УДК 004.62

К ВОПРОСУ О ЗАЩИТЕ И ПРОВЕРКЕ ДОСТОВЕРНОСТИ ИНФОРМАЦИИ ПРИ ЕЕ ПЕРЕДАЧЕ ПО ОТКРЫТЫМ КАНАЛАМ СВЯЗИ[1]

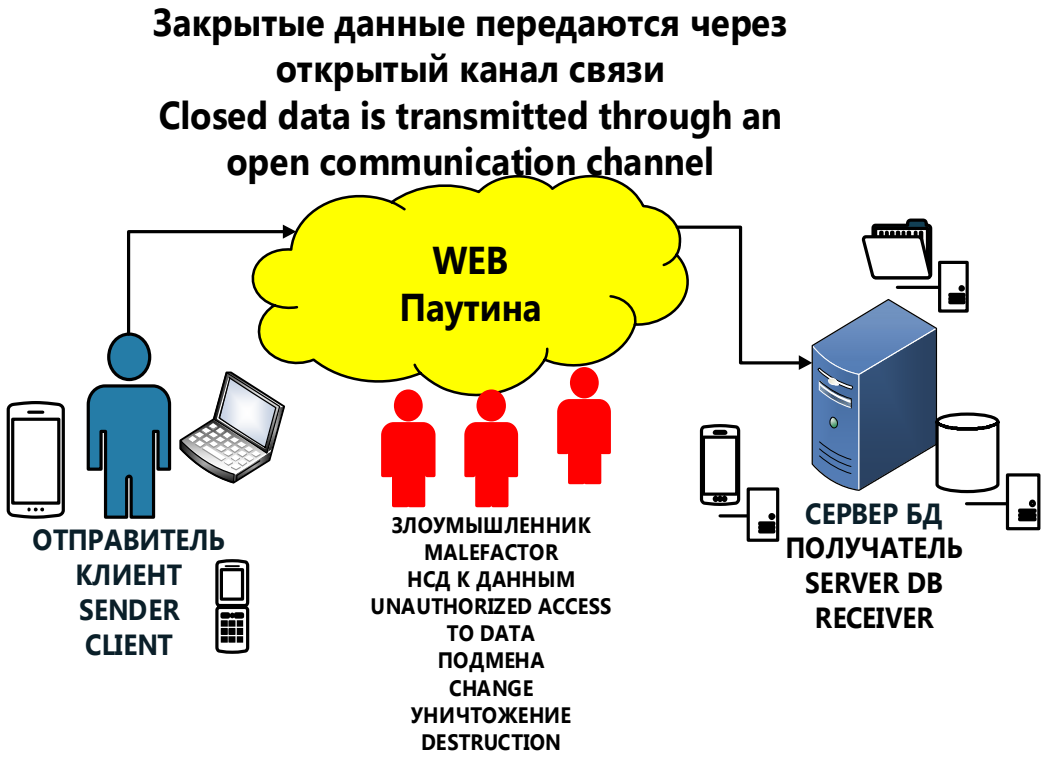
Статья поступила в редакцию 30.04.2020, в окончательном варианте – 01.06.2020.

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

В статье рассмотрена методика защиты и проверки достоверности данных при передаче закрытой информации по открытым каналам связи с применением различных способов шифрования. Приведены способы шифрования, состоящие из симметричного, несимметричного, гибридного шифрования с использованием биометрических данных человека для дальнейшей авторизации на примере отпечатка пальца. Рассмотрены алгоритмы работы каждого из видов шифрования. Для осуществления быстрого сравнения отпечатка пальца с отпечатками из базы данных при авторизации и идентификации пользователей предложено использование графовой системы управления базами данных. Данное решение проблемы позволяет производить операции сравнения графов с высокой скоростью. В статье также продемонстрированы примеры программного обеспечения их технические характеристики; основной функционал, который использует различные способы шифрования, а также проводится их сравнение.

Ключевые слова: защита и проверка информации, конфиденциальность сведений, канал связи, шифрование, биометрия, отпечаток пальца, папиллярный узор, мультиграф, база данных, передача и прием данных, система управления базами данных

Графическая аннотация (Graphical annotation)



[1] Работа поддержана грантом РФФИ № 19-01-00596 «Теоретико-числовые и алгоритмические аспекты разработки математических моделей систем защиты информации, содержащих диофантовы трудности».

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

The article was received by the editorial board on 30.04.2020, in the final version – 01.06.2020.

Bagdasaryan Rafael Kh., Krasnodar State Institute of Culture, 33 40-letiya Pobedy 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

The article describes the methodology for protecting and verifying the reliability of data during the transfer of proprietary information over open communication channels using various encryption methods. Encryption methods are presented, consisting of symmetric, asymmetric, hybrid encryption using human biometric data for further authorization using the example of a fingerprint. The algorithms of each type of encryption are considered. For the quick comparison of fingerprints with fingerprints from the database during authorization and user identification, the use of a graph database management system is proposed. This solution to the problem possibly allows performing graph comparison operations with high speed. The article also demonstrated examples of software, their technical characteristics, the main functionality that uses various encryption methods and their comparison is also carried out.
Keywords: information protection and verification, information confidentiality, communication channel, encryption, biometrics, fingerprint, papillary pattern, multigraph, database, data transmission and reception, database management system

Введение. Сохранение целостности и защита данных при передаче информации на сегодняшний день является очень актуальной и значимой процедурой в обществе. Персональные компьютеры и сервера коммерческих и государственных предприятий имеют достаточно надежную защиту. Однако порой при обмене сведениями через открытые каналы связи возникает высокий риск несанкционированного доступа и их утечки [6]. Применение малоэффективных устройств и программного обеспечения защиты является главной причиной утери в компаниях служебной информации, которая несет в себе коммерческую тайну. Поэтому применение актуальных средств и методов защиты данных при использовании каналов связи становится одной из главных задач служб безопасности различных предприятий. Ниже на рисунке 1 представлена основная схема целей и задач защиты информации.

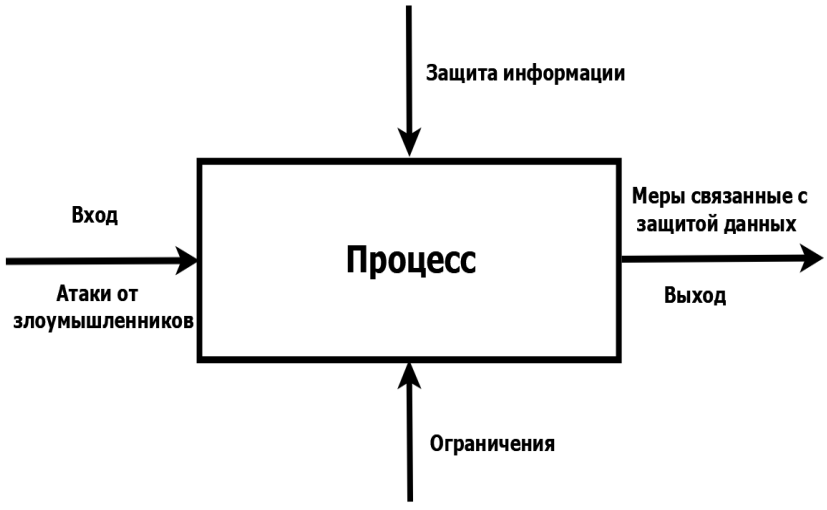


Рисунок 1 – Схема целей и задач защиты информации

Данные – это некоторый вид актива, способствующий высокой конкурентоспособности любой организации в различных сферах деятельности. Они также могут являться неким инструментом управления, так как использование их злоумышленниками, открывает простор для манипулирования поведением общества, предприятий, государственных служб, правительства и в целом всей страны.

Защита данных является важной задачей не только субъектов рынка и потребителей, но и государств вместе с правоохранительными органами. На уровне межгосударственных

отношений принимаются новые законы о защите данных, в уголовные кодексы многих стран мира уже внесены статьи, которые связаны с угрозами и преступлениями в сфере информационной безопасности [7, 13, 14].

При отправке данных по открытым сетям (каналам связи) возникает угроза кражи, повреждения или искажения закрытой информации третьими лицами. При этом имеются и актуальные методы ее защиты.

Один из основных способов – шифрование данных, а именно меры по изменению информации в целях скрытия от круга лиц, которые не должны иметь к ней доступа. В то же время доступ должен быть открытым для пользователей с определенной авторизацией [10].

Пример, изображенный ниже на рисунке 2, – это графическая схема обмена данных, применяющая гибридное шифрование с распределенной передачей некоторых закрытых сведений [1].

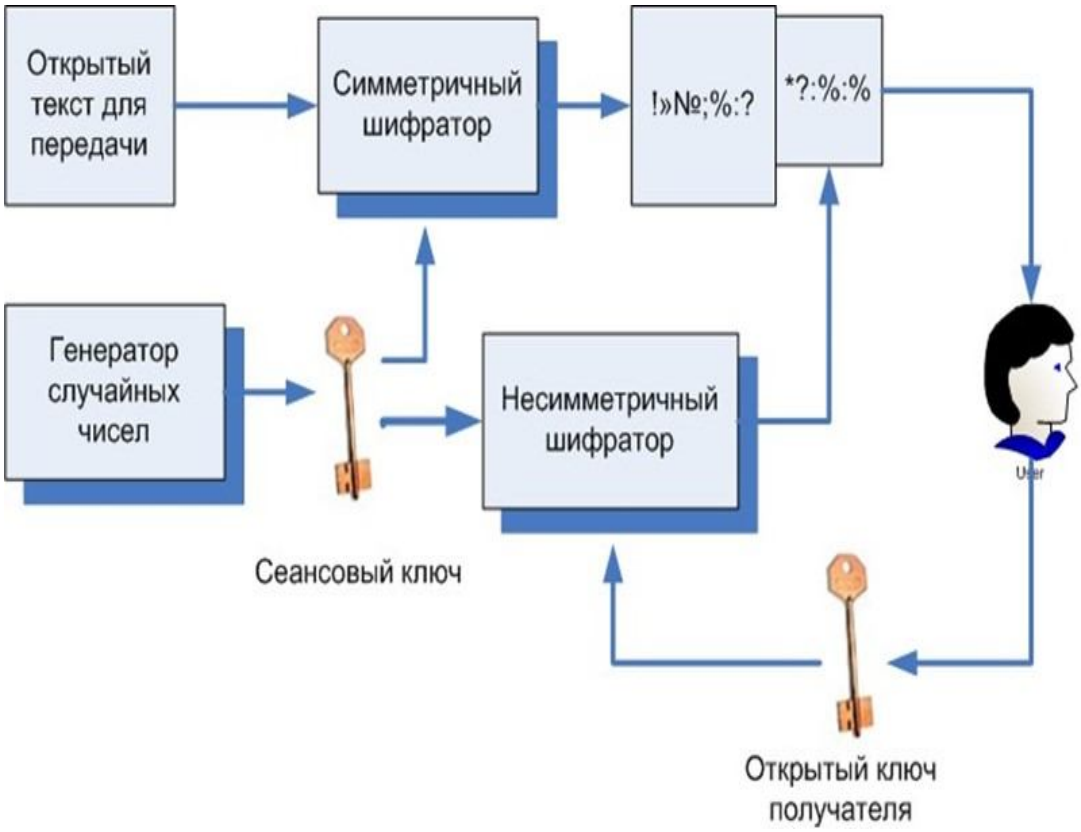


Рисунок 2 – Пример работы схемы шифрования

Под гибридным шифрованием обычно понимают такой вид шифрования, который позволяет соединять в себе достоинства защищённых систем с открытым ключом с производительностью симметричных криптосистем [18]. Симметричный ключ предназначен для шифрования информации, а асимметричный применяют в основном для шифрования самого симметричного ключа, то есть, иначе говоря, – это его числовая упаковка [16].

