zhurnal Kubanskogo gosudarstvennogo agrarnogo universiteta [Polythematic network electronic scientific journal of the Kuban State Agrarian University], 2018, pp. 1–4.

4. Dostova A. A., Tynchenko V. V. Analiz novovvedeniy v obektno-orientirovannom yazyke programmirovaniya Java [Analysis of innovations in the object-oriented programming language Java]. *Aktualnye problemy aviatsii i kosmonavtiki* [Actual problems of aviation and astronautics], 2018, pp. 10–23.

5. Iskhakov S. Yu., Shelupanov A. A. Razrabotka struktury sistemy upravleniya setyu [Development of the network management system structure]. *Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki* [Reports of Tomsk State University of Control Systems and Radioelectronics], 2011, pp. 259–262.

6. Kodzheshau M. A. Tekhnologii i algoritmy informatsionnoy bezopasnosti [Information Security Technologies and Algorithms]. *Vestnik Adygeyskogo gosudarstvennogo universiteta. Seriya 4: Yestestvenno-matematicheskie i tekhnicheskie nauki* [Bulletin of Adygea State University. Series 4: Natural Mathematical and Technical Sciences], 2017, pp. 129–132.

7. Medvedev N. V., Grishin G. A. Modeli upravleniya dostupom v raspredelennykh informatsionnykh sistemakh [Models of access control in distributed information systems]. *Mashinostroenie i kompyuternye tekhnologii* [Mechanical Engineering and Computer Technologies], 2011, pp. 1–19.

8. Nasterenko D. Yu. Obektno-orientirovannoe programmirovanie na primere yazyka Java [Object-oriented programming on the example of the Java language]. *Nauchnyy zhurnal* [Initial log], 2016, pp. 17–30.

9. Oladko A.Yu. Podsistema monitoringa i audita informatsionnoy bezopasnosti v operatsionnoy sisteme Linux [The subsystem for monitoring and auditing information security in the Linux operating system]. *Izvestiya Yuzhnogo federalnogo universiteta. Tekhnicheskie nauki* [Proceedings of the Southern Federal University. Technical science], 2012, pp. 22–28.

10. Rogachev A. F., Fedorova Ya. V. Ispolzovanie UML-modeley dlya issledovaniya i obespecheniya informatsionnoy bez-opasnosti slozhnykh tekhnicheskikh sistem [Using UML-models for research and ensuring information security of complex technical systems]. *Izvestiya Nizhnevolzhskogo agrouniversi-tetskogo kompleksa: nauka i vysshee professionalnoe obrazovanie* [News of the Nizhnevolzhsky agrouniversity complex: science and higher vocational education], 2014, pp. 1–6.

11. Rukasueva S. Yu., Bagaeva A. P. Windows i alternativnye ey operatsionnye sistemy [Windows and alternative operating systems to it]. *Aktualnye problemy aviatsii i kosmonavtiki* [Actual problems of aviation and astronautics], 2011, pp. 459–460.

12. Shubin A. N. Otsenka svoystv informatsionnykh sistem v standartakh po informatsionnoy bezopasnosti [Assessment of the properties of information systems in standards for information security]. *Izvestiya Tulskogo gosudarstvennogo universiteta. Tekhnicheskie nauki* [Proceedings of the Tula State University. Technical science], 2013, pp. 336–345.

13. George K. Thiruvathukal. What's in an Algorithm? *Computing in Science & Engineering*, 2013, no. 15, pp. 15–27.

14. Johanson A., Hasselbring W. Software Engineering for Computational Science: Past, Present, Future. *Computing in Science & Engineering*, 2018, no. 20, pp. 90–112.

УДК 004.62

О РАЗРАБОТКЕ МЕТОДА ПРОВЕРКИ ДОСТОВЕРНОСТИ ДАННЫХ ПРИ ПЕРЕДАЧЕ ИНФОРМАЦИИ[1]

Статья поступила в редакцию 14.04.2019, в окончательном варианте – 14.05.2019.

Багдасарян Рафаэль Хачикович, Кубанский государственный университет, 350040, Российская Федерация, г. Краснодар, ул. Ставропольская, 149,
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

Лукащик Елена Павловна, Кубанский государственный университет, 350040, Российская Федерация, г. Краснодар, ул. Ставропольская, 149,
кандидат физико-математических наук, e-mail: lep_9091@mail.ru

Синица Сергей Геннадьевич, Кубанский государственный университет, 350040, Российская Федерация, г. Краснодар, ул. Ставропольская, 149,
кандидат технических наук, e-mail: podrugomu@gmail.com

Жук Арсений Сергеевич, Кубанский государственный университет, 350040, Российская Федерация, г. Краснодар, ул. Ставропольская, 149,
аспирант, e-mail: arseniyzhuck@mail.ru

Литвинов Кирилл Игоревич, Кубанский государственный университет, 350040, Российская Федерация, г. Краснодар, ул. Ставропольская, 149,
аспирант, e-mail: lyrik-1994@yandex.ru

Предлагается метод проверки достоверности данных при передаче закрытой информации по открытым каналам связи между узлами сети. Приводятся требования к системам, внутри которых совершается передача данных. Описываются технические аспекты предлагаемого метода, совместно использующего мультиграф, шифрование и биометрическую идентификацию для проверки достоверности передаваемых данных. В схеме, соответствующей данному

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

методу, используется гибридное шифрование с распределенной передачей информации. Это обеспечивает эффективные возможности проверки достоверности передаваемых данных в отношении отсутствия фактов внедрения злоумышленников. Симметричный метод шифрования применяется для шифрования данных, в то время как ассиметричный ключ зашифровывает сам симметричный ключ. Таким образом, в предлагаемом методе высокая производительность симметричных криптосистем сочетается с преимуществами ассиметричных методов в отношении уровней защиты.

Ключевые слова: достоверность данных, аутентикация, передача информации, шифрование, дешифрование, защита данных, гибридное шифрование, безопасность передачи информации, биометрическая идентификация, мультиграф, сетевые атаки

Графическая аннотация (Graphical annotation)

ON THE DEVELOPMENT OF THE METHOD OF CHECKING THE DATA RELIABILITY IN THE TRANSMISSION OF INFORMATION

The article was received by editorial board on 14.04.2019, in the final version – 14.05.2019.

Bagdasaryan Rafael Kh., Kuban State University, 149 Stavropolskaya St., Krasnodar, 350040, 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
Lukashchik Elena P., Kuban State University, 149 Stavropolskaya St., Krasnodar, 350040, Russian Federation,
Cand. Sci. (Physics and Mathematics), Associate Professor, e-mail: lep_9091@mail.ru
Sinitsa Sergey G., Kuban State University, 149 Stavropolskaya St., Krasnodar, 350040, Russian Federation,
Cand. Sci. (Engineering), e-mail: podrugomu@gmail.com
Zhuk Arseniy S., Kuban State University, 149 Stavropolskaya St., Krasnodar, 350040, Russian Federation,
post-graduate student, e-mail: arseniyzhuck@mail.ru
Litvinov Kirill I., Kuban State University, 149 Stavropolskaya St., Krasnodar, 350040, Russian Federation,
post-graduate student, e-mail: lyrik-1994@yandex.ru

A method is proposed for verifying the accuracy of data when transmitting sensitive information on open communication channels between network nodes. The requirements for the systems within which the data is transmitted are given. Describes the technical aspects of the proposed method, sharing multigraph, encryption and biometric identification to verify the reliability of the transmitted data. The scheme corresponding to this method uses hybrid encryption with distributed information transfer. This provides effective means of verifying the reliability of the transmitted data in the absence of evidence of intruders. The symmetric encryption method is used to encrypt data, while the asymmetric key encrypts the symmet-

ric key itself. Thus, in the proposed method, the high performance of symmetric cryptosystems is combined with the advantages of asymmetric methods in terms of levels of protection.

Keywords: data accuracy, authentication, information transfer, encryption, decryption, data protection, hybrid encryption, information transfer security, biometric identification, multigraph, network attacks

Введение. Одним из важнейших качеств любой информационной системы (ИС) является безопасность ее использования. Это связано с возросшим количеством атак злоумышленников на сетевые ресурсы во всём мире [8]. Любая ИС, позволяющая проводить обмен данными, должна гарантировать, что отправленная информация не будет перехвачена или подделана. Для проверки достоверности получаемой информации узлом (т.е. отсутствия каких-либо ее корректировок в процессе передачи) необходимо рассмотреть меры по обеспечению безопасного обмена данными. Под безопасным обменом подразумевается невозможность повлиять на процесс передачи данных со стороны третьих лиц. В связи с этим должны быть изучены все возможные варианты действия потенциальных взломщиков – нарушителей информационной безопасности. Поэтому есть необходимость рассмотреть слабости проектируемой ИС по отношению к максимально возможному разнообразию сетевых атак – изнутри и извне локальной вычислительной сети.

Для участников обмена сообщениями необходимо создать среду, в которой соблюдаются следующие правила.

1. Между участниками процесса обмена информацией не должно быть нежелательных посредников.
2. Не допускается возможность для злоумышленника выдать себя за доверенное лицо, т.е. идентифицировать себя в качестве истинного пользователя.
3. Среда, в которой происходит обмен, должна быть изолирована при открытости сети. Иными словами, эта среда должна иметь внутреннюю защиту данных (брандмауэр, антивирус и т.д.).

С учетом существующих проблем, угроз и недостатков при передаче любой информации по сети, есть большая вероятность возникновения несанкционированной расшифровки и захвата данных злоумышленниками с дальнейшим искажением достоверности информации [14, 16]. Поэтому целесообразна разработка метода проверки достоверности данных при передаче информации с использованием гибридного шифрования, в частности совместного применения асинхронных и синхронных ключей, биометрии и мультиграфов.

Шифрование канала обмена данными. Прежде всего рассмотрим решение проблемы «прослушиваемости» сети, в которой происходит обмен информацией. Именно криптографические методы шифрования помогут нам обеспечить защиту от прослушивания канала передачи данных со стороны. С их помощью мы сможем преобразовывать транспортируемую информацию так, чтобы лица без авторизации для работы в ИС не имели к ней доступа.

Предлагаемый метод защиты канала от внедрения злоумышленников подразумевает использование гибридного шифрования, при этом передача информации будет являться распределённой. Симметричный метод шифрования будет использоваться для шифрования данных, в то время как ассиметричный ключ зашифрует сам симметричный ключ. В таком случае производительность симметричных криптосистем будет сочетаться с преимуществами ассиметричных методов. Процесс обмена должен начинаться с аутентикации клиента [6, 9, 12, 18].

Рассмотрим на примере схемы по рисунку 1 состав участников сети. Клиент непосредственно связан с сервером аутентикации, сервером приёма сообщений и распределёнными серверами [1], которые связаны с базой данных (БД) ИС.

На рисунке 2 схематически показаны действия по обеспечению передачи закрытой информации в сети.

Сначала клиент должен сгенерировать открытый ($PublicKey_A$) и закрытый ($PrivateKey_A$) ключи. На следующем шаге необходимо передать сообщение серверу аутентикации (B) с идентификатором (ID_A) и открытым ключом:

$$S_1 = PublicKey_A + ID_A.$$

Сервер аутентикации создаст запись в базе данных с открытым ключом клиента и сгенерирует собственный закрытый ($PrivateKey_B$) и открытый ключи ($PublicKey_B$), а после отправит клиенту сообщение, содержащее открытый ключ сервера.

$$S_2 = PublicKey_A.$$

Далее клиенту необходимо сгенерировать транзакционный ключ ($TransactKey_A$), зашифровать симметричным методом пароль клиента ($Password_A$). Далее транзакционный ключ должен быть зашифрован ассиметрично открытым ключом сервера. После проделанных операций ассиметрично зашифрованный транзакционный ключ отправляется принимающей стороне.

$$S_3 = PublicKey_B|TransactKey_A|Password_A||.$$

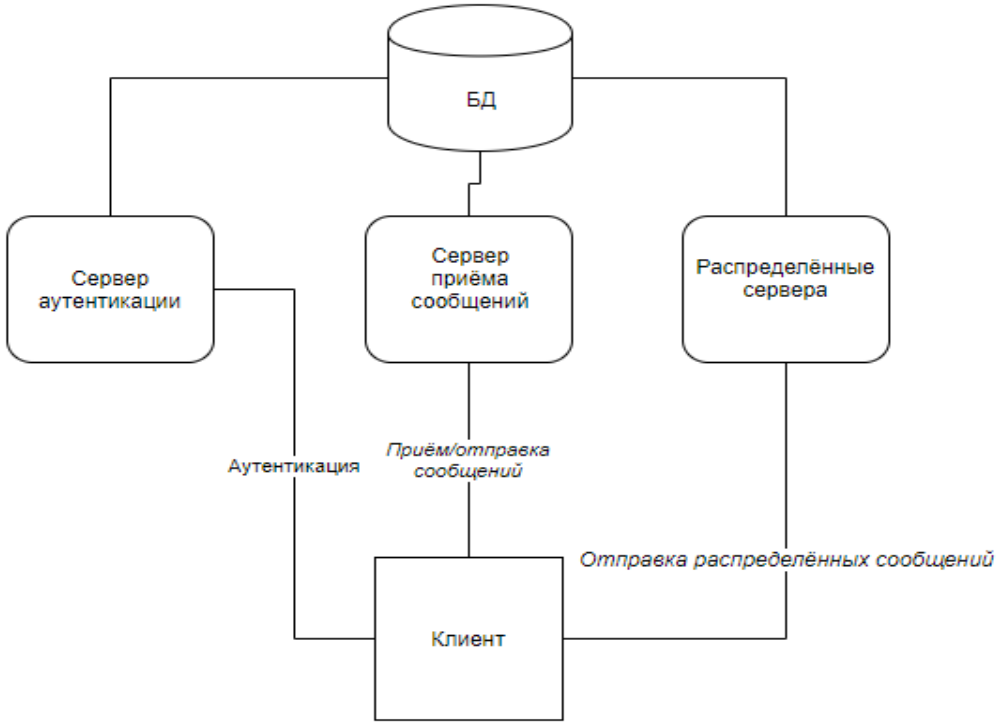

Рисунок 1 – Схема взаимосвязи в ИС между клиентом и сервером

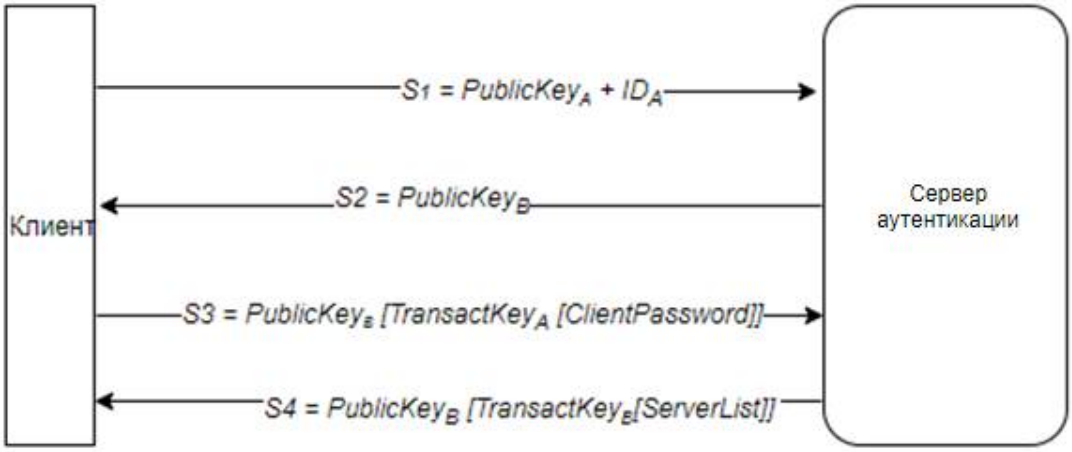

Рисунок 2 – Схема передачи данных по открытым сетям в процессе аутентикации

Принимающая сторона «В» расшифровывает транзакционный ключ ассиметрично, используя собственный закрытый ключ. На следующем шаге принимающей стороной расшифровывается пароль клиента симметричным методом с использованием транзакционного ключа клиента. Сервер проверяет идентификатор отправителя, пароль клиента и сообщает об ошибке, если обнаруживается несоответствие.

Если идентификатор клиента и пароль верны, то сторона «В» должна сгенерировать транзакционный ключ и в итоге,зашифровать им список серверов ($ServerList$), которые принимают данные, зашифрованные открытым ключом. Зашифрованный список отправляется клиенту.

$$S_4 = OK_A|TK_B|LS||.$$

Если ID_A и $Password_A$ неверны, то в таком случае S_4 является сообщением об ошибке. Клиенту необходимо расшифровать транзакционный ключ сервера с помощью собственного приватного ключа ассиметрично. Под приватным ключом понимается сохраняемый в тайне компонент ключевой пары, применяющейся в асимметричных шифрах, т.е. таких шифрах, в которых для прямого и обратного преобразований используются разные ключи. После этого клиент должен применить симметричный метод для расшифровки списка серверов при помощи транзакционного ключа. В итоге сервер может идентифицировать сторону «А» по паре логин/пароль. В случае успешной проверки данной пары клиенту отправляется сводка

серверов для дальнейшей отправки распределённых данных. Отметим, что транзакционный ключ необходимо генерировать при каждой передаче, а срок действия такого ключа составляет один час [2].

Использование биометрических показателей для подтверждения личности. Второй способ ограничить канал связи от доступа нежелательных лиц заключается в идентификации участников сети по их биометрическим показателям. В таком случае можно определить, что пользователь действительно является тем человеком, за которого себя выдаёт. Отметим, что используемые биометрические показатели должны быть уникальны и неповторимы. Это могут быть, например, показатели, относящиеся к сетчатке глаза или отпечаткам пальцев. Такой способ идентификации нередко применяется в биллинговых системах и для подтверждения личности в банковской сфере. Идентификация пользователя по отпечатку пальца – надёжный способ исключить возможность взломщиков выдать себя за пользователя. Проверку по таким биометрическим параметрам, как отпечатки пальцев, удобно встраивать в мобильные устройства и терминалы оплаты [4, 5, 20]. Отметим также, что уже появились смартфоны, которые могут идентифицировать владельца не только по отпечаткам пальцев и лицу, но и по характеристикам радужной оболочки глаза.

Далее рассмотрим технологию распознавания по отпечатку пальцев. Одним из способов распознавания отпечатков является метод нахождения количества пересечений папиллярных линий (CN). В таком методе анализируются папиллярные линии, разбитые на мелкие квадратные фрагменты. В дальнейшем происходит вычисление количества пересечений папиллярных линий на пальце человека [13, 15].

Найдём число пересечений CN по следующей формуле:

$$CN = 0.5 * \sum_{i=1}^{8} |R_i - R_{i+1}|, \quad R_9 = R_1,$$

где R_i – это значение в окрестности точки R. Это восемь значений, которые проверяются в порядке «против часовой стрелки» (рис. 3).

R_4	R_3	R_2
R_5	R	R_1
R_6	R_7	R_8

Рисунок 3 – Значения соседних точек относительно R

На основании полученных данных классифицируем квадратную часть в соответствии со следующими правилами категорий папиллярных линий:

- значение «0» присваивается для изолированной точки;
- значение «1» присваивается конечной точке папиллярной линии;
- неконечной точке папиллярной линии соответствует «2»;
- точке раздвоения присваивается «3»;
- значение «4» применяется к точке пересечения.

В дальнейшем тексте используется термин «минуция», соответствующий пересечению папиллярных линий. Совокупность минуций характеризует уникальные для каждого отпечатка пальца признаки, определяющие особенности структуры папиллярных линий, их ориентацию, координаты и углы связанных папиллярных линий.

Зная количество пересечений папиллярных линий, определим для каждой минуции следующую информацию:

- координаты *x* и *y*;
- угол связанной папиллярной линии;
- тип минуции.

Далее показаны окончание папиллярной линии и разветвление (рис. 4).

