2. Free Software in education : Advise, vision and proposed action plan [Elektronnyj resurs] / H. Bruyninckx, M. De Quid, W. Feijens, K. Lauwers, E. Verhulst [Education Department, Ministry of the Flemish Community]. – Rezhym dostupu: http://www.ond.vlaanderen.be/ict/english/free_software_in_ed_Flemish_Community_advise.pdf (12.01.2015 r.).
3. Karpenko M. Perspektyvy ta mozhlyvosti vprovadzhennya vil'nogo programnogo zabezpechennya v navchal'nyh zakladah ta derzhavnyh ustanovah Ukrainy [Elektronnyj resurs] / M. Karpenko, M. Kiyak. – Rezhym dostupu: http://old.niss.gov.ua/Monitor/june2009/15.htm (12.02.2015 r.).
4. Kravchina O. Є. Osnovni napryamy vykoristannya vil'nogo programnogo zabezpechennya v zakladah osvity zarubizhzhya / O. Є. Kravchyna // Materialy Zvitnoi nauk.-prakt. konferencii In-tu inform. tehnologij i zasobiv navch. NAPN Ukrainy. – K. : IITZN NAPNU, 2011. – S. 22-24.
5. What is free software? [Elektronnyj resurs] // Operacionnaya sistema GNU. – Rezhym dostupu: https://www.gnu.org/philosophy/free-sw.html (6.09.2014 r.).
6. Buch G. Obiektno-orientirovannyj analiz i proektirovanie / G. Buch. – M. : Vil'yams, 2008. – 720 s.
7. Kaufman V. Sh. Yazyki programmirovaniya. Koncepcii i principy / V. Sh. Kaufman. – M. : DMK «Press», 2010. – 464 s.
8. Larman K. Primenenie UML 2.0 i shablonov proektirovaniya. Vvedenie v ob`ektno-orientirovannyj analiz, proektirovanie i iterativnuyu razrabotku / K. Larman. – SPb. : Vil'yams. – 2013. – 736 s.
9. Straustrup B. Yazyk programmirovaniya S++ / B'ern Straustrup. – M. : Binom ; Nevskij dialekt, 2008. – 1136 s.
10. Ekkel B. Filosofiya Java / Bryus Ekkel. – [4-e vid.]. – SPb. : Piter, 2015. – 1168 s.
11. Wagner B. Effective C# (Covers C# 4.0): 50 Specific Ways to Improve Your C# / Bill Wagner. – [2nd Ed.]. – Boston : Pearson Education, Inc, 2010. – 352 s.
12. AS «Dekanat» : programnyj produkt [Elektronnyj resurs] / Naukovo-doslidnyj instytut prykladnyh programnyh informacijnyh tehnologij, m. Kyiv [vyrobnyk]. – Rezhym dostupu: http://www.ndipit.com.ua/ua/rozrobky/as-dekanat (12.02.2015 r.).
13. Dekanat : paket program [Elektronnyj resurs] / Politek-soft : oficijnyj sajt vyrobnyka. – Rezhym dostupu: http://www.politek-soft.kiev.ua/ru/index.php?do=products&product=deanery (26.12.2014 r.).
14. Visual Studio : oficijnyj sajt [Elektronnyj resurs]. – Rezhym dostupu: http://www.visualstudio.com/ (12.01.2015 r.).
15. Xamarin : oficijnyj sajt [Elektronnyj resurs]. – Rezhym dostupu: http://xamarin.com/ (12.11.2014 r.).
16. Qt : oficijnyj sajt [Elektronnyj resurs]. – Rezhym dostupu:http://www.qt.io/ (12.01.2015 r.).
17. OpenGL : oficijnyj sajt [Elektronnyj resurs]. – Rezhym dostupu: https://www.opengl.org/ (12.01.2015 r.).
18. Extensible Markup Language (XML) [Elektronnyj resurs] / W3C : oficijnyj sajt. – Rezhym dostupu: http://www.w3.org/XML/ (12.11.2014 r.).
19. Sammerfild M. Qt professional'noe programmirovanie / M. Sammerfild. – M. : Simvol-Plyus, 2011. – 552 s.
20. Shlee M. Qt 4.8. Professional'noe programmirovanie na C++ / M. Shlee. – SPb. : BHV-Peterburg, 2012. – 912 s.
21. MySQL. Optimizaciya proizvoditel'nosti / B. Shvarc, P. Zajcev, V. Tkachenko D. Zavodny. – M. : Simvol-Plyus, 2010. – 816 s.
22. Dyubua P. MySQL / P. Dyubua. – SPb. : Vil'yams, 2004. – 1056 s.
23. MySQL : oficijnyj sajt [Elektronnyj resurs]. – Rezhym dostupu: http://www.mysql.com/ (12.01.2015 r.).
24. A Structured Approach to Enterprise Modeling & Analysis [Elektronnyj resurs] / IDEF. Intergated DEFinition Methods. – Rezhym dostupu: http://www.idef.com/ (12.01.2015 r.).
25. Osnovy metodologii IDEFX1 [Elektronnyj resurs] / G. Vernikov // CIT Forum. – Rezhym dostupu: http://citforum.ck.ua/cfin/idef/idef1x.shtml (26.14.2014 r.).
26. Workbench 6.2 // MySQL : oficijnyj sajt [Elektronnyj resurs]. – Rezhym dostupu: http://www.mysql.com/products/workbench/ (12.01.2015 r.).
27. Goma H. UML. Proektirovanie sistem real'nogo vremeni, raspredelennyh i parallel'nyh prilozhenij / H. Goma. – M. : DMK «Press». – 2014. – 700 s.
28. Unified Modeling Language (UML) Resource Page [Elektronnyj resurs] / Object Management Group. – Rezhym dostupu: http://www.uml.org/ (12.01.2015 r.).

Рецензія/Peer review : 8.1.2015 р. Надрукована/Printed :24.1.2015 р.
Стаття рецензована редакційною колегією

УДК 004.056.53 +530.145

Е.В. ВАСИЛИУ
Одесская национальная академия связи им. А.С. Попова

СХЕМА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ СИСТЕМЫ ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ С ИСПОЛЬЗОВАНИЕМ ПРОТОКОЛОВ КВАНТОВОЙ КРИПТОГРАФИИ

Предложена схема криптографической защиты системы электронного голосования. Криптографическая защита основана на использовании квантового битового обязательства и квантового разделения секрета, что обеспечивает повышенный уровень безопасности по сравнению со схемами, не использующими протоколы квантовой криптографии.

Ключевые слова: квантовое битовое обязательство, квантовое разделение секрета, квантовая криптография, электронное голосование.

YE.V. VASILIU
Odessa National Academy of Telecommunications n.a.A.S. Popov

SCHEME OF CRYPTOGRAPHIC PROTECTION OF ELECTRONIC VOTE SYSTEM BY THE USE OF QUANTUM CRYPTOGRAPHY PROTOCOLS

The scheme of cryptographic protection of electronic vote system is proposed. Cryptographic protection is based on use of the quantum bit commitment and quantum secret sharing that provides the higher level of security in comparison with the schemes, which are not using protocols of quantum cryptography.

Keywords: quantum bit commitment, quantum secret sharing, quantum cryptography, electronic vote.

Введение

Постановка задачи и анализ исследований по данной проблеме. Использование квантовых технологий в криптографической защите информации обладает определенными преимуществами [1]. Прежде всего, протоколы и шифры классической (не квантовой) криптографии, обладают, как правило, только вычислительной стойкