**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ**

УДК 004.62

# О ТЕХНОЛОГИИ РАСПРЕДЕЛЕННОЙ ПЕРЕДАЧИ ДАННЫХ И ПРОБЛЕМАХ ПРОВЕРКИ ДОСТОВЕРНОСТИ ИНФОРМАЦИИ ПО КАНАЛУ СВЯЗИ[1]

*Статья поступила в редакцию 26.08.2021, в окончательном варианте – 19.10.2021.*

***Багдасарян Рафаэль Хачикович***, Краснодарский государственный институт культуры, 350072, Российская Федерация, г. Краснодар, ул. 40-летия Победы, 33,
кандидат технических наук, e-mail: rafael_555@mail.ru
***Осипян Валерий Осипович***, Кубанский государственный университет, 350040, Российская Федерация, г. Краснодар, ул. Ставропольская, 149,
доктор физико-математических наук, доцент, ORCID 0000-0001-6558-7998, e-mail: v.osippyan@gmail.com
***Литвинов Кирилл Игоревич,*** Кубанский государственный университет, 350040, Российская Федерация, г. Краснодар, ул. Ставропольская, 149,
аспирант, e-mail: lyrik-1994@yandex.ru
***Сергеев Александр Евгеньевич***, Краснодарский государственный институт культуры, 350072, Российская Федерация, г. Краснодар, ул. 40-летия Победы, 33,
магистрант, e-mail: alex_serg88@bk.ru
***Шокола Елена Игоревна***, Краснодарский государственный институт культуры, 350072, Российская Федерация, г. Краснодар, ул. 40-летия Победы, 33,
магистрант, e-mail: shokola.1998@mail.ru

Статья посвящена проблеме проверки достоверности информации при ее передаче по незащищенным каналам связи, обозреваются технология и особенности передачи информации, демонстрируется преимущество использования и применения в распределенной информационной системы. Представлены модели передачи данных и проверки достоверности в открытых сетях и каналах связи с использованием алгоритмов симметричного и асимметричного преобразования информации. Приведена схема распределенной системы передачи информации с использованием гибридного преобразования. Его преимущество заключается в возможностях синтеза преимуществ систем, в работе которых используется открытый ключ с производительностью, которую может предоставить симметричная система. Симметричным методом происходит шифрование данных, а ассиметричным ключом зашифровывается сам ключ с зашифрованными данными, что позволяет обеспечить дополнительную защиту передаваемой информации. В предлагаемом методе сочетаются как высокая производительность криптосистем, так и преимущества в области уровня защиты ассиметричных методов. Технологию распределенной передачи данных и проверки достоверности сведений по общедоступной линии передачи необходимо описать множественной моделью, которая имеет функции, информационные элементы и их группы. Представленный способ дает возможность обеспечить надежность и высокую степень защиты данных при их передаче в открытых сетях.

**Ключевые слова:** передача данных, достоверность информации, прямое преобразование, обратное преобразование, канал связи, информационная система, распределенная информационная система, база данных, ключ, аутентикация, открытая сеть, симметричное преобразование информации, асимметричное преобразование информации

# ABOUT THE TECHNOLOGY OF DISTRIBUTED DATA TRANSMISSION AND THE PROBLEMS OF VERIFYING THE RELIABILITY OF INFORMATION OVER A COMMUNICATION CHANNEL

*The article was received by the editorial board on 26.08.2021, in the final version – 19.10.2021.*

***Bagdasaryan Rafael Kh.***, Krasnodar State Institute of Culture, 33 40-letiya Pobedy St., Krasnodar, 350072, Russian Federation,
Cand. Sci. (Engineering), e-mail: rafael_555@mail.ru
***Osipyan Valeriy O.***, Kuban State University, 149 Stavropolskaya St., Krasnodar, 350040, Russian Federation,
Doct. Sci. (Physics and Mathematics), Associate Professor, ORCID 0000-0001-6558-7998, e-mail: v.osippyan@gmail.com

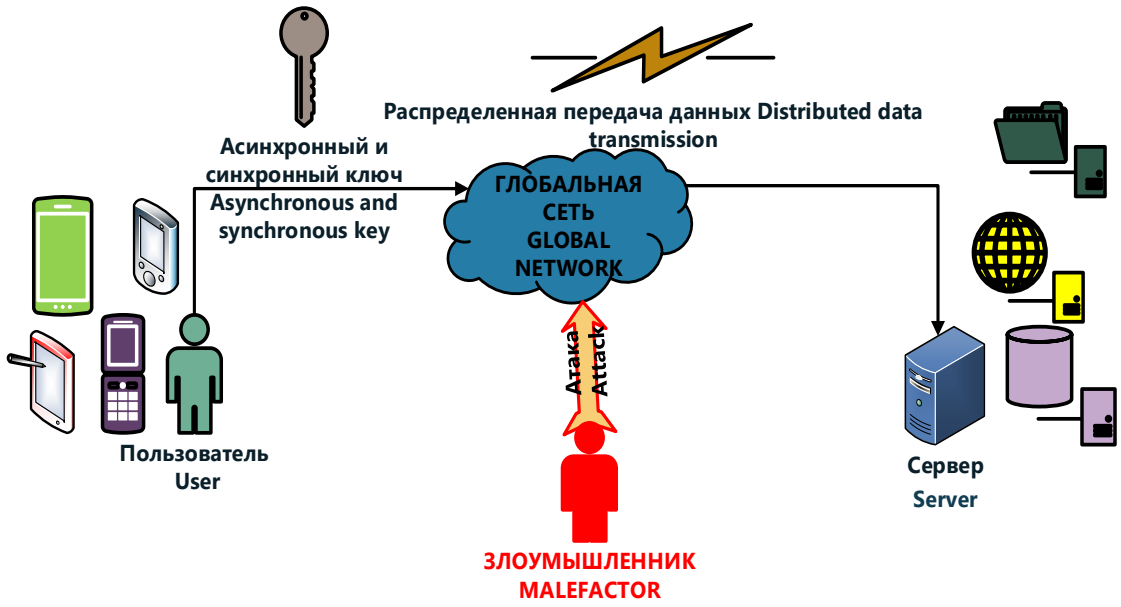
[1] Работа поддержана грантом РФФИ № 19-01-00596.