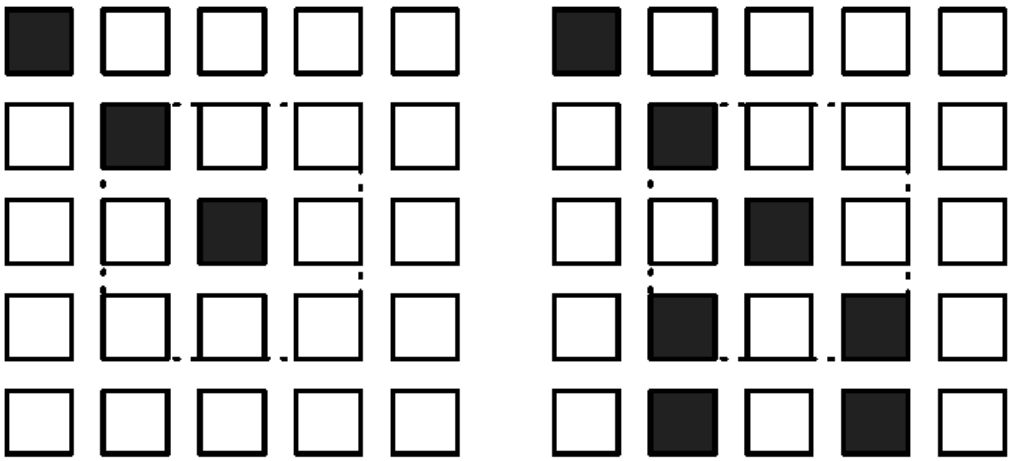

Рисунок 4 – Окончание и разветвление папиллярных линий

Для построения матрицы отпечатка пальца необходимо выделить квадратную часть отпечатка, в центре которой будет папиллярный узор [19, 20]. В процессе построения матрицы отпечатка пальца выделим квадратный участок с папиллярным узором, который будет находиться в центре квадратной части отпечатка (рис. 5).

Рисунок 5 – Отпечаток пальца и его выделенная квадратная часть

Переводя папиллярную линию в квадратную матрицу, будем следовать следующему алгоритму:

- для пустых квадратных частей записывается «1»;
- окончаниям приписываются значения «2»;
- для разветвлений записывается «4»;
- для остальных случаев присваивается «3».

После этого необходимо выделить квадратную область центра отпечатка пальца (рис. 6).

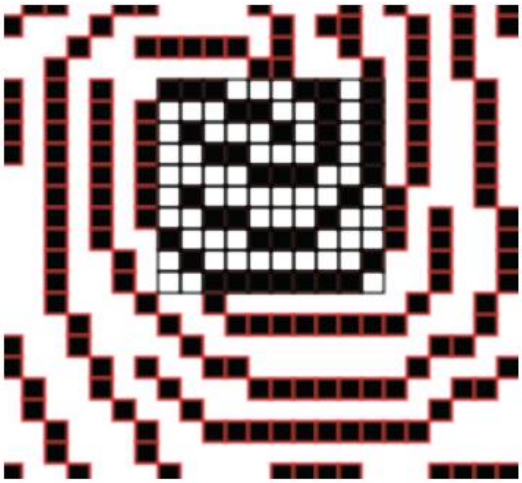

Рисунок 6 – Квадратная область отпечатка пальца

Для упрощения решения построим матрицу отпечатка пальца для области распознавания 10 х 10 точек и вычислим определитель этой матрицы, представляющий собой совокупность 100 целых чисел в диапазоне от «1» до «3».

3	3	3	1	1	1	3	3	1	3
1	1	1	3	3	1	1	3	1	3
1	2	1	1	1	2	1	3	1	3
1	1	3	3	1	1	1	3	1	3
1	1	1	1	3	3	3	1	1	3
1	2	1	1	1	1	1	1	3	1
1	1	3	3	1	1	1	3	1	1
3	1	1	1	3	3	3	1	1	1
1	3	1	1	1	1	1	1	1	3
1	1	3	3	3	3	3	3	3	1

Определитель матрицы в данном случае равен 0,000000000001151079231931З6. Примем максимальное количество пользователей ИС – 10^9. Соответственно пароль должен состоять не менее чем из 9 символов. Для предложенного выше примера пароль пользователя будет состоять из первых девяти значимых чисел, и он будет иметь следующий вид: 115107923. Иными словами, на выходе получим числовой пароль, который будет являться определителем для матрицы значений папиллярных линий [3].

Определение достоверности информации с помощью мультиграфа. Биометрическая идентификация и шифрование канала связи упрощают дальнейшую проверку данных на достоверность, поскольку исключается возможность большинства способов атак, в процессе которых данные могут быть подменены. Однако канал связи, несмотря на всю предусмотренную защиту, уязвим к «Атаке посредника», в которой злоумышленник становится скрытым посредником при передаче информационных сообщений [10]. Нарушитель может осуществлять мониторинг всех данных, производить их подмену и кражу. Оставаться незамеченным ему помогает использование украденных соответствующих ключей, борьба с таким родом атак является нетривиальной задачей [7, 11].

Будем рассматривать достоверность информации как интегральную характеристику, которая зависит от физической и логической составляющей системы.

Рассмотрим множество данных, приходящих от пользователя s:

$$d_n = \{d_s^n\},$$

где s – пользователь; n – количество пользователей.

