РАДИОТЕХНИКА, В ТОМ ЧИСЛЕ СИСТЕМЫ И УСТРОЙСТВА ТЕЛЕВИДЕНИЯ / RADIO ENGINEERING, INCLUDING TELEVISION SYSTEMS AND DEVICES

DOI: https://doi.org/10.60797/IRJ.2024.147.17

ТЕЛЕКОММУНИКАЦИОННАЯ МОДЕЛЬ КОМПЬЮТЕРНОЙ СЕТИ С МНОГОУРОВНЕВЫМ АНАЛИЗОМ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ АЛГОРИТМОВ КВАНТОВОГО ШИФРОВАНИЯ ДЛЯ ГЕНЕРАЦИИ КЛЮЧЕЙ

Научная статья

Толстель А.О.[1, *], Нестеров С.В.[2]

[1, 2] Балтийский федеральный университет имени Иммануила Канта, Калининград, Российская Федерация

* Корреспондирующий автор (lekst-[at]mail.ru)

Аннотация

Целостность и конфиденциальность многоуровневой безопасности связи гарантируется с помощью ключа полученного в результате генерации квантового компьютера. Этот процесс важен для обеспечения безопасности. В данной статье этот процесс используется для генерации ключей аутентификации и ключей сеанса, которые используется в процессе IPSec. Таким образом, реализуется многоуровневое защищённая безопасная связь с использованием квантового ключа и IPSec. Он добавляет поле для реализации стратегии управления на основе безопасности пакета, использует ключевое эффективное время для удовлетворения различных требований безопасности и использует «одноразовый блокнот», алгоритм, обеспечивающий безусловную безопасность. После правил с использованием ключей показан процесс передачи пакетов данных. В данной статье описывается процесс обмена пакетами в данной системе, а также моделирования системы и анализ полученных результатов.

Ключевые слова: распределение ключей, защищенная связь, квантовое шифрование, защита каналов связи, магистральный тракт, периферийное оборудование, трафик.

TELECOMMUNICATION MODEL OF COMPUTER NETWORK WITH MULTILEVEL SECURITY ANALYSIS USING QUANTUM ENCRYPTION ALGORITHMS FOR KEY GENERATION

Research article

Tolstel A.O.[1, *], Nesterov S.V.[2]

[1, 2] Immanuel Kant Baltic Federal University, Kaliningrad, Russian Federation

* Corresponding author (lekst-[at]mail.ru)

Abstract

The integrity and confidentiality of multi-level communication security is guaranteed by a key derived from the generation of a quantum computer. This process is important to ensure the security. In this article, this process is used to generate authentication keys and session keys, which are used in IPSec process. In this way, a multi-level secure communication using quantum key and IPSec is implemented. It adds a field to fulfil the packet security based control strategy, uses key effective time to satisfy different security requirements and uses "one-time cipher pad", an algorithm that provides unconditional security. After key-based rules, the process of data packet transmission is shown. This paper describes the process of packet exchange in this system, as well as modelling the system and analysing the results obtained.

Keywords: key distribution, secure communication, quantum encryption, channel protection, trunk line, peripheral equipment, traffic.

Введение

Современный мир требует постоянно более высокого уровня безопасности. Во многих ситуациях это достигается с помощью криптографии, для которой одним из критических элементов является непредсказуемость ключей шифрования. Другие приложения безопасности, такие как управление идентификацией и доступом, также требуют надежной криптографической основы, основанной на уникальных токенах.

Ключи используются для шифрования информации, а также в других криптографических схемах, такие как цифровые подписи, коды личной идентификации и аутентификации сообщений. Они используются повсюду в современных цифровых коммуникациях и обеспечивают доверие, которое лежит в основе коммуникаций в нашем глобализированном мире, включая Интернет и финансовые системы.

Безопасность этих ключей или цифровых токенов зависит от качества случайности, использованной для создания самого ключа. Если генерация случайных чисел и процессы, связанные с ней, слабы, то ключ можно легко скопировать, подделать или угадать, и безопасность всей системы будет поставлена под угрозу. Поэтому высококачественная генерация ключей, обеспечивающая непредсказуемость случайных ключей, имеет решающее значение для безопасности.

Ключ является основой безопасности защищённых систем передачи данных и используется для обеспечения:

1) конфиденциальности (секретность данных)
2) целостности (данные не были подделаны)
3) аутентификации (данные отправляются нужному человеку в правильном порядке)
4) отказоустойчивости (можно доказать, кто отправил данные)
5) безопасного контроля доступа (с помощью токенов безопасности или паролей)

В такой ситуации логично использовать ключи шифрования, использующие при создании надёжные методы генерации случайных чисел (ГСЧ). В отличие от классической физики, квантовая физика фундаментально случайна. Существуют процессы, непредсказуемость которых является фундаментальной и может быть доказана.

Возможность смоделировать квантовый процесс и доказать его случайность важна в двух отношениях. Во-первых, это позволяет идентифицировать критические параметры, которые затем можно отслеживать в реальном времени, чтобы заранее гарантировать качество создаваемых случайных битов. Это свойство позволяет уменьшить или даже исключить необходимость статистического тестирования выходного потока в реальном времени.

Второе важное преимущество, связанное с использованием квантового процесса, заключается в том, что его режимы отказа можно моделировать и оценивать. Это позволяет разрабатывать ГСЧ, которые «корректно отрабатывают», обеспечивая, например, блокировку случайного потока битов в случае сбоя вместо создания несовершенных случайных чисел. Учитывая тот факт, что квантовая физика описывает поведение фундаментальных строительных блоков (атомов, частиц и т. д.) физического мира, можно утверждать, что все является квантовым, и, следовательно, ГСЧ, основанные на классической физике, также являются квантовыми.

Например, можно сказать, что для ГСЧ, основанного на тепловом шуме электронного компонента, этот шум также является квантовым. Эта точка зрения имеет некоторые основания, но этот шум можно рассматривать как грязный квант, поскольку он состоит из большого ансамбля квантовых процессов, которые взаимодействуют друг с другом. Из-за этого процесс не отражает фундаментальную случайность элементарного квантового процесса. Существуют хорошие ГСЧ, основанные на классической физике, но все, что о них можно сказать, это то, что они создают поток, который, вероятно, является случайным. Напротив, поток битов, создаваемый квантовым ГСЧ (QRNG), доказуемо случаен.

Относительно защищённой придачи данных существуют протоколы связи сетевой безопасности, такие как L2TP, MPLS, TLS/SSL, IPSec [1]. Эти протоколы должны обеспечивать целостность и конфиденциальность, а также должны соблюдать требования к многоуровневой безопасности. Чтобы реализовать безопасную связь между хостами в телекоммуникационной системе в некоторых исследованиях сосредоточились на модели многоуровневой политики безопасности, в частности в работе [2] изучена и улучшена модель контроля доступа [2], а в [3] модель политики доступа сети [3]. Другие исследования направлены на модификации протокола IPSec. В одном из них добавили теги безопасности в IPSec SA [4], в другом — улучшили IPSec на основе авторизации пользователя и программы [5].

Хотя эти методы могут быть в состоянии реализовать многоуровневую сетевую безопасность связи, но ключ, который они используют, получен путем традиционных математических вычислений методом расчета. С развитием компьютерных технологий вычислительная мощность, особенно после появления квантовых компьютерный и квантовых алгоритмов, этот метод обмена ключами, безопасность которого зависит от сложности вычислений, сталкиваются с серьезными проблемами.

Технология квантового распределения ключей (QKD), чья безопасность гарантируется основными принципами квантовой механики, обеспечивает безопасный метод распределения ключей для удаленных пользователей, которые могут обмениваться случайными числами. Развитие надежных реле, квантового реле и квантовой маршрутизации позволяют построить сеть QKD. Ученые создали DARPA сеть, сеть SECOQC [6] и другие сети QKD. Один из методов использования квантовой криптографии – это сочетание квантовой криптографии и классических протоколов связи. Также учёные разработали протокол Q3P путем объединения квантового распределения ключей с протоколом «точка-точка» (PPP) [7], модернизировали протокол TLS/SSL [8], [9] для использования квантового ключа для защиты безопасности данных, использовали QKD в 802.11 [11], [12]. Другие доказали, что интеграция QKD и ISAKMP осуществимы [13].

Квантовые ключи можно использовать во многих сценариях, например в сети правительства, телефонной сети, финансовых сетях и электросетях [14], [15]. Но нет подходящего метода использования технологии квантового распределения ключей для удовлетворения особых требований безопасности в многоуровневых сетях безопасности.