***Litvinov Kirill I.***, Kuban State University, 149 Stavropolskaya St., Krasnodar, 350040, Russian Federation,
postgraduate student, e-mail: lyrik-1994@yandex.ru
***Sergeev Alexander E.***, Krasnodar State Institute of Culture, 33 40-letiya Pobedy St., Krasnodar, 350072, Russian Federation,
undergraduate student, e-mail: alex_serg88@bk.ru
***Shokola Elena I.,*** Krasnodar State Institute of Culture, 33 40-letiya Pobedy St., Krasnodar, 350072, Russian Federation,
undergraduate student, e-mail: shokola.1998@mail.ru

The article is devoted to the problem of verifying the reliability of information during its transmission through unprotected communication channels, the technology and features of information transfer are reviewed, the advantage of using and applying in a distributed information system is demonstrated. Models of data transmission and validation in open networks and communication channels are presented, using algorithms for symmetric and asymmetric information transformation. A diagram of a distributed information transmission system with using hybrid transformation. Its advantage lies in the ability to synthesize the advantages of systems that use a public key with the performance that a symmetric system can provide. The data is encrypted using a symmetric method, and the key itself with encrypted data is encrypted with an asymmetric key, which allows for additional protection of the transmitted information. The proposed method combines both high performance of cryptosystems and advantages in the area of the protection level of asymmetric methods. The technology of distributed data transmission and validation of information over a public transmission line must be described by a multiple model, which has functions, information elements and their groups. The presented method makes it possible to ensure the reliability and high degree of data protection during their transmission in open networks.

**Keywords:** transmission, information reliability, direct transformation, inverse transformation, communication channel, information system, distributed information system, database, key, authentication, open network, symmetric information transformation, asymmetric information transformation

**Графическая аннотация (Graphical annotation)**




**Введение.** Планомерное развитие человеческого общества неразрывно связано с накоплением информации и ее сохранением. С ростом глобализации, возрасла роль обмена данных с использованием информационных носителей и распеделенных технологий. По мере развития средств информационного обмена, стали развиваться и способы ее защиты. Появлялось бесчисленное количество методов шифрования сообщений. Чаще всего шифрованию подвергались военные сообщения и доклады, прочтение которых третьими лицами нельзя было допустить ни в коем случае. Однако в связи с тем, что один и тот же шифр начинали использовать большое количество людей, а также находились способы дешифровки без наличия ключа методом прослеживания определенных алгоритмов, шифры усложнялись. Возникала потребность в более тщательной защите информации. Востребованность сетевого информационного обмена создаёт потребность в систематизации и упорядочивании информационных ресурсов, с сохранением возможности интуитивного использования компьютерного интерфейса. В случае регулярных сбоев в системе распределения

информации по базам данных (БД), использование открытых сетей стало бы невозможным. Перед специалистами IT встают важные задачи распределения и обеспечения безопасности передаваемых данных по каналам связи. Последнее является наиболее значимым, поскольку с расширением использования сети Интернет, увеличилось и пространство для мошенничества и киберугроз. На современном этапе необходимо обеспечить непрерывную актуализацию накопленных знаний по обеспечению информационной безопасности и разработку новых. Безопасность информации подвергается как преднамеренным, так и непреднамеренным угрозам. К непреднамеренным угрозам можно отнести угрозы стихийных бедствий, непредсказуемых поломок и сбоев программных средств. Однако преднамеренные угрозы связаны непосредственно с незаконными действиями злоумышленников и получением информации третьим лицом. Результатом получения информации злоумышленником могут быть как использование шпионских программ, так и непрофессиональные действия ответственных за сохраненность конфиденциальной информации. Таким образом сегодня существует потребность в создании и совершенствовании криптографических систем и совершенствовании имеющихся методов сохранения информации.

Криптография внедрена во все сферы жизнидеятельности человечества: передаваемые через современные мессенджеры сообщения проходят процедуру шифрования, также активно используются QR-коды для оплаты и идентификации устройств. Интернет является как удобным методом быстрой передачи информации, так и крайне уязвимым без использования шифрования [2]. Несмотря на преимущества единого информационного пространства, возникает и ряд угроз, возникающих при отправке сведений, находящихся на распределенных серверах БД. Одной из главных является утечка информации неавторизированным лицам, во избежания этого, данные преобразуются для передачи, однако и это не гарантирует полную защищенность [4].

**Модель распределенной передачи данных.** Обеспечение безопасности информации при передачи по открытым сетям на современном этапе развития является очень востребованной задачей. Использование открытых сетей требует использования внедрения новейших механизмов и алгоритмов авторизации и аутентикации клиент-пользователей. Под распределенной информационной системой будем понимать удаленные друг от друга множества баз данных, имеющих общие параметры. Использование параметров уровня БД позволяет производить настройку нескольких конфигураций баз данных на уровне отдельных БД.

При пользовании общедоступных каналов связей и отправке закрытых данных в первую очередь они нуждаются в преобразовании. Под шифрованием понимается преобразование информации в целях защиты от прочтения неавторизованными лицами и недопущения кражи информации, но при этом предоставление данных авторизованным пользователям. Шифрование на современном этапе развития – это основной метод защиты информации. Без шифрования распределенные информационные системы, используемые сейчас во многих областях жизни человека, становятся крайне уязвимыми к перехвату конфиденциальной информации третьими лицами. В современной теории информационных процессов и систем, распределенная информационная система трактуется как совокупность аппаратных и программных средств, выполняющих основные процессы по работе с данными, а точнее их хранение, накопление, передачу и обработку. С помощью единой системы обеспечивается работа с единым массивом данных пользователей, расположенных территориально удаленными друг от друга и использующих разные сервера, программные платформы и форматы хранения. Таким образом, при помощи системы осуществляется шифрование и расшифровка, а также интеграция данных с другими системами. Эти процессы происходят автоматически, предоставляя пользователям работу с удобным интуитивным интерфейсом. Современные системы шифрования позволяют совершать процесс шифровки и дешифровки сообщений, не снижая скорость передачи сообщения, но вместе с этим надежно защищая и не допуская перехват информации неавторизованными лицами.

Масштабируемость и отказоустойчивость являются отличительными особенностями распределенной информационной системы. Под масштабируемостью понимается возможность беспрепятственного апгрейда вычислительных машин, а отказоустойчивость характеризуется обязательным выполнением распределенных вычислений программ даже при неисправности вычислительных узлов [3, 7]. Масштабируемость также дает рентабельность информационной распределенной системе – несмотря на высокую стоимость, система быстро обретает преимущество над традиционной за счет быстрого наращивания вычислительной мощности.

Структурными элементами модели распределенной передачи данных являются [7]:

$F = \{f_i \mid i = \overline{1,I}\}$ – множество функций, используемых при распределенной передачи данных (табл. 1);

$D = \{d_j \mid j = \overline{1,J}\}$ – множество информационных элементов, используемых при распределенной передачи данных (табл. 2).

Далее в таблицах 1 и 2 приведены множества и информационных элементы, применяемые при распределенной отправке данных [7].

Таблица 1 – Элементы множества функций, используемые при распределенной передаче информации

| Обозначение множеств | Описание | Входная информация функции | Выходная Информация функции | Обозначение на рисунке 3 |
|---|---|---|---|---|
| $f_1$ | генерация ключей клиента | $t$ – тип генерируемых ключей: 0 – пара из открытого и закрытого ключа клиента, 1 – транзакционный ключ клиента | пара из открытого и закрытого ключа клиента или транзакционный ключ клиента | |
| $f_2$ | генерация ключей сервера | $t$ – тип генерируемых ключей: 0 – пара из открытого и закрытого ключа сервера, 1 – транзакционный ключ сервера | пара из открытого и закрытого ключа сервера или транзакционный ключ сервера | |
| $f_3$ | отправка сообщений клиенту | отправка информации | | ← |
| $f_4$ | отправка сообщений серверу | отправка информации | | → |
| $f_5$ | сохранение информации в бд | сохраняемая информация | | |
| $f_6$ | симметричное преобразование | $f_6(m,k)$: $m$ – исходное сообщение, $k$ – ключ | $c$ – преобразованное сообщение | $E1(m,k)$ |
| $f_7$ | асимметричное преобразование | $f_7(m,e)$: $m$ – исходное сообщение, $e$ – открытый ключ | $c$ – преобразованное сообщение | $E2(m,e)$ |
| $f_8$ | обратное симметричное преобразование | $f_8(c,k)$: $c$ – преобразованное сообщение, $k$ – ключ | $m$ – исходное сообщение | $D1(c,k)$ |
| $f_9$ | обратное асимметричное преобразование | $f_9(c,d)$: $c$ – преобразованное сообщение, $d$ – закрытый ключ | $m$ – исходное сообщение | $D2(c,d)$ |
| $f_{10}$ | проверка подлинности | $f_{10}(a,b)$: $a$ и $b$ – данные для сравнения | true или false | |

Таблица 2 – Информационные элементы используемые при распределенной передачи данных

| Обозначение элементов | Описание | Обозначение на рисунке 3 |
|---|---|---|
| $x_1$ | открытый ключ клиента | $e_1$ |
| $x_2$ | закрытый ключ клиента | $d_1$ |
| $x_3$ | транзакционный ключ клиента | $k$ |
| $x_4$ | открытый ключ сервера | $e_2$ |
| $x_5$ | закрытый ключ сервера | $d_2$ |
| $x_6$ | транзакционный ключ сервера | $k_2$ |
| $x_7$ | идентификатор пользователя | ID/ID1 |
| $x_8$ | отпечаток пользователя | |
| $x_9$ | пароль пользователя | PWD/PWD1 |
| $x_{10}$ | список серверов приема данных | LIST |
| $x_{11}$ | сообщение клиенту | |
| $x_{12}$ | хэш-сумма сообщения | HASH |
| $x_{13}$ | метка времени отправки | TIME |

Расположенные ниже отношения между множествами функций и информационными элементами применяются при отправке сведений, кортежи отношений определяются использованием функций, поэтому ниже продемонстрирована логическая матрица их взаимосвязи [7].

| | $x_1$ | $x_2$ | $x_3$ | $x_4$ | $x_5$ | $x_6$ | $x_7$ | $x_8$ | $x_9$ | $x_{10}$ | $x_{11}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $f_1$ | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $f_2$ | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| $f_3$ | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| $f_4$ | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 |
| $f_5$ | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| $f_6$ | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 |
| $f_7$ | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 |
| $f_8$ | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 |
| $f_9$ | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 |
| $f_{10}$ | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 |

Используя матрицы смежности, можно задать структуру предметной области. У представленной выше матрицы отсутствуют строки и столбцы с поэлементной суммой, равной 0, поэтому, исходя из этих данных, можно сделать определенные выводы [7]:

- не существует таких функций множества *F*, которым не соответствовал хотя бы один информационный элемент множества *D*:

$$\forall i, i = \overline{1, P(F)}: \sum_{i=1}^{P(F)} (f\mathrm{x})_i > 0;$$

- не существует таких информационный элемент множества *D*, которым не соответствовала хотя бы одна функция множества *F*:

$$\forall j, j = \overline{1, P(D)}: \sum_{j=1}^{P(D)} (f\mathrm{x})_j > 0.$$

При использовании матриц и графов задается структура предметной области.

В таблице 3 показан состав переменных групп информационных элементов. Рисунок 1 представляет систему грифов взаимодействия.

Таблица 3 – Состав переменных

| Группы | Информационные элементы |
|---|---|
| $\mathrm{x}_1^{\mathrm{гр}}$ | $\mathrm{x}_1, \mathrm{x}_2, \mathrm{x}_3$ |
| $\mathrm{x}_2^{\mathrm{гр}}$ | $\mathrm{x}_4, \mathrm{x}_5, \mathrm{x}_6$ |
| $\mathrm{x}_3^{\mathrm{гр}}$ | $\mathrm{x}_7, \mathrm{x}_8, \mathrm{x}_9$ |

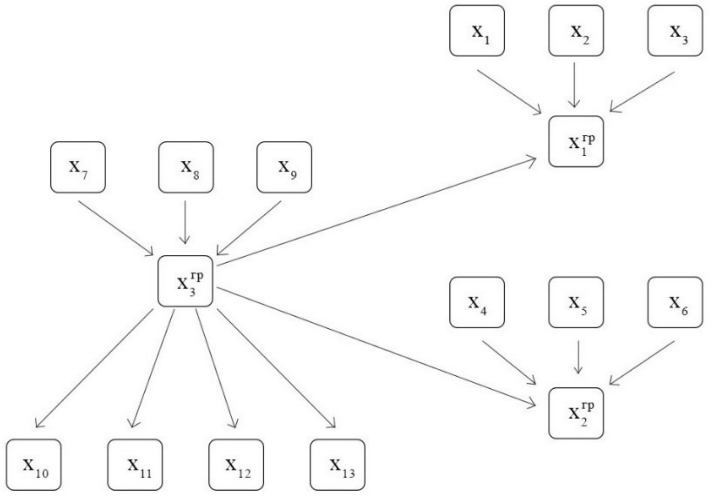



Рисунок 1 – Схематическая система графов ИС

Далее представленная ниже схема (рис. 2) применяет гибридное шифрование с распределенной передачей данных БД. Используемая система совмещает в себе преимущества симметричных систем и с открытым каналом связи [5, 6]. Передача данных осуществляется с использованием транзакционных, открытых и закрытых ключей, каждый из которых обладает уникальными преимуществами. Так, первый из перечисленных ключей позволяет дешифровать данные в симметрическом прямом

преобразовании, а два других используются для безопасного обмена данными [8]. В данной системе симметричный ключ используется при непосредственном прямом преобразовании данных, а ассиметричным ключом шифруется используемый симметричный ключ.

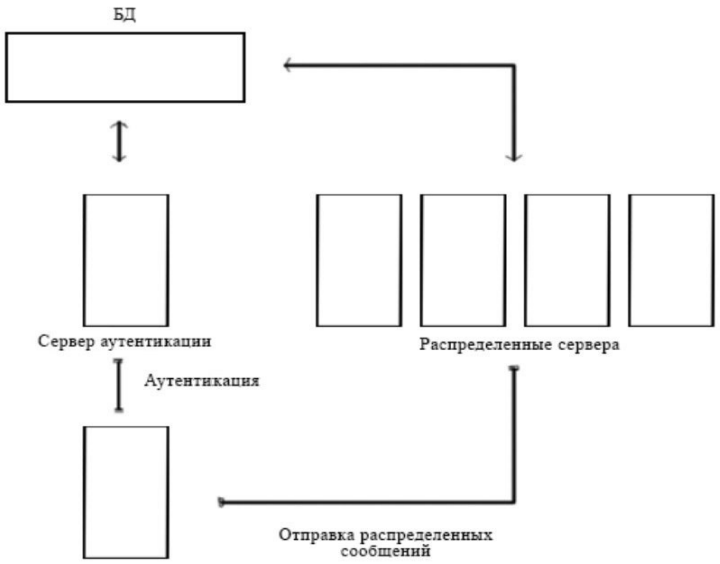



Рисунок 2 – Система передачи информации

**Алгоритмы распределенной передачи данных и ее проверки достоверности по открытым каналам связи.** На рисунке 3 представлен алгоритм процесса аутентикации клиента при инициализации обмена и передачи данных по открытым каналам связи, который выполняется пошагово следующим образом:

1. Генерируется пара ключей открытого и закрытого типа $\{e_1, d_1\}$. После данной процедуры клиент осуществляет передачу сообщения серверу аутентикации. Данное сообщение включает в себя логин (идентификатор) отправителя ID и открытый ключ клиента $e_1$.

2. В базу данных сервера поступает открытый ключ $e_1$. Происходит генерация пары ключей сервера (открытый и закрытый ключ) $\{e_2, d_2\}$. Клиент получает отчет, в котором кроится открытый серверный ключ.

3. Далее формируется транзакционный ключ $k$ и шифруется пароль PWD (биометрия пользователя, например любой палец одной руки) с использованием этого ключа $k$ и симметричного метода. Данное сообщение зашифровывается открытым ключом сервера $e_2$ и отправляется серверу.

4. Сервер раскрывает сообщение с помощью закрытого ключа $d_2$. Далее сервер расшифровывает PWD, используя ключ через $k$ симметричным методом. Сервер аутентикации производит проверку логина и пароля. При верных элементах генерируется транзакционный ключ $k_2$. Данным ключом зашифровывается список имеющихся серверов, которые принимают сообщения. Сервер аутентикации проверяет в свою очередь присланный пароль и пароль, хранящийся на сервере. Если данные элементы оказываются верны, сервер гененрирует транзакционный ключ $k_2$, которым зашифровывается список серверов LIST, принимающих данные пользователя-клиента. Принятое сведение шифруется ассиметричным алгоритмом благодаря открытому клиентскому ключу $e_1$ и пересылается ему.