Ключ – это некая приватная информация, которая позволяет определить, какое изменение из многочисленных вариантов всевозможных видов преобразований будет проходить в конкретной ситуации над открытыми сведениями. По разновидности применения ключа алгоритмы шифрования можно разделить на два вида – симметричные и несимметричные. Рассмотрим первый вид ключа – в самом шифраторе пользователя, который будет отправлять информацию, и дешифраторе лица-получателя применяется всего один ключ. Второй вид подразумевает, что адресат сначала по открытому каналу связи отправляет лицу-отправителю открытый ключ, позволяющий ему зашифровать данные. При доставке материалов адресат дешифрует их, использовав этот 2-й ключ [9, 11].

В несимметричных криптосистемах обычно используют очень длинные ключи – (это > 1024 бит). Это влечет за собой увеличение времени самого процесса шифрования, а генерирование ключей также становится более долгим. Однако обмениваться ключами можно будет уже по открытым каналам обмена данными.

В симметричных криптосистемах обычно используют достаточно короткие ключи. Поэтому процессы шифрования/дешифрования проходят намного короче. Однако пересылка ключей уже будет представлять из себя сложную операцию. Клиент при передаче информации генерирует пару ключей (открытый/закрытый) и отправляет серверу. Сервер, в свою очередь, идентифицирует данные отправителя и шифрует его по симметричной схеме. После этот ключ шифруется асимметричной схемой и передается конечному пользователю. Если идентификация пользователя прошла успешно, то он в обратном порядке его расшифровывает [2, 3].

Ярким представителем данного метода может выступить программное обеспечение (ПО) под названием Files Cipher от разработчиков FCsoft. Данное ПО имеет свой оригинальный алгоритм шифрования с закрытым ключом, длина которого колеблется в интервале 4–255 символов. При этом ключ, являющийся паролем, не сохраняется внутри зашифрованных данных, что в свою очередь намного снижает вероятность его взлома. Также Files Cipher позволяет уменьшать в объеме шифруемые пакеты при помощи своего внутреннего алгоритма сжатия. Поэтому после окончания шифрования файл-исходник можно смело стереть с используемого диска без возможности его восстановления.

Это ПО может функционировать с различными типами данных и работает с объектами, превышающими размер 4 Гб. Необходимо также сказать, что его системные требования к персональному компьютеру и операционной системе очень невысоки – это позволяет работать с данной программой и на довольно старых устройствах.

Есть и иные виды шифрования, основанные на более современном способе – биометрическом шифровании данных с использованием отпечатка пальца пользователя [17]. В связи с популяризацией сканеров отпечатков пальцев было предложено использование отпечатка пальца для авторизации доступа к разным устройствам и, соответственно, к получению информации. На данный момент эта технология пользуется огромным спросом среди потребителей в IT-сфере. Также практически все современные выпускаемые гаджеты и смартфоны уже имеют встроенные сканеры отпечатков пальцев. Некоторые производители, например, Apple, заходят дальше и внедряют в свою технику сканер биометрии всего лица. Тем самым максимизируется безопасность личной информации пользователей от несанкционированного прямого доступа посторонних лиц [15].

Как и в случае с гибридным шифрованием, тут тоже используются ключи и пароли. Однако формируются они уже не на основе случайных чисел, а с использованием полученного уникального отпечатка конкретного пользователя. Суть работы такова: пользователь сканирует отпечаток, система анализирует полученный результат и ищет так называемые пересечения папиллярных линий – это рельефные линии на пальцах, ладонных и подошвенных поверхностях у человека [15, 19, 20]. После этого записывается результат в виде матрицы. Чтобы построить матрицу отпечатка пальца, требуется обозначить квадратную область отпечатка, посередине которой и находится сам папиллярный узор [8, 12]. При следующем входе в систему данные матрицы сверяются и при совпадении будут использоваться как ключ для расшифровки информации и/или непосредственного доступа к ней.

Основные преимущества такого метода шифрования данных:

1. Нет необходимости использовать генерацию случайных комбинаций при создании нового пароля.
2. Если даже известен пароль, то невозможно будет построить саму матрицу отпечатка пальца.
3. Метод может применяться без сканера отпечатков пальцев на стороне клиента.
4. Имеется возможность увеличения размера пароля в любое время.

Однако шифрование данных – это еще не залог полной защиты информации, так у злоумышленника есть возможность просто повредить все передаваемые данные (стереть, исказить или даже уничтожить). Чтобы это предотвратить, существуют методы оценки достоверности передаваемой информации с помощью построения мультиграфа. По существу, это способ передачи информации с помощью множества значений информационных элементов и связей между ней. Суть метода состоит в том, что при обмене сведениями между адресатом и отправителем информационные указания создаются при помощи мультиграфа, где любой вершине принадлежит некоторый массив информационных данных. Ориентированные дуги мультиграфа показывают очередность подключений к клиент-серверной архитектуре при обмене сведениями. Иными словами, это означает, что между многообразием точек или информационных элементов будет множество связей. По ним данные будут передаваться и в конечном итоге соберутся в той последовательности, которая необходима на определенную ситуацию в различный промежуток времени сборки информации. Исходя из этого, на выходе получаются целостные данные.

Для осуществления входа конечного потребителя в защищенную ИС с использованием биометрии требуется алгоритм для сверхбыстрого сравнения введенного отпечатка с уже имеющимся и сохраненным в БД на сервере; подтверждения отпечатка. Необходимость реализации процесса сравнения биометрических данных (отпечаток пальца) [5] требует дополнительных финансовых

затрат на закупку мощных серверных устройств и тем самым затрудняет ее реализацию. Для обхода этой проблемы нужно применять графовые базы данных. Они позволяют выполнять операции сопоставления графов с очень высоким быстродействием [4].

Граф строится на основе следующего алгоритма действий:

1. Сканирование отпечатка пальца в изображение.

2. Получение из изображения отпечатка пальца, изображения поля ориентации папиллярных линий. Затем изображение разбивается на квадратные блоки со стороной больше 4 пикселей, и по градиентам яркости вычисляется угол ориентации линии для фрагмента отпечатка;

3. Определение областей с одинаковыми полями ориентации папиллярных линий; определение центров этих областей.

4. Соединение центров областей и построение на их основе графа.

5. Добавление графов в БД.

Ниже на рисунке 3 демонстрируется пример построения графа отпечатка пальца:

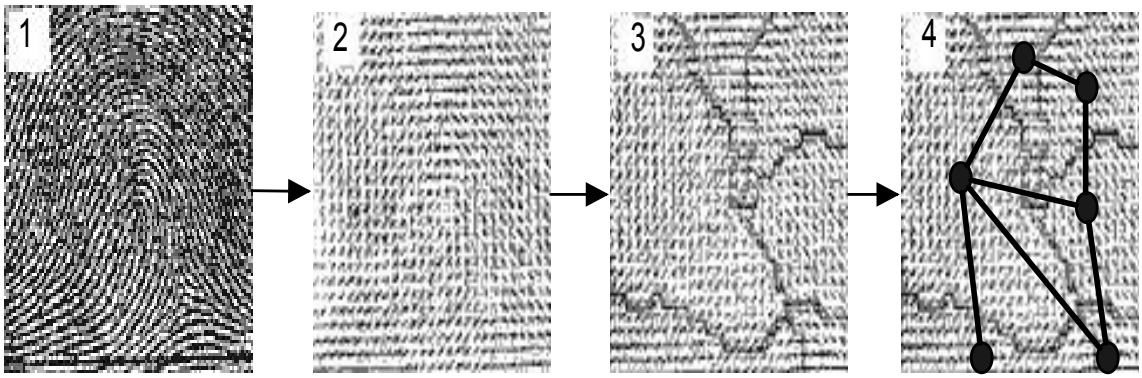


Рисунок 3 – Пример построения графа отпечатка пальца

Далее на рисунке 4 отдельно изображен граф отпечатка пальца с обозначением его вершин. На основе этого графа получена матрица (табл.), в которой значение элемента a_{ij} равно длине пути l_k из вершины a_i в вершину a_j.

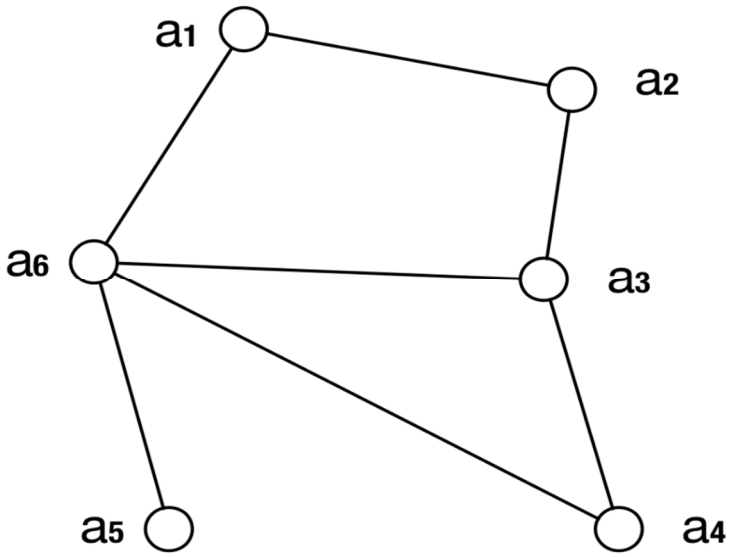


Рисунок 4 – Граф отпечатка пальца

Таблица – Матрица, полученная на основе графа

	a_1	a_2	a_3	a_4	a_5	a_6
a_1	0	l_1	0	0	0	l_7
a_2	l_1	0	l_2	0	0	0
a_3	0	l_2	0	l_3	0	l_6
a_4	0	0	l_3	0	0	l_4
a_5	0	0	0	0	0	l_5
a_6	l_7	0	l_6	l_4	l_5	0

Данная матрица (табл.) будет являться входным массивом данных.

Графовые БД позволяют решить такие задачи, где информация тесно связана между собой в отношениях, которые могут углубляться в несколько уровней. Следовательно, такие БД достаточно хорошо удовлетворяют требованиям к запуску функций поиска при сравнении биометрических данных. Графовая БД является одной из видов баз данных – в ней используются межсетевые модели в виде «графа с обобщениями». Они применяют два вида элементов: именованные дуги и узлы. Графовая БД также используется при моделировании социальных графов.

В настоящее время пользуется популярностью графовая система управления БД Neo4j. Это разработка американской компании Neo Technology, которая активно ведётся с 2003 г. Она представляет собой очень высокопроизводительную БД, которая состоит из графов.

Neo4j позволяет использовать различного рода транзакции, дает возможность индексировать много различной информации и имеет в том числе – масштабируемость. Ее БД работает и сопровождается кластером, состоящим из большого количества серверов. Чтобы быстро сделать обход всех имеющихся узлов графа, в Neo4j внедрен особый алгоритм-фреймворк. Он в качестве языка запросов использует собственный язык Cypher, во многом очень схожий с SQL-запросами. Ниже на рисунке 5 приведена структура хранения данных в графовой системе управления базами данных.

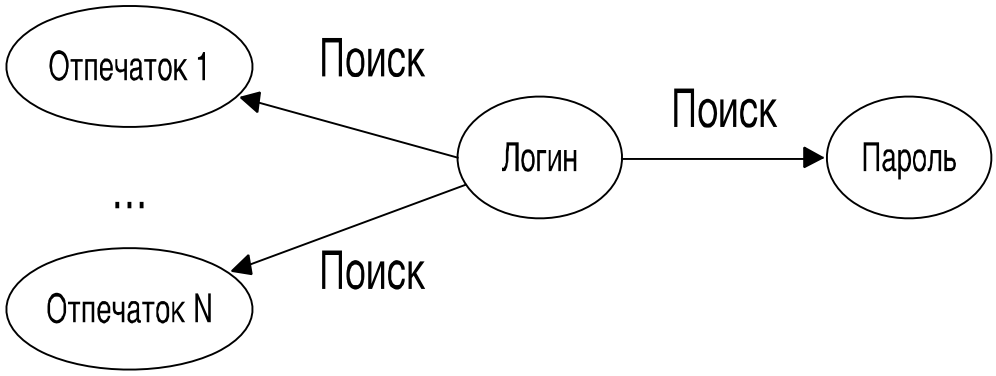


Рисунок 5 – Структура хранения данных в графовой системе управления базами данных

