_m		
		0	**0.05**	**0.1**
p_y	0	2.469	1.5719	0
	0.05	1.5719	0.1919	0
	0.45	0	0	0

Нижней границы, равной 0, коэффициент достигает, если $C_3 = 0$. Верхней границе необходимо уделить особое внимание. Для этого сравним предложенную в [1] модель передачи информации 1 (МПИ-1) с МФШК-1. В обеих моделях производится поочередная передача сообщений, однако во второй модели дополнительно присутствует нарушитель E. Задача нарушителя сводится к получению (формированию) общего СК для трех сетевых ОС. Это обуславливает определенные ограничения в МФШК-1 по сравнению с МПИ-1. При выполнении поочередной передачи сообщений в МПИ-1 ОС A может каждый раз передавать ОС B и C одно и тоже сообщение. При выполнении поочередной передачи сообщений в МФШК-1 ОС A не может делать этого за исключением одного случая. Рассмотрим, почему ОС A так нельзя делать. Если ОС A выполняет поочередную передачу одного и того же сообщения $\bar{g}$, где $\bar{g} \in G^k$, в МФШК-1 и после этого выбирает его в качестве общего СК, тогда нарушается требование по скорости получения информации о СК нарушителем E [2], т.к. после обеих передач нарушитель имеет в наличии 2 версии одного и того же сообщения $\bar{z}_1$ и $\bar{z}_2$, где $\bar{z}_1, \bar{z}_2 \in Z^n$. Тогда информация его $I(\bar{g};(\bar{z}_1, \bar{z}_2))$ после обеих передач увеличивается и становится больше, чем информация $I(\bar{g};\bar{z}_1)$ при первой передаче (или второй), что не допустимо согласно требования по скорости получения информации о СК нарушителем E [2]. Покажем это с использованием свойств средней взаимной информации [20]:

$$I(\bar{g};(\bar{z}_1, \bar{z}_2)) = I(\bar{g};\bar{z}_1) + I(\bar{g};\bar{z}_2/\bar{z}_1) \ge I(\bar{g};\bar{z}_1) \quad (12)$$

Для того, чтобы этого избежать, необходимо ОС А при выполнении второй передачи снова генерировать сообщение $\bar{g}'$, где $\bar{g}' \in G^k$ (которое является кодовым словом асимптотического кода [21]) и передавать его. В этом случае вероятность выполнения неравенства (12) значительно уменьшится. После этого ОС A выбирает сформированный СК одного из ОС (например, с ОС B) за общий

СК и передает его другому ОС (например, ОС C) по каналу, закрытому с помощью СК, сформированного с этим ОС. Ранее было сказано, что имеется одно исключение. Рассмотрим ситуацию с формированием (передачей) $\bar{g}'$, где $\bar{g}' \in G^k$, когда КП находится в состоянии «обрыва», т.е. $p_w = 0{,}5$. Тогда неравенство (12) превращается в равенство, причем $I(\bar{g};(\bar{z}_1, \bar{z}_2)) = 0$, т.к. $\bar{z}_1$ и $\bar{z}_2$ статистически не зависят от $\bar{g}$. И тогда можно предположить, что нарушителя нет и для формирования СК можно использовать модель МПИ-1 из [1]. В этом случае χ_0 определятся из выражения для коэффициента асимптотического выигрыша по времени передачи сообщения по ДвШКБП κ_0, который приведен в [1].

Верхняя граница для χ_0 при $p_w = 0{,}5$ могла бы равняться 3, если ОС формируют СК с использованием МФШК-1 для которой $p_w = 0{,}5$, $p_y = 0$ и $p_m = 0$. Однако, случай для $p_w = 0{,}5$ исследован выше, поэтому χ_0 менее 3.

Если $p_y = 0$ (или $p_m = 0$), тогда χ_0 больше 1. Это объясняется тем, что в (7) первый множитель в числителе и знаменатель равны и сокращаются, а второй множитель в числителе будет всегда больше 1.

Анализ остальных значений таблиц 1 и 2 показывает, что при достаточно малых значениях вероятностей ошибок в составляющих ДвШКБП $p_y << 0$ и $p_m << 0$ показатель χ_0 больше 1. Однако, с ухудшением качества составляющих ДвШКБП $p_y \longrightarrow 0{,}5$ и (или) $p_m \longrightarrow 0{,}5$ χ_0 становится менее 1 (или вообще равен нулю, т.к. $C_3 = 0$) и соответственно при этих сочетаниях p_y и p_m использование МФШК-2 становится не эффективным. Объяснить это можно следующим образом. Введем коэффициент $K2$ из (9), равный отношению второго множителя числителя к произведению $C_{11}\,C_{12}$ ключевых пропускных способностей составляющих каналов ДвШКБП, описываемых моделями ДСКБП

$$K2 = \frac{(2h(p_w) - h(p_y) - h(p_m))}{(h(p_w)\,h(p_w) - h(p_y) - h(p_m) + h(p_y)\,h(p_m))}. \quad (13)$$

Анализ (13) показывает, что $K2 > 1$, т.к. второе слагаемое в (13) будет всегда больше 1, когда $C_3 > 0$, т.к. представляет собой отношение суммы ключевых пропускных способностей составляющих каналов ДвШКБП к их произведению. Коэффициент $K2$ определен при большем числе сочетаний p_y и p_m, если $p_w \longrightarrow 0{,}5$, и возрастает при увеличении p_y и p_m. При фиксированном p_w и увеличении p_y и p_m C_3 уменьшается быстрее (энтропийная функция ДвШКБП возрастает быстрее), чем возрастает коэффициент $K2$. Это приводит к тому, что коэффициент χ_0 уменьшается, что уменьшает область временной эффективности формирования СК в МФШК-2.

Заключение

Подводя итоги, отметим следующее. В работе исследована асимптотическая эффективность открытого сетевого ключевого согласования. В ходе научного поиска введено понятие асимптотической эффективности процесса формирования СК для трех ОС, которое описывается коэффициентом асимптотического выигрыша по времени формирования СК. Предложены модель и методика оценки асимптотической эффективности открытого сетевого ключевого согласования где, определяется коэффициент асимптотического выигрыша по времени формирования общего ключа для трех сетевых ОС. Возможны два варианта формирования СК. В первом случае СК может формироваться при поочередной передаче информации по каждому составляющему каналу ДШКБП, который соответствует формированию СК в модели Чисара и Кернера [5, 10]. После формирования ОС разных СК, ОС А формирует 2 закрытых канала, выбирает один из ключей за общий СК и передает его по закрытому каналу тому ОС, у которого другой ключ. Второй случай связан с формированием СК, когда ведется передача информации одновременно по обоим составляющим каналам ДШКБП. Модель, описывающая первый случай, названа моделью формирования СК № 1 (МФШК-1), а модель, описывающую второй случай – моделью формирования СК № 2 (МФШК-2). Одним из важнейших аспектов синтеза систем формирования СК является время формирования СК [22, 23, 24], т.к. это связано с информационными потерями, связанными с задержкой конфиденциальной информации, необходимой для передачи в сети, при компрометации СК и возникновении временных затрат на установление криптосвязности на новом СК для продолжения закрытого информационного обмена. Поэтому для МФШК-1 и МФШК-2 введен коэффициент асимптотического выигрыша по времени формирования СК для трех сетевых ОС χ_0, равный отношению времени формирования СК в МФШК-1 к времени формирования СК в МФШК-2 при выполнении заданных требований к формируемому СК и неограниченном увеличении длины СК. Оценки значений χ_0 для двоичного ДШКБП показывают, что при достаточно малых значениях вероятностей ошибок в составляющих ДСКБП χ_0 больше 1, что предопределяет преимущественные условия использования МФШК-2. Улучшение качества КП приводит к уменьшению области эффективного использования МФШК-2. Коэффициент ограничен интервалом значений $0 \le \chi_0 < 3$. Таким образом, высокое качество составляющих каналов ДСКБП определяет предпочтительное использование МФШК-2 в режиме

одновременного формирования СК. Полученные результаты углубляют ранее описанные результаты оценок эффективности различных известных моделей открытого ключевого согласования: Вайнера [25], Чисара и Кернера [5, 10], Мауера [8, 14], квантового согласования ключей [26, 27] и могут быть полезны исследователям для анализа различных перспективных подсистем информационной безопасности телекоммуникационных систем, включающих подсистемы управления криптографическими ключами [5] и криптографические системы защиты информации [8], для оценки и поиска путей достижения потенциальных возможностей по уменьшению времени восстановления криптографической связности объектов связи после компрометации сетевого ключа нарушителем.

Полученные результаты углубляют и расширяют известные теоретико-информационные оценки эффективности различных моделей ключевого согласования.

Литература

1. *Синюк А. Д., Тарасов А. А., Остроумов О. А. Метод оценки временной эффективности передачи информации дискретного широковещательного канала связи // Телекоммуникации. 2021. № 7. С. 10–17. DOI: 10.31044/1684-2588-2021-0-7-10-17. EDN JMFKNS.*
2. *Синюк А. Д., Остроумов, О. А. Оценка ключевой пропускной способности сети связи // Вестник компьютерных и информационных технологий. 2020. Т. 17. № 11(197). С. 47–54. DOI: 10.14489/vkit.2020.11. Pp. 047–054.*
3. *Zhang Qikun, Li Yongjiao, Gan Yong, Zheng Chuanyang, Luo Xiangyang, Zheng Jun Group Key Agreement Protocol Based on Privacy Protection and Attribute Authentication // IEEE Access. Volume: 7. Page(s): 87085–87096. DOI: 10.1109/ACCESS.2019.2926404.*
4. *Pinar Sen, Sung Hoon Lim, Young-Han Kim On the Optimal Achievable Rates for Linear Computation With Random Homologous Codes // IEEE Transactions on Information Theory (Volume: 66), Issue: 10, October 2020) Page(s): 6200–6221 Date of Publication: 20 July 2020 DOI: 10.1109/TIT.2020.3010253*
5. *Hongchao Zhou, Abbas El Gamal Network Information Theoretic Security with Omnipresent Eavesdropping // IEEE Transactions on Information Theory. Volume: 67. Issue: 12. December 2021. Page(s): 8280–8299. DOI: 10.1109/TIT.2021.3116962.*
6. *Onur Günlü, Rafael F. Schaefer, Holger Boche, H. Vincent Poor Secure and Private Distributed Source Coding With Private Keys and Decoder Side Information // IEEE Transactions on Information Forensics and Security (Volume: 18) Page(s): 3803–3816 Date of Publication: 14 June 2023. DOI: 10.1109/TIFS.2023.3286285*
7. *Tetsunao Matsuta; Tomohiko Uyematsu Coding Theorems for Asynchronous Slepian-Wolf Coding Systems // IEEE Transactions on Information Theory (Volume: 66), Issue: 8, August 2020), Page(s): 4774–4795, Date of Publication: 18 February 2020, ISSN Information: Print ISSN: 0018-9448 Electronic ISSN: 1557-9654, DOI: 10.1109/TIT.2020.2974736*
8. *Matthieu Bloch, Onur Günlü, Aylin Yener, Frédérique Oggier, H. Vincent Poor, Lalitha Sankar, Rafael F. Schaefer An Overview of Information-Theoretic Security and Privacy: Metrics, Limits and Applications // IEEE Journal on Selected Areas in Information Theory. Volume: 2. Issue: 1. March 2021. Page(s): 5–22. DOI: 10.1109/JSAIT.2021.3062755.*
9. *Остроумов О. А., Синюк А. Д. Пропускная способность широковещательного канала связи // Вестник компьютерных и информационных технологий. 2019. № 9 (183). С. 33–42. DOI: 10.14489/vkit.2019.09.pp.033-042.*
10. *Cheuk Ting Li; Venkat Anantharam One-Shot Variable-Length Secret Key Agreement Approaching Mutual Information // IEEE Transactions on Information Theory (Volume: 67), Issue: 8, August 2021) Page(s): 5509–5525 at of Publication: 09 June 2021 DOI: 10.1109/TIT.2021.3087963*
11. *Zhang Qikun, Li Yongjiao, Gan Yong, Zheng Chuanyang, Luo Xiangyang, Zheng Jun Group Key Agreement Protocol Based on Privacy Protection and Attribute Authentication // IEEE Access. Volume: 7. Page(s): 87085–87096. Date of Publication: 02 July 2019 Electronic ISSN: 2169-3536 INSPEC Accession Number: 18826825. DOI: 10.1109/ACCESS.2019.2926404.*
12. *Vamoua Yachongka, Hideki Yagi, Hideki Ochiai Key Agreement Using Physical Identifiers for Degraded and Less Noisy Authentication Channels // IEEE Transactions on Information Forensics and Security (Volume: 18) Page(s): 5316 – 5331, Date of Publication: 23 August 2023 DOI: 10.1109/TIFS.2023.3307976*
13. *Onur Günlü;Rafael F. Schaefer Controllable Key Agreement With Correlated Noise // IEEE Journal on Selected Areas in Information Theory (Volume: 2, Issue: 1, March 2021) Page(s): 82–94 Date of Publication: 25 January 2021 Electronic ISSN: 2641-8770 DOI: 10.1109/JSAIT.2021.3054035*
14. *Mohamed Nafea, Aylin Yener Generalizing Multiple Access Wiretap and Wiretap II Channel Models: Achievable Rates and Cost of Strong Secrecy // IEEE Transactions on Information Theory. Volume: 65. Issue: 8. August 2019. Page(s): 5125 – 5143. DOI: 10.1109/TIT.2019.2908832.*
15. *Остроумов О. А., Синюк А. Д. Информационная скорость формирования сетевого ключа по открытым виртуальным каналам связи // Вопросы кибербезопасности. 2023. № 3(55). с. 78–89. DOI: 10.21681/2311-3456-2023-3-78-89.*
16. *Anuran Makur Coding Theorems for Noisy Permutation Channels // IEEE Transactions on Information Theory (Volume: 66, Issue: 11, November 2020) Page(s): 6723–6748 Date of Publication: 16 July 2020. DOI: 10.1109/TIT.2020.3009468*
17. *Haoheng Yuan, Yanghe Feng, Chuanchuan Yang, Zhuojun Zhuang, Bin Dai Two-User Gaussian Broadcast Wiretap Channel With Common Message and Feedback: Revisit // IEEE Transactions on Information Forensics and Security (Volume: 19) Page(s): 178–193 Date of Publication: 25 September 2023. DOI: 0.1109/TIFS.2023.3318948*
18. *Meryem Benammar, Pablo Piantanida, Shlomo Shamai on the Compound Broadcast Channel: Multiple Description Coding and Interference Decoding // IEEE Transactions on Information Theory (Volume: 66). Issue: 1, January 2020) Page(s): 38–64 Date of Publication: 23 September 2019. DOI: 10.1109/TIT.2019.2942615*
19. *Alejandro Cohen, Rafael G. L. D'Oliveira, Salman Salamatian, Muriel Médard Network Coding-Based Post-Quantum Cryptography // IEEE Journal on Selected Areas in Information Theory (Volume: 2, Issue: 1, March 2021) Page(s): 49 – 64 Date of Publication: 26 January 2021 Electronic ISSN: 2641-8770. DOI: 10.1109/JSAIT.2021.3054598*