У каждого из протоколов подключения есть свои требования к использованным ресурсам, так же есть свои особенности при взаимодействии. Поэтому логично проводить работы по сборке системы с генерацией ключей шифрования используя наиболее распространённые протоколы.

В этой статье новая модель телекоммуникационной сети разработана используя квантовое распределение ключей и усовершенствования протокола IPSec.

Проектирование модели

А. Иерархическая сеть

Пример многоуровневой сети показан на рис.1, который включает в себя два домена безопасности: производственную сеть и сервисную сеть.

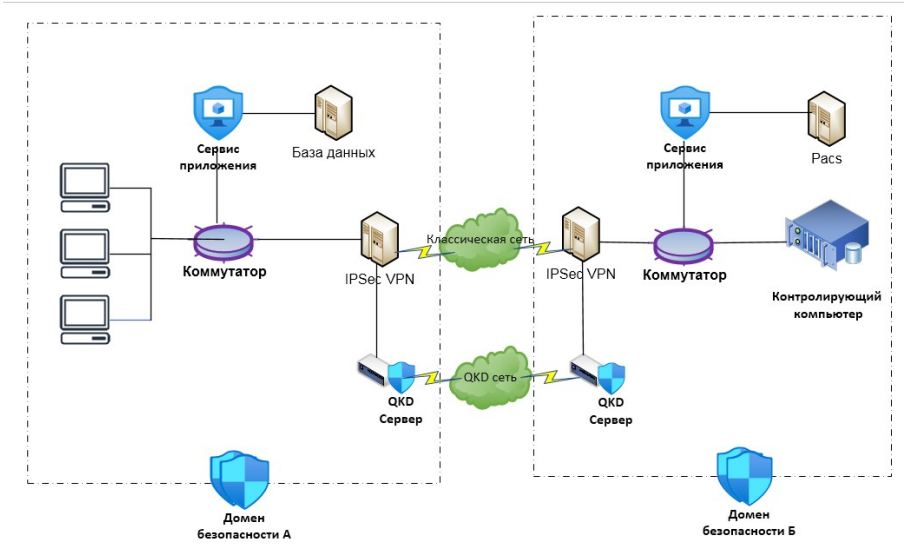

Рисунок 1 - Пример многоуровневой сети
DOI: https://doi.org/10.60797/IRJ.2024.147.17.1

Домен безопасности А представляет собой сервисную сеть, пользователи которой могут получить доступ к службам приложений для работы в сфере офиса, дизайна и разработки. Домен безопасности В представляет собой производственную сеть, пользователи которой используют специальный управляющий компьютер и систему для планирования работ, производства и других задач. Обмен данными между двумя службами безопасности доменов происходит через сервер IPsec, VPN анализирует данные, чтобы убедиться, что передача данных соответствует условиям безопасности. Если условия будут выполнены, передача данных будет завершена через классическую сеть; в противном случае передача будет прекращена. Чтобы использовать функцию безопасности квантового ключа распределения в иерархической сети, мы размещаем сервера квантовых ключей в каждом домене безопасности для организации сервиса квантового распределения и хранения ключей.

Б. Модель использования квантового ключа

Квантовый ключ хранится в базе данных, каждая пара IP-адресов (IP1, IP2) соответствует последовательности данных квантового ключа $K_{IP1,IP2}$, и «C» представляет собой существующую емкость хранилища ключей, C_m представляет собой критические значения ключевых величин, адрес которых необходимо восстановить. Условие запуска для процесса распределения квантовых ключей описывается следующим образом:

$$C < C_m$$

Алгоритм «Одноразовый блокнот» (One-time pad (OTP)) доказал свою эффективность и безусловную безопасность. Длина его ключа равна длине текста. Для достижения безусловной безопасности передачи данных, мы добавляем алгоритм «одноразового блокнота» в набор алгоритмов шифрования и дешифрования, определенный как AT = {AES, OTP, DES и т. д.}.

По структурным характеристикам IPSec протокола, весь процесс состоит из трех типов ключей: ключ аутентификации, главный ключ и ключ сеанса. В нашей модели основная идея – замена ключа аутентификации и сеанса, на ключи сгенерированный с помощью квантовых ключей. При использовании квантового ключа для обеспечения многоуровневой безопасности данных необходимо учитывать баланс между производительностью QKD и требованиями безопасности. Поэтому введем временной параметр TM, который используется для обозначения времени действия сеансового ключа. Мы используем TM для обозначения сколько раз можно использовать ключ. Например, время действия сеансового ключа для алгоритма OTP – TM=1.