Согласно разработанной блок-схеме ниже приведен запрос на добавление нового пользователя в графовую СУБД:

```
//Ввод данных пользователя
$userLogin = «testUser»;
$userPassword = «UserPassword»;
$userFingerprintsArray = array("Fingerprint 1», "Fingerprint 2», "Fingerprint 3»);

//Установка соединения с базой данных
use Everyman\Neo4j\Client,
 Everyman\Neo4j\Transport,
 Everyman\Neo4j\Node,
 Everyman\Neo4j\Relationship;
$client = new Client(new Transport('localhost', 7474));

//Создание узла с логином
$login = new Node($client);
$login->setProperty('login', $userLogin)->save();
```

```
//Создание узла с паролем
$password = new Node($client);
$password->setProperty('password', $userPassword)->save();

//Создание отношения логина с паролем
$login->relateTo($password, 'IN')->save();
foreach ($userFingerprintsArray as $fingerprint)

//Создание узла с отпечатком пальца
$fingerprint = new Node($client);
$fingerprint->setProperty('fingerprint', $fingerprint)->save();

//Создание отношения логина с отпечатком
$login->relateTo($fingerprint, 'IN')->save();
```

Все пользовательские данные хранятся в реляционной БД. К ней осуществляется доступ после успешной авторизации в системе, которая реализована с использованием Neo4j. Блок-схема работы в графовой БД представлена на рисунке 6.