Обозначим множество данных, передающихся в сети между n пользователями:

$$\mathrm{d} = \bigcup_n d_n,$$

где d_n– множество данных, приходящих от n пользователей; n – количество пользователей.

Сформируем ориентированный мультиграф, в котором каждая вершина будет принимать определённое множество значений:

$$h_i^{ns} h_i^n,$$

где h_i^{ns}– множество информационных сообщений; h_i^n – множество вершин информационных сообщений пользователя *s* из общего числа *n*; i – текущее информационное сообщение.

Определим дуги мультиграфа, которые будут задавать последовательность обращений к узлу:

$$p_v^{ns} p_s^n,$$

где p_v^{ns} – дуги мультиграфа, которые указывают передачу данных пользователя s из общего числа *n*; p_s^n – множество дуг мультиграфа в целом; v – текущая дуга.

Рассмотрим множества всех сообщений графа:

$$h_z = \bigcup_n \bigcup_s h_s^n,$$

$$p_z = \bigcup_n \bigcup_s p_s^n.$$

Связи между элементами могут иметь вид «1:1», «1:M», «M:M». В нашем случае между двумя информационными элементами имеется связь типа «1:1», тогда вводится связь типа «1:M» в прямом направлении и связь типа «M:M» в обратном направлении. Семантическое значение каждой из полученных связей определяется семантическим значением исходной связи.

Построим мультиграф G_s^n, для которого $M_s^n: G_s^n =< h_s^n, p_s^n, \varphi_s^n >$, где $h_s^n = \{h_{is}^n\}$ – вершины, $p_s^n = (h_i^{ns}, h_l^{ns})$ – связи. Таким образом, функция $\varphi_s^n: p_s^n \to h_i^{ns} h_i^n$ сопоставляет дуге p_s^n вершины (h_i^{ns}, h_j^{ns}). Каждая отдельно взятая вершина является отмеченной, поэтому рассмотрим свойства мультиграфа G_s^n. Отметки вершин – это уникальные идентификаторы информационных элементов, позволяющие задать семантическое значение.

Все дуги p_s^n имеют метки двух категорий:

1. $Type_{p_{ijv}^{ns}} = (h_i^{ns}, h_j^{ns})_v = \{\overrightarrow{1:1};\ \overrightarrow{1:M};\ \overleftarrow{1:M}\}$ – категория направления и типа связи между вершинами в G_s^n;

2. $U_{h_{ijv}^{ns}}$ задаёт семантику дуги p_{ijv}^{ns} и связи между h_i^{ns}, h_j^{ns}.

Даже если у двух вершин будет несколько взаимосвязей, необходимо, чтобы соединяющие их дуги отличались хотя бы меткой второго типа.

Функция φ_s^n задаётся матрицей инцидентности $W_s^n = \omega_{iv}^{ns}$. В таком случае:

$$\omega_{iv}^{ns} = \begin{cases} +1,\ \exists p_{ijv}^{ns}\left(Type_{p_{ijv}^{ns}}\right) = \{\overrightarrow{1:1};\ \overrightarrow{1:M};\ \overrightarrow{M:1}\}, \\ -1,\ \exists p_{ijv}^{ns}\left(Type_{p_{ijv}^{ns}}\right) = \{\overleftarrow{1:1}; \overleftarrow{1:M}; \overleftarrow{M:1}\} \end{cases}.$$

Ключевой возможностью рассматриваемого мультиграфа является проверка данных на достоверность. Избавиться от лишних взаимосвязей между элементами модели поможет расчет путей доступа, в процессе которого достоверность информации нарушится, если будут удалены избыточные связи и информационные элементы.

Рассмотрим выражение, которое поможет нам проверить достоверность информации:

$$C_{ZU} = \frac{\xi_{p_I P_{ZU}} \chi_i + \xi_{L_{ijv} L_{ZU}} N_{L_{ijv}}}{\xi_{p_I P_2} \chi_i + \xi_{L_{ijv}} N_{L_{ijv}}},$$

где χ – количество экземпляров информационного объекта с индексом i; $L_{ijv}(L_{ij\mu})$ – количество экземпляров связей между элементами.

Совокупность информационных элементов со связями:

$$P_U = \bigcup_n \bigcup_s p_s^n.$$

Пересечение информационных элементов и их связей:

$$P_{zu} = P_z \cap P_U.$$

Множество путей доступа из вершин с точкой входа:

$$L_z = \bigcup_n \bigcup_s L_s^n.$$

Пересечение путей доступа из входных вершин и множества путей доступа:

$$P_{zU} = P_z \cap P_U.$$

Рассчитанные показатели достоверности информации сравниваются с заданными, при их несоответствии определяются причины возникновения ошибок, производится их локализация и вносятся исправления в структуру данных.

Заключение. Рассмотренные теоретические основы способа проверки достоверности информации, передаваемой в открытой сети, позволяют разработать полноценный метод для решения поставленной задачи. Использование гибридного шифрования, а именно совместное применение асинхронных и синхронных ключей, биометрической идентификации личности и мультиграфов позволяют получить метод проверки достоверности данных при передаче информации, который является более защищённым и надежным от атак в сетевом окружении. За счет этого пользователи смогут безопасно производить обмен закрытой информацией по открытым каналам связи.