Зададим четыре уровня безопасности: совершенно секретно (top secret (TS)), конфиденциально (confidential (CS)), секретно (secret (S)) и не секретно (no secret (N)), правила для данных пакетов разного уровня представлены в Таблице 1.

В Таблице 1 параметры, a_1, a_2, a_3, a_4 являются целыми положительными числами, и их значения удовлетворяют:

$$a_4 \geq a_3 \geq a_2 \geq a_1 = 1$$

С. Емкость хранилища ключей

Когда скорость генерации ключей квантового распределения ключей системы равна R, а время обработки каждого пакета с длинной l равна t. То для каждого уровня безопасности, средняя длина сеансового ключа будет определяться как L_i, а объем пакетных данных будет определяться как M_i, где $i \in \{1,2,3,4\}$. Когда обе стороны хотят добиться бесперебойной передачи данных с длиной Mi, объем предварительной памяти между ними должен соответствовать следующим условиям:

$$C_{mi} + Rt\frac{M_i}{l} \geq \frac{L_i}{a_i}\frac{M_i}{l}$$

Затем,

$$C_{mi} \geq \frac{M_i}{l}\left(\frac{L_i}{a_i} - Rt\right), i \in \{1,2,3,4\}$$

Таким образом, общая емкость хранилища ключей для передачи в обе стороны может быть получена,

$$C_m = \sum_i C_{mi} \geq \sum_i \frac{M_i}{l}\left(\frac{L_i}{a_i} - Rt\right), i \in \{1,2,3,4\}$$

Когда среднее количество ключей, используемых каждым пакетом меньше количеству ключей QKD при обработке пакета времени, то есть $L_i/a_i < Rt$, тогда предварительное сохранение не требует квантового ключа.

Таблица 1 - Правила для пакетов данных

DOI: https://doi.org/10.60797/IRJ.2024.147.17.2

Уровень безопасности	Алгоритм	ТМ
Совершенно секретно (TS)	OTP	a_1=1
Конфиденциально (CS)	Выберите один из AT	a_2
Секретно (S)	Выберите один из AT	a_3
Не секретно (N)	Выберите один из AT	a_4

Таблица 2 - Пример SPD политики

DOI: https://doi.org/10.60797/IRJ.2024.147.17.3

Уровень безопасности отправителя	Уровень безопасности получателя	Уровень безопасности пакта	Направление	Режим обработки
TS	S	TS	Наружу	Отказ
TS	S	S	Наружу	Отправка

Новый процесс передачи данных

Была внедрена локальная база данных доступа к пользовательским данным (User Access Database (UAD)). Завершено сопоставление сетевого оборудования, идентификация пользователя, идентификация уровня безопасности пользователя в улучшенном IPSec на основе авторизации пользователя. Полезная нагрузка полномочий вставляется в сообщения 5 и 6 для осуществления обмена уровнем безопасности. Эти два сообщения принадлежат мастер-режиму IKE и будут использоваться для аутентификации. База данных политики безопасности SPD в модифицированной версии. IPSec на основе прав пользователя используется для управления режимом обработки пакетов данных.

Наша модель основана на предположении, что каждый пакет имеет флаг уровня безопасности. Улучшаем структуру базы данных, добавив новое поле с именем «уровень безопасности пакета», чтобы можно было не только поддерживать классификацию пользователя, но также и для поддержки классификации пакетов. Когда отправитель и получатель имеют одинаковый уровень безопасности, а пакеты данных имеют разные уровни безопасности, пример стратегии данных доставки пакетов показан в Таблице 2.

После добавления к процессу распределения квантовых ключей, весь процесс отправки/получения данных меняется. Процесс отправки показан на рис.2, а процесс получения – показан на рис.3.