20. *Cheuk Ting Li, Venkat Anantharam One-Shot Variable-Length Secret Key Agreement Approaching Mutual Information // IEEE Transactions on Information Theory. Volume: 67. Issue: 8. August 2021. Page(s): 5509–5525. DOI: 10.1109/TIT.2021.3087963.*
21. *Vidhi Rana, Rémi A. Chou, Hyuck M. Kwon Information-Theoretic Secret Sharing From Correlated Gaussian Random Variables and Public Communication // IEEE Transactions on Information Theory (Volume: 68), Issue: 1, January 2022) Page(s): 549–559 Date of Publication: 27 October 2021. DOI: 0.1109/TIT.2021.3122808*
22. *Starostin V., Korzhik V., Kabardov M., Gerasimovich A., Yakovlev V., Morales-Luna G Key generation protocol executing through non-reciprocal fading channels // International Journal of Computer Science and Applications. 2019. Т. 16. № 1. С. 1–16.*
23. *Синюк А. Д., Тарасов А. А., Остроумов О. А. Теоретико-информационное представление виртуализации сетевого канала перехвата // Информатика и автоматизация. 2023. Т. 2. № 4. с. 721–744. DOI: 10.15622/ia.22.4.1.*
24. *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.*
25. *Amin Gohari, Onur Günlü, Gerhard Kramer Coding for Positive Rate in the Source Model Key Agreement Problem // IEEE Transactions on Information Theory. Volume: 66. Issue: 10. October 2020. Page(s): 6303–6323. DOI: 10.1109/TIT.2020.2990750.*
26. *Ignazio Pedone, Andrea Atzeni, Daniele Canavese, Antonio Lioy Toward a Complete Software Stack to Integrate Quantum Key Distribution in a Cloud Environment // IEEE Access (Volume: 9) Page(s): 115270–115291 Date of Publication: 03 August 2021 Electronic ISSN: 2169-3536 DOI: 10.1109/ACCESS.2021.3102313*
27. *Yi Luo; Hao-Kun Mao; Qiong Li; Nan Chen An Information-Theoretic Secure Group Authentication Scheme for Quantum Key Distribution Networks // IEEE Transactions on Communications (Volume: 71), Issue: 9, September 2023) Page(s): 5420–5431. Date of Publication: 29 May 2023. DOI: 10.1109/TCOMM.2023.3280561*