Однако, если логин и пароль не совпадают, пользователь получает информацию в форме сообщения о произошедшей ошибке при аутентикации.

5. Клиент расшифровывает сообщение с помощью закрытого ключа $d_1$. Затем происходит процедура расшифровки списка серверов с использованием симметричного метода и транзакционного ключа $k_2$.

6. При проведении успешной аутентикации происходит идентификация клиента благодаря логину/паролю. Когда происходит авторизация, пользователю открывается доступ к разным серверам для дальнейшей отправки информации. Поэтому при новой отсылке данных будет сгенерирован новейший уникальный транзакционный ключ. По прошествии часа сервер вновь запросит пройти аутентикацию [9].

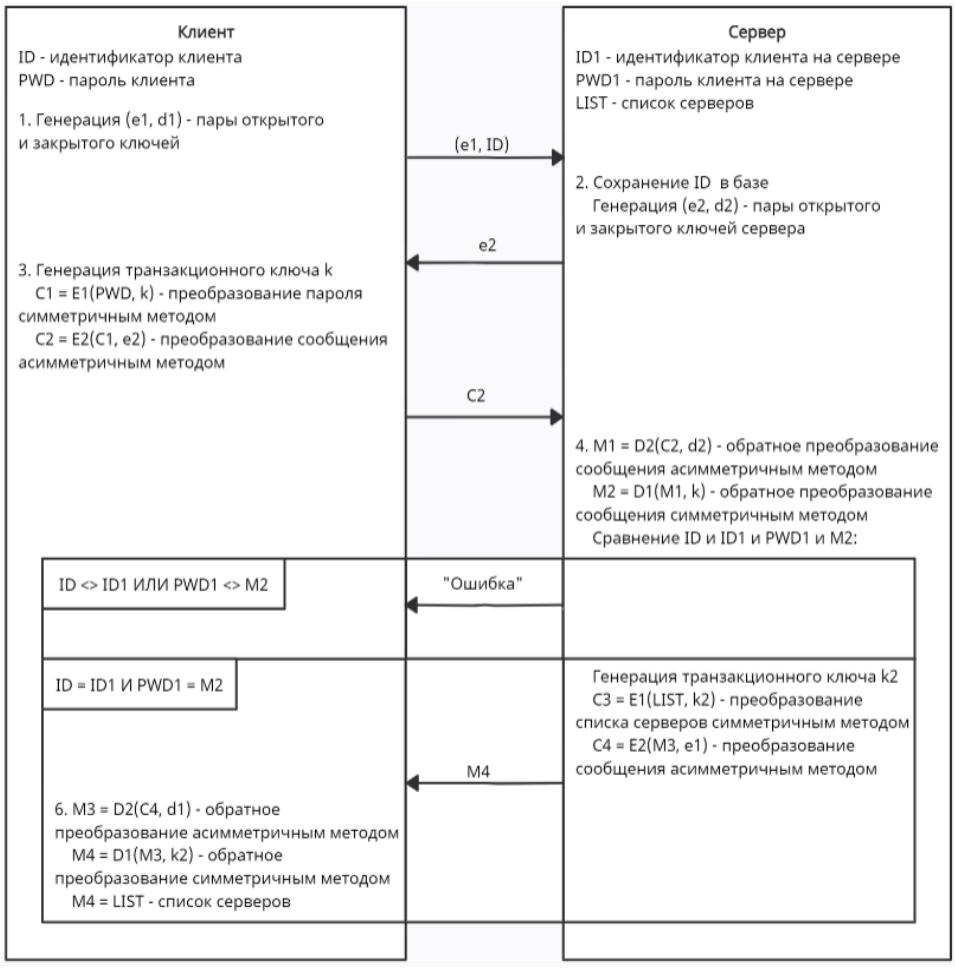



Рисунок 3 – Алгоритм процесса аутентикации клиента при инициализации обмена и передачи данных по открытым каналам связи

На современном этапе развития проблема шифрования информации при ее передачи наиболее актуальна при использовании мобильных приложений. Далее рассмотрим как происходит работа сервера с мобильным приложением. Запрос с определенными параметрами передается серверу и ожидается ответ [10]. Из списка доступных серверов выбирается случайный сервер, куда осуществляется передача данных. Если в течение 30 секунд от сервера не поступает ответ, приложение отправляет сообщение следующему доступному файлсерверу БД [11].

Далее представлен еще один метод отсылки сведений по общедоступным каналам связи при передаче информации удаленной серверной БД (рис. 4):

1. Начинается генерирование транзакционного ключа $k$ и зашифровывается симметричным способом хеш-сумма передаваемой информации. Соответственно преобразовывается и количество данных $m$. После чего, принятые сведения шифруются ассиметричным методом с применением открытого ключ $e_2$. Полученные данные направляются случайной серверной БД из списка; если нет ответа в течение 30 секунд, то сообщение направляется в другой случайный сервер [7].

2. Происходит разбивание сообщения на $n$ фрагментов. Каждый фрагмент приобретает через прямое преобразование метку времени отправки. Каждый из фрагментов шифруется симметричным методом через ключ $k$. После чего принятые сведения зашифровываются открытым ключом $e_2$ и передаются в заданном ранее порядке [7].

3. После принятых данных с серверных БД клиенту приходит отчет об успешном завершении алгоритма; если же отчета нет, то сведения переадресуются с неизменной меткой времени на сторонний сервер БД [7].

4. Приняв команду, сервер БД передает полученную информацию в центральную БД. На данном этапе сервер расшифровки расшифровывает транзакционный ключ $k$, используя закрытый ключ сервера $d_2$. Данная расшифровка производится ассиметричным методом.

5. В последнюю очередь собирается исходное сообщение и сверяется хэш-сумма. После данных действий происходит ответ клиенту.