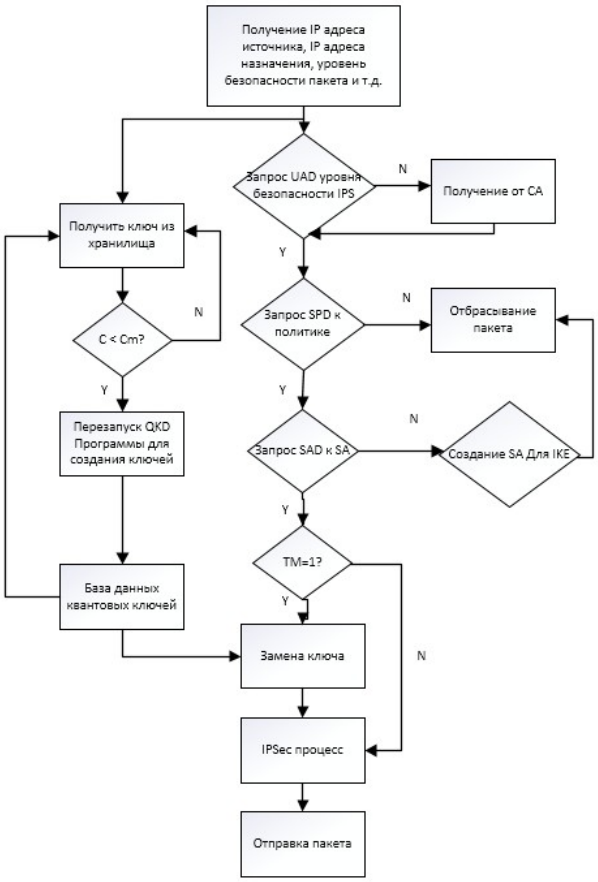

Рисунок 2 - Процесс отправки пакета данных
DOI: https://doi.org/10.60797/IRJ.2024.147.17.4

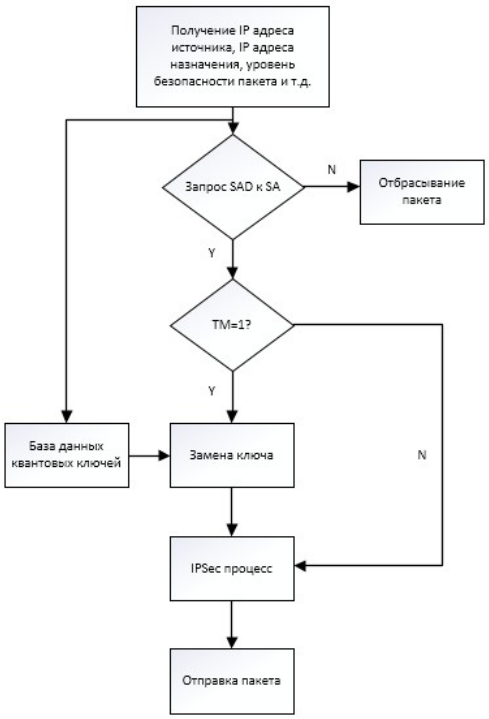

Рисунок 3 - Процесс получения пакета данных
DOI: https://doi.org/10.60797/IRJ.2024.147.17.5

На отправляющем узле программа сначала извлекает источник и IP-адрес назначения, уровень безопасности пакета из пакета данных. Затем она запрашивает UAD, чтобы получить информацию о безопасности уровня обеих

сторон связи в соответствии с IP-адресом. Если в базе данных нет уровня безопасности пользователя, применяется CA для сертификации. После этого программа запрашивает SPD, чтобы определить можно ли отправить пакет. Если ответ ДА, необходим доступный SA. Если его нет, то пакет будет отброшен. Когда в SA нет подходящего SAD, необходимо вызвать IKE, чтобы создать его. Когда TM=1, текущий сеансовый ключ необходимо заменить с помощью квантового ключа. Наконец, программа отправляет пакет после шифрования.

В принимающем узле программа сначала получает источник и IP-адрес назначения, идентификацию SA и другую информацию из пакета данных. Затем она запрашивает SAD определить, существует ли эффективная SA в соответствии с идентификацией. Когда действующая SA не существует, пакет будет отброшен. В противном случае она заменяет текущий сеансовый ключ используя квантовый ключ если TM=1. Наконец, программа отправляет пакет на верхний уровень после расшифровки.

В этих двух процессах распределение квантовых ключей не всегда будет активно. После получения IP-адреса отправителя и получателя программе необходимо получить сумму ключей, которые принадлежат паре IP-адресов. Если объем памяти меньше критического значения Cm, то программу квантового распределения ключей необходимо перезапустить.

Заключение

В этой статье представлена модель коммуникации, в которой время действия сеансового ключа используется для решения проблем низкой скорости распространения квантового ключа, а алгоритм OTP используется для достижения безусловной безопасности для данных самого высокого уровня. Были разработаны правила использования квантового ключа и описаны процессы отправки и получения пакета. Использование этой модели может удовлетворить потребности разный уровень безопасности. Этот новый метод может обеспечить безопасность передачи с различной конфиденциальностью.