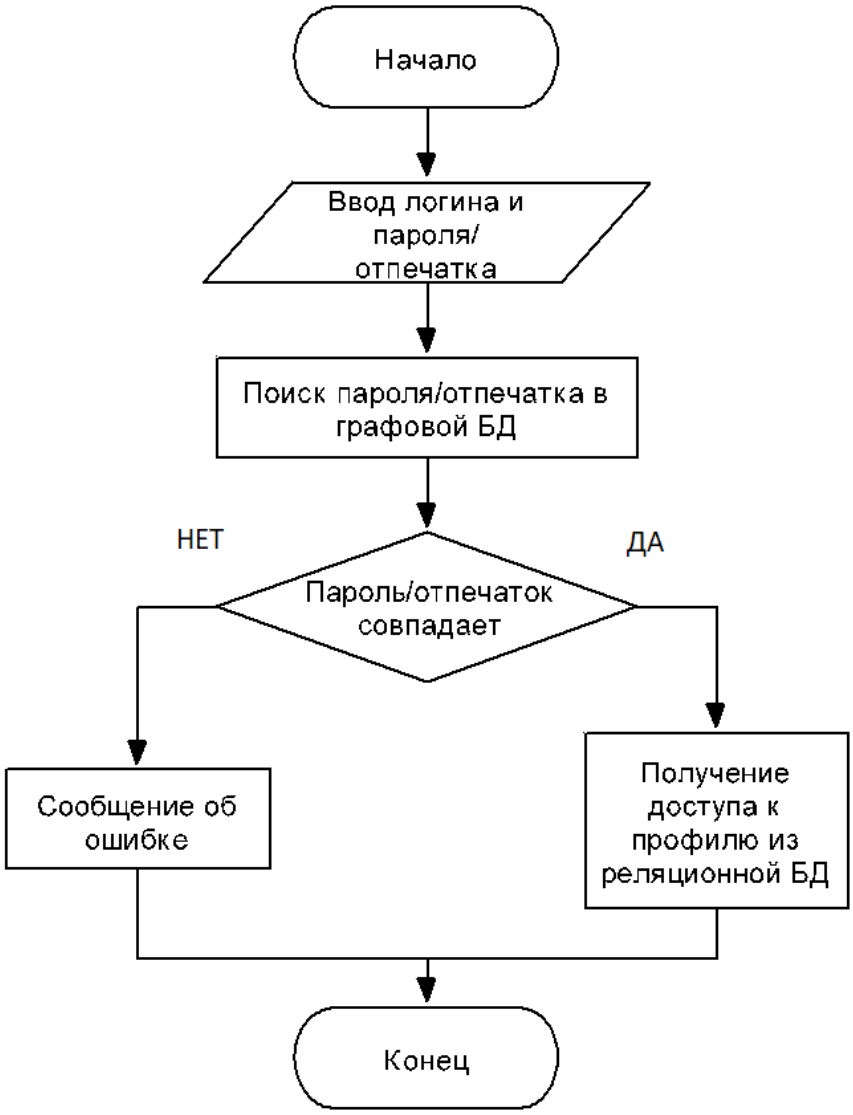


Рисунок 6 – Блок-схема работы с графовой БД

Заключение. Научный прогресс не стоит на месте, поэтому рассмотренные современные методы проверки достоверности информации и способы ее защиты нуждаются в использовании более новых и улучшенных алгоритмов защиты данных с применением гибридного шифрования. Для обеспечения более полной безопасности и надежности при работе с различными сведениями целесообразно совместное применение асинхронных/синхронных ключей, биометрии идентификации личности (в частности отпечатка пальца) и использование графовой БД. Такие подходы позволяют во много раз уменьшить угрозы потери/стирания, перехвата и несанкционированного доступа к данным различных злоумышленников в сети. С каждым днем эти злоумышленники находят все более новые ухищренные способы воздействия на закрытую информацию, которая передается по открытым каналам связи. И это, несомненно, будет создавать все новые дополнительные сложности в сфере информационной защиты данных и, безусловно, являться одной из главных проблем обеспечения кибербезопасности.

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 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. – Краснодар, 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 : сборник научных статей. – 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. Ищейнов В. Я. Защита конфиденциальной информации : учебное пособие / В. Я. Ищейнов, М. В. Мецатунян. – М. : Форум, 2013. – 256 с.

8. Кухарев Г. А. Биометрические системы: методы и средства идентификации личности человека / Г. А. Кухарев. – Санкт-Петербург : Политехника, 2001. – 240 с.

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

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

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

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

13. Хорев П. Б. Программно-аппаратная защита информации : учебное пособие / П. Б. Хорев. – Москва : Форум, 2013. – 352 с.

14. Чипига А. Ф. Информационная безопасность автоматизированных систем / А. Ф. Чипига. – Москва : Гелиос АРВ, 2017. – 336 с.

15. Шаньгин В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. – Москва : ДМК, 2014. – 702 с.

16. Chor B. A knapsack-type public key cryptosystem 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, no. 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 : 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. 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]. Krasnodar, 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 : sbornik nauchnyh statey* [V International Scientific and Practical Conference of Young Scientists dedicated to the 54th anniversary of the flight of Yu.A. Gagarin in space : proceedings]. 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 technologies], 2011, vol. 4, pp. 62–65.

7. Ishcheynov V. Ya., Metsatunyan M. V. *Zashchita konfidentsialnoy informatsii : uchebnoe posobie* [Protection of confidential information : textbook]. Moscow, Forum Publ., 2013. 256 p.

8. Kukharev G. A. *Biometricheskie sistemy: metody i sredstva identifikatsii lichnosti cheloveka* [Biometric systems: methods and means of identification of a person's personality]. St Petersburg, Politekhnika Publ., 2001. 240 p.

9. 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 Publ., 2004, p. 168.

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

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

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

13. Khorev P. B. *Programmno-apparatnaya zashchita informatsii : uchebnoe posobie* [Software and hardware information protection : textbook]. Moscow, Forum Publ., 2013. 352 p.

14. Chipiga A. F. *Informatsionnaya bezopasnost avtomatizirovannykh sistem* [Information Security of Automated Systems]. Moscow, Gelios APB Publ., 2017. 336 p.

15. Shangin V. F. *Informatsionnaya bezopasnost i zashchita informatsii* [Information Security and Information Protection]. Moscow, DMK Publ., 2014. 702 p.

16 Chor B., Rivest R. A knapsack-type public key cryptosystem 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.