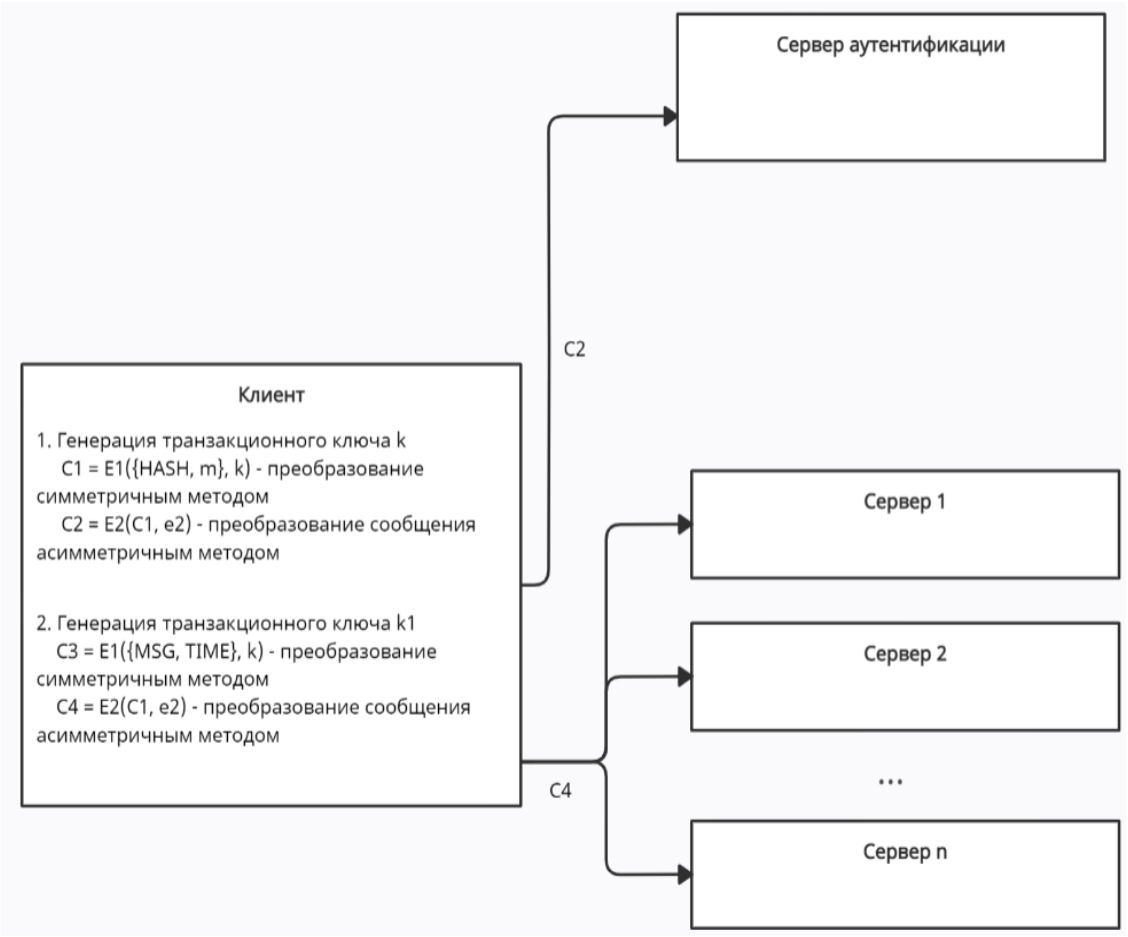



Рисунок 4 – Схематическое представление отправки данных по общедоступным каналам связи при передаче информации серверной БД

**Заключение.** На современном этапе передача информации посредством сети Интернет является наиболее популярной и безопасной. Стоит отметить, что развитие систем информационной безопасности – это непрерывный и важный процесс, поскольку информационные угрозы также будут возникать и развиваться. Технологию распределенной передачи данных и проверки достоверности информации по открытому каналу связи можно представить множественной моделью, которая подробно приведена в статье. Продемонстрированная авторами технология обмена информацией по общедоступным линиям передач, обладает высокой степенью безопасности при операциях шифрования/дешифрования и увеличивает надежность передачи данных за счет распределенной передачи данных на необходимое количество серверов.

**Библиографический список**

1. Атрощенко, В. А. К вопросу разработки алгоритма передачи закрытых данных по открытым сетям между мобильным устройством и распределенными серверами / В. А. Атрощенко, Р. А. Дьяченко, М. В. Руденко, Р. Х. Багдасарян // III Международная научно-практическая конференция молодых ученых, посвященная 52-й годовщине полета Ю.А. Гагарина в космос : сборник научных статей. – Краснодар : ООО «Издательский дом – Юг», 2013. – С. 327–331.

2. Атрощенко, В. А. К вопросу повышения защищенности информационных биллинговых систем / В. А. Атрощенко, М. В. Руденко, Р. А. Дьяченко, Р. Х. Багдасарян // Научные чтения имени профессора Н.Е. Жуковского : сборник научных статей IV Международной научно-практической конференции. – Краснодар : ООО «Издательский Дом – Юг», 2014. – С. 126–129.

3. Атрощенко, В. А. К вопросу оценки достоверности информации для предотвращения MITM-атаки при передаче закрытой информации по открытым каналам связи / В. А. Атрощенко, М. В. Руденко, Р. А. Дьяченко, Р. Х. Багдасарян // Современные проблемы науки и образования. – 2013. – № 3. – С. 82.

4. Багдасарян, Р. Х. О разработке метода проверки достоверности данных при передаче информации Р. Х. Багдасарян, В. О. Осипян, Е. П. Лукащик, С. Г. Синица, А. С. Жук, К. И. Литвинов // Прикаспийский журнал: управление и высокие технологии. – 2019. – № 2 (46). – С. 143–152.

5. Багдасарян, Р. Х. О современных проблемах проверки достоверности данных при передаче информации и компрометации канала связи / Р. Х. Багдасарян, В. О. Осипян // IX Международная научно-практическая конференция молодых ученых, посвященная 58-й годовщине полета Ю. А. Гагарина в космос : сборник научных статей. – 2019. – С. 289–291.

6. Багдасарян, Р. Х. К вопросу о защите и проверке достоверности информации при ее передаче по открытым каналам связи / Р. Х. Багдасарян, В. О. Осипян // Прикаспийский журнал: управление и высокие технологии. – 2020. – № 2 (50). – С. 127–135.

7. Руденко, М. В. Информационная система мобильных устройств для оплаты коммунальных услуг : дис. … канд. техн. наук / М. В. Руденко. – Краснодар : Кубанский государственный технологический университет, 2016.

8. Холкин, Д. О. Метод передачи сообщений с использованием лучших способов организации обмена данными и криптографических протоколов обмена мгновенными сообщениями с использованием сквозного шифрования / Д. О. Холкин, М. А. Маслова, А. С. Дмитриев // Инженерный вестник Дона. – 03.06.2021. – № 6. – Режим доступа: www.ivdon.ru/ru/magazine/archive/n6y2021/7054, свободный. – Заглавие с экрана. – Яз. рус.

9. Скоба, А. Н. Решение задачи обеспечения оптимальной эффективности функционирования распределенных систем обработки информации / А. Н. Скоба, В. К. Михайлов, Айеш Ахмед Нафеа Айеш // Инженерный вестник Дона. – 03.06.2021. – № 6. – Режим доступа: www.ivdon.ru/ru/magazine/archive/n6y2021/7053, свободный. – Заглавие с экрана. – Яз. рус.

10. Chor, B. A Krapsack-type pubkie key cryptosystem based on arithmetic in finite fields / B. Chor, R. Rivest // IEEE Transactions on Information Theory. – 1988. – Vol. 34. – P. 901–909.

11. Osipyan, V. O. Development of information security system mathematical models by the solutions of the multigrade diophantine equation systems / V. O. Osipyan, K. I. Litvinov, R. Kh. Bagdasaryan, E. P. Lukashchik, S. G. Sinitsa, A. S. Zhuk // International Conference Proceeding Series, Association for Computing Machinery. – 2019.

**References**

1. Atroschenko, V. A., Dyachenko, R. A., Rudenko, M. V., Bagdasaryan, R. Kh. K voprosu razrabotki algoritma peredachi zakrytykh dannykh po otkrytym setyam mezhdu mobilnym ustroystvom i raspredelennymi serverami [On the development of an algorithm for transmitting private data on open networks between a mobile device and distributed servers]. *III Mezhdunarodnaya nauchno-prakticheskaya konferentsiya molodykh uchenykh, posvyashchennaya 52-y godovshchine poleta Yu.A. Gagarina v kosmos : sbornik nauchnykh statey* [III International Scientific and Practical Conference of Young Scientists dedicated to the 52nd anniversary of the flight of Yu.A. Gagarin in space : proceedings]. Krasnodar, “Publishing House – South” LLC, 2013, pp. 327–331.

2. Atroschenko, V. A., Rudenko, M. V., Dyachenko, R. A., Bagdasaryan, R. Kh. K voprosu povysheniya zashchishchennosti informatsionnykh billingovykh sistem [On the issue of increasing the security of information billing systems]. *Nauchnye chteniya imeni professora N.E. Zhukovskogo : sbornik nauchnykh statey IV Mezhdunarodnoy nauchno-prakticheskoy konferentsii* [Scientific readings named after Professor N.Ye. Zhukovsky : proceedings of the IV International Scientific Practical Conference]. Krasnodar, “Publishing House – South” LLC, 2014, pp. 126–129.

3. Atroshhenko, V. A., Rudenko, M. V., Dyachenko, R. A., Bagdasaryan, R. Kh. K voprosu otsenki dostovernosti informatsii dlya predotvrashheniya MITM-ataki pri peredache zakrytoy informatsii po otkrytym kanalam svyazi» [«On the issue of assessing the reliability of information to prevent MITM attacks when transmitting classified information over open communication channels»]. *Sovremennye problemy nauki i obrazovaniya* [Modern Problems of Science and Education], 2013, no. 3, p. 82.

4. Bagdasaryan, R. Kh., Osipyan, V. O., Lukashchik, E. P., Sinitsa, S. G., Zhuk, A. S., Litvinov, K. I. O razrabotke metoda proverki dostovernosti dannykh pri peredache informatsii [On the development of a method for checking the reliability of data when transferring information]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Control and High Technologies], 2019, no. 2 (46), pp. 143–152.

5. Bagdasaryan, R. Kh., Osipyan, V. O. O sovremennykh problemakh proverki dostovernosti dannykh pri peredache informatsii i komprometatsii kanala svyazi [On modern problems of data validation when transmitting information and compromising a communication channel] *IX mezhdunarodnaya nauchno-prakticheskaya konferentsiya molodykh uchenykh, posvyashchennaya 58-y godovshchine poleta Yu. A. Gagarina v kosmos : sbornik nauchnykh statey* [IX International Scientific and Practical Conference of Young Scientists, dedicated to the 58th anniversary of Yu. A. Gagarin into space], 2019, pp. 289–291.

6. Bagdasaryan, R. Kh., Osipyan, V. O. K voprosu o zashchite i proverke dostovernosti informatsii pri ee peredache po otkrytym kanalam svyazi [On the issue of protecting and verifying the reliability of information during its transmission over open communication channels]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Control and High Technologies], 2020, no. 2 (50), pp. 127–135.

7. Rudenko, M. V. *Informatsionnaya sistema mobilnykh ustroystv dlya oplaty kommunalnykh uslug : dissertatsiya na soiskanie uchenoy stepeni kandidata tekhnicheskikh nauk* [Information system of mobile devices for payment of utility bills : dissertation for the degree of candidate of technical sciences]. Krasnodar, Kuban State Technological University, 2016.

8. Holkin, D. O., Maslova, M. A., Dmitriev, A. S. Metod peredachi soobshheniy s ispolzovaniem luchshikh sposobov organizatsii obmena dannymi i kriptograficheskikh protokolov obmena mgnovennymi soobshheniyami s ispolzovaniem skvoznogo shifrovaniya [A method of transferring messages using the best communication methods and cryptographic instant messaging protocols using end-to-end encryption.] *Inzhenernyy vestnik Dona* [Engineering Journal of Don], 03.06.2021, no. 6. Available at: www.ivdon.ru/ru/magazine/archive/n6y2021/7054.

9. Skoba, A. N., Mikhaylov, V. K., Ayesh, Akhmed Nafea Ayesh. Reshenie zadachi obespecheniya optimalnoy effektivnosti funktsionirovaniya raspredelennykh sistem obrabotki informatsii [Solving the problem of ensuring the optimal efficiency of functioning of distributed information processing systems]. *Inzhenernyy vestnik Dona* [Engineering Journal of Don], 03.06.2021, no. 6. Available at: www.ivdon.ru/ru/magazine/archive/n6y2021/7053.

10. Chor, B., Rivest, R. A Krapsack-type pubkie key cryptosystem based on arithmetic in finite fields. *IEEE Transactions on Information Theory*, 1988, vol. 34, pp. 901–909.

11. Osipyan, V. O., Litvinov, K. I., Bagdasaryan, R. Kh., Lukashchik, E. P., Sinitsa, S. G., Zhuk, A. S. Development of information security system mathematical models by the solutions of the multigrade diophantine equation systems. *International Conference Proceeding Series, Association for Computing Machinery*, 2019.

УДК 004.421.5

## ВАРИАНТ РЕАЛИЗАЦИИ СХЕМЫ ПРЕОБРАЗОВАНИЯ ВХОДНОГО ПОТОКА ДАННЫХ АСИММЕТРИЧНЫМ МЕТОДОМ НА БАЗЕ КЛЕТОЧНЫХ АВТОМАТОВ[1]

*Статья поступила в редакцию 24.08.2021, в окончательном варианте – 09.09.2021.*

***Кулешова Елена Александровна***[2], Юго-Западный государственный университет, 305004, Россия, г. Курск, ул. Челюскинцев, 19, корпус Б,
аспирант, ORCID: 0000−0002−8270−564X, e–mail: lena.kuleshova.94@mail.ru

В настоящее время известны такие приложения теории клеточных автоматов, как симметричное шифрование, сжатие данных, обработка цифровых изображений и некоторые другие. Также существуют исследования, предполагающие возможность построения системы с открытым ключом на базе клеточных автоматов, однако данная задача пока не была решена. В данной статье предлагается вариант схемы преобразования входного потока данных асимметричным методом на базе клеточных автоматов. Предложена схема преобразования, основанная на последовательном изменении битов исходного файла согласно инструкциям в ключе. Открытым параметром в данном случае будет являться число столбцов информационной матрицы, а закрытый ключ будет состоять из матрицы шифрования и правила обхода матрицы данных. В целях повышения стойкости и поддержания высокой скорости обработки потока данных предложена математическая модель преобразования данных на базе клеточных автоматов с использованием расширенного ключа, определяющего индивидуальную окрестность обрабатываемого бита данных с учетом положения данного бита в матрице исходных данных. Для верификации математической модели был разработан программный модуль для анализа индивидуальных цепочек в блоках данных, позволяющий сопоставить блоки данных в виде бинарных матриц. Практическая значимость предложенного решения заключается в том, что полученные результаты можно использовать в исследовательских целях и в возможности применения полученных решений для развития методов криптографического преобразования данных.

**Ключевые слова:** информационная безопасность, потоковая передача данных, клеточные автоматы, асимметричное шифрование, системы защиты конфиденциальной информации

## A VARIANT OF IMPLEMENTATION OF THE SCHEME FOR CONVERSION OF THE INPUT DATA FLOW BY THE ASYMMETRIC METHOD ON THE BASIS OF CELLULAR AUTOMATA

*The article was received by the editorial board on 24.08.2021, in the final version – 09.09.2021.*

***Kuleshova Elena A.***, Southwest State University, building B, 19 Chelyuskintsev St., Kursk, 305004, Russian Federation,
postgraduate student, ORCID: 0000−0002−8270−564X, e-mail: lena.kuleshova.94@mail.ru

At present, such applications of the theory of cellular automata as symmetric encryption, data compression, digital image processing, and some others are known. There are also studies suggesting the possibility of building a public key system based on cellular automata, but this problem has not yet been solved. This article proposes a variant of the scheme for transforming the input data stream by an asymmetric method based on cellular automata. The proposed conversion scheme is based on the sequential change of the bits of the source file according to the instructions in the key. The public parameter in this case will be the number of columns of the information matrix, and the private key will consist of the encryption matrix and the rule for traversing the data matrix. In order to increase the stability and maintain a high processing speed of data streams, a mathematical model of data transformation based on cellular automata with the use of an extended key, which determines the individual neighborhood of the processed data bit, taking into account the position of this bit in the initial data matrix, is proposed. To verify the mathematical model, a software module was developed for the analysis of individual chains in data blocks, which makes it possible

[1] Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 19-31-90069.

[2] Научный руководитель – Добрица Вячеслав Порфирьевич, Юго-Западный государственный университет, 305004, Российская Федерация, г. Курск, ул. Челюскинцев, 19, корпус Б, доктор физико-математических наук, профессор, e-mail: dobritsa@mail.ru