Конфликт интересов

Не указан.

Рецензия

Гибадуллин Р.Ф., Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ, Казань, Российская Федерация

DOI: https://doi.org/10.60797/IRJ.2024.147.17.6

Conflict of Interest

None declared.

Review

Gibadullin R.F., Kazan National Research Technical University named after A.N. Tupolev – KAI, Kazan, Russian Federation

DOI: https://doi.org/10.60797/IRJ.2024.147.17.6

Список литературы на английском языке / References in English

1. Kent S. Security Architecture for the Internet Protocol / S. Kent, K. Seo // IETF RFC 4301. — 2005
2. Cao L.F. Research on access control model of enclave boundary in multi-level secure network / L.F. Cao, X.Y. Chen, X.H. Du [et al.] // Computer Engineering and Applications. — 2011. — Vol. 47. — № 32. — P. 118–122.
3. Liu H.L. A model of multilevel security policy in combination with user access / H.L. Liu, B. Yu // Computer Engineering. — 2010. — Vol. 36. — № 4. — P. 134–137.
4. Yang X. Research of IPsec Based on Implicit Security Label / X. Yang, L. Cao // Computer Engineering. — 2011. — Vol. 37. — № 13. — P. 109–112.
5. Meng X.Y. Research of Multilevel Security Network / X.Y. Meng. — Xian: XidianUniversity, 2008.
6. Poppe A. Outline of the SECOQC quantum-key-distribution network in Vienna / A. Poppe, M. Peev, O. Maurhart // International Journal of Quantum Information. — 2008. — Vol. 6. — P. 209–218.
7. Ghernaouti-Helie S. Upgrading PPP security by Quantum Key Distribution / S. Ghernaouti-Helie, M.A. Sfaxi // International Conference on Network Control and Engineering for QoS, Security and Mobility. — 2005. — P. 45–59.
8. Elboukhari M. Improving TLS Security By Quantum Cryptography / M. Elboukhari, M. Azizi, A. Azizi // International Journal of Network Security & Its Applications. — 2010. — № 2(3). — P. 87–100. — DOI: 10.5121/ijnsa.2010.2306.
9. Pivk M. SSL/TLS with Quantum Cryptography / M. Pivk, C. Kollmitzer, S. Rass // 2009 Third International Conference on Quantum, Nano and Micro Technologies. — Cancun, 2009. — P. 96–101. — DOI: 10.1109/ICQNM.2009.29.
10. Huang X. Implementation of Quantum Key Distribution in Wi-Fi (IEEE 802.11) Wireless Networks / X. Huang, S. Wijesekera, D. Sharma // 2008 10th International Conference on Advanced Communication Technology. — 2008. — Vol. 2. — P. 865–870.
11. Wijesekera S. Multi-Agent Based Approach for Quantum Key Distribution in WiFi Networks / S. Wijesekera, X. Huang, D. Sharma // Agent and Multi-Agent Systems: Technologies and Applications. KES-AMSTA 2009. Lecture Notes in Computer Science / A. Håkansson, N.T. Nguyen, R.L. Hartung [et al.]. — Berlin: Springer, 2009. — Vol. 5559. — P. 293–303. — DOI: 10.1007/978-3-642-01665-3_30.
12. Elliott C. Building the quantum network / C. Elliott // New Journal of Physics. — 2002. — № 4. — P. 46–46.
13. Sfaxi M.A. Using Quantum Key Distribution within IPSEC to secure MAN communications / M.A. Sfaxi, S. Ghernaouti-Hélie, G. Ribordy [et al.] // Proceedings of metropolitan area networks. — 2005.
14. Suchat S. Quantum key distribution via an optical wireless communication link for telephone network / S. Suchat, W. Khunnam, P. Yupapin // Optical Engineering. — 2007. — Vol. 46. — № 10. — P. 100502. — DOI: 10.1117/1.2786479.
15. Liu D. Application of quantum keys in SSL VPN of power grid / D. Liu, S. Wang, J. Zhou [et al.] // Power System Technology. — 2014. — Vol. 38. — № 2. — P. 544-548. — DOI: 10.13335/j.1000-3673.pst.2014.02.042.