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. – 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 надежности построения биллинговых информационных систем / В. А. Атрощенко, Р. А. Дьяченко, Р. Х. Багдасарян, М. В. Руденко // Математические методы и информационно-технические средства : материалы IX Всероссийской научно-практической конференции. – 2013. – С. 37–39.

4. Атрощенко В. А. Разработка алгоритма работы с графовой БД при авторизации с помощью отпечатков пальцев / В. А. Атрощенко, Н. Д. Чигликова, Р. А. Дьяченко, М. В. Руденко, Р. Х. Багдасарян // V Международная научно-практическая конференция молодых ученых, посвященная 54-й годовщине полета Ю. А. Гагарина в космос. – Краснодар, 2015. – С. 277–280.

5. Болл Р. М. Руководство по биометрии / Р. М. Болл. – Москва : Техносфера, 2007. – 368 с.

6. Большаков Т. Организация надежных каналов связи при передаче технологических данных / Т. Большаков // Современные технологии автоматизации. – 2011. – Т. 4. – С. 62–65.

7. Дьяченко Р. А. Анализ современных методов и средств оптимизации запросов к распределённым хранилищам информации / Р. А. Дьяченко, Р. Х. Багдасарян, М. В. Руденко, А. М. Зима, С. А. Макеев // Научные чтения имени профессора Н. Е. Жуковского : сборник научных статей V Международной научно-практической конференции. – 2015. – С. 183–185.

8. Иванов М. А. Криптографические методы защиты информации в компьютерных системах и сетях / М. А. Иванов. – Москва : Кудиц-Образ, 2001. – 363 с.

9. Кульба В. В. Теоретические основы проектирования оптимальных структур распределённых баз данных. Серия «Информатизация России на пороге XXI века» / В. В. Кульба, С. С. Ковалевский, С. А. Косяченко, В. О. Сиротюк. – Москва : СИНТЕГ, 1999. – 660 с.

10. Осипян В. О. Разработка методов построения систем передачи и защиты информации : монография / В. О. Осипян. – Краснодар : КубГУ, 2004. – С. 168.

11. Осипян В. О. Моделирование систем защиты информации, содержащих диофантовы трудности. Разработка методов решений многостепенных систем диофантовых уравнений. Разработка нестандартных рюкзачных криптосистем : монография / В. О. Осипян. – LAMBERT Academic Publishing, 2012. – 344 с.

12. Ричард Э. Смит. Аутентификация: от паролей до открытых ключей / Ричард Э. Смит. – Москва : Вильямс, 2002. – С. 432.

13. Руденко М. В. Исследование и разработка современной информационной системы оплаты коммунальных услуг на базе мобильных устройств связи / М. В. Руденко, В. А. Атрощенко, Р. Х. Багдасарян, В. Е. Бельченко, И. В. Бельченко, Р. А. Дьяченко, Д. Л. Пиотровский. – Армавир, 2017. – С. 168.

14. Саломаа А. Криптография с открытым ключом / А. Саломаа. – Москва : Мир, 1995. – 318 с.

15. Самищенко С. С. Атлас необычных папиллярных узоров / С. С. Самищенко. – Москва : Юриспруденция, 2001. – 320 с.

16. Chor B. A knapsack-type public key cryptoystem based on arithmetic in finite fields / B. Chor, R. Rivest // IEEE Transactions on Information Theory. – 1988. – Vol. IT – 34. – P. 901–909.

17. Ishpreet Singh Virk. Fingerprint Image Enhancement and Minutiae Matching in Fingerprint Verification / Ishpreet Singh Virk, Raman Maini // Journal of Computing Technologies. – June 2012. – Vol. 1.

18. Koblitz N. A Course in Number Theory and Cryptography / N. Koblitz. – New York : Springer-Verlag, 1987. – 235 p.

19. Raymond Thai. Fingerprint Image Enhancement and Minutiae Extraction Technical Report / Raymond Thai. – The University of Western Australia, 2003.

20. Sharath Pankanti. On the individuality of fingerprints / Sharath Pankanti, Salil Prabhakar, Anil K. Jain // IEEE Transactions on Pattern Analysis and Machine Intelligence. – 2002. – Vol. 24, № 8. – P. 1010–1025.

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 godovshchine poleta Yu. A. Gagarina v kosmos* [III International Scientific and Practical Conference of Young Scientists dedicated to the 52nd anniversary of the flight of Yu.A. Gagarin in space]. 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 : collection of scientific articles of the IV International Scientific Practical Conference]. Krasnodar, "Publishing House – South LLC", 2014, pp. 126–129.

3. Atroschenko V. A., Dyachenko R. A., Bagdasaryan R. Kh., Rudenko M. V. K voprosu otsenki nadezhnosti postroeniya billingovykh informatsionnykh sistem [On the issue of assessing the reliability of building billing information systems]. *Matematicheskie metody i informatsionno-tekhnicheskie sredstva : materialy IX Vserossiyskoy nauchno-prakticheskoy konferentsii* [Mathematical methods and information technology tools : Proceedings of the IX All-Russian Scientific and Practical Conference], 2013, pp. 37–39.

4. Atroschenko V. A., Chiglikova N. D., Dyachenko R. A., Rudenko M. V., Bagdasaryan R. Kh. Razrabotka algoritma raboty s grafovoy BD pri avtorizatsii s pomoshchyu otpechatkov paltsev [Development of the algorithm for working with a graph database for authorization using fingerprints]. *V Mezhdunarodnaya nauchno-prakticheskaya konferentsiya molodykh uchenykh, posvyashchennaya 54-y godovshchine poleta Yu. A. Gagarina v kosmos* [V International Scientific and Practical Conference of Young Scientists dedicated to the 54th anniversary of the flight of Yu. A. Gagarin in space]. Krasnodar, 2015, pp. 277–280.

5. Boll R. M. Rukovodstvo po biometrii [Guide to biometrics]. Moscow, Tekhnosfera Publ., 2007. 368 p.

6. Bolshakov T. Organizatsiya nadezhnykh kanalov svyazi pri peredache tekhnologicheskikh dannykh [Organization of reliable communication channels when transferring technological data]. *Sovremennye tekhnologii avtomatizatsii* [Modern automation technology], 2011, vol. 4, pp. 62–65.

7. Dyachenko R. A., Bagdasaryan R. Kh., Rudenko M. V., Zima A. M., Makeev S. A. Analiz sovremennykh metodov i sredstv optimizatsii zaprosov k raspredelyonnym khranilishcham informatsii [Analysis of modern methods and means of optimizing queries to distributed repositories of information]. *Nauchnye chteniya imeni professora N.E. Zhukovskogo : sbornik nauchnykh statey V Mezhdunarodnoy nauchno-prakticheskoy konferentsii* [Scientific readings named after Professor N. E. Zhukovsky : Proceedings of the V International Scientific Practical Conference], 2015, pp. 183–185.

8. Ivanov M. A. Kriptograficheskie metody zashchity informatsii v kompyuternykh sistemakh i setyakh [Cryptographic methods for protecting information in computer systems and networks. Moscow, Kudits-Obraz Publ., 2001. 363 p.

9. Kulba V. V., Kovalevskiy S. S., Kosyachenko S. A., Sirotyuk V. O. *Teoreticheskie osnovy proektirovaniya optimalnykh struktur raspredelyonnykh baz dannykh. Seriya «Informatizatsiya Rossii na poroge XXI veka»* [Theoretical bases of designing optimal structures of distributed databases. Series "Informatization of Russia on the threshold of the XXI century"]. Moscow, SINTEG, 1999. 660 p.

10. Osipyan V. O. Razrabotka metodov postroeniya sistem peredachi i zashchity informatsii : monografiya[Development of methods for building information transmission and protection systems : monograph]. Krasnodar, Kuban State University, 2004, p. 168.

11. Osipyan V. O. *Modelirovanie sistem zashchity informatsii soderzhashchikh diofantovy trudnosti. Razrabotka metodov resheniy mnogostepennykh sistem diofantovykh uravneniy. Razrabotka nestandartnyh ryukzachnykh kriptosistem : monografiya* [Modeling information security systems containing Diophantine difficulties. Development of methods for solving multi-step systems of Diophantine equations. Development of custom backpack cryptosystems : monograph]. LAMBERT Academic Publishing, 2012. 344 p.

12. Richard E. Smit. *Autentifikatsiya: ot paroley do otkrytykh klyuchey* [Authentication: from passwords to public keys]. Moscow, Williams Publ., 2002. p. 432.

13. Rudenko M. V., Atroschenko V. A., Bagdasaryan R. Kh., Belchenko V. E., Belchenko I. V., Dyachenko R. A., Piotrovskiy D. L. *Issledovanie i razrabotka sovremennoy informatsionnoy sistemy oplaty kommunalnykh uslug na baze mobilnykh ustroystv svyazi* [Research and development of a modern information system for utilities payment based on mobile communication devices]. Armavir, 2017, p. 168.

14. Salomaa A. *Kriptografiya s otkrytym klyuchom* [Cryptography with a public key]. Moscow, Mir Publ., 1995. 318 p.

15. Samishchenko S. S. *Atlas neobychnykh papillyarnykh uzorov* [Atlas of unusual papillary patterns]. Moscow, Yurisprudentsiya, 2001. 320 p.

16. Chor B., Rivest R. A knapsack-type public key cryptoystem based on arithmetic in finite fields. *IEEE Transactions on Information Theory*, 1988, vol. IT – 34, pp. 901–909.

17. Ishpreet Singh Virk, Raman Maini. Fingerprint Image Enhancement and Minutiae Matching in Fingerprint Verification. *Journal of Computing Technologies*, June 2012, vol. 1.

18. Koblitz N. *A Course in Number Theory and Cryptography*. New York, Springer-Verlag, 1987. 235 p.

19. Raymond Thai. *Fingerprint Image Enhancement and Minutiae Extraction Technical Report*. The University of Western Australia, 2003.

20. Sharath Pankanti, Salil Prabhakar, Anil K. Jain. On the individuality of fingerprints. *IEEE Transactions on Pattern Analysis and Machine Intelligence,* 2002, vol. 24, no. 8, pp. 1010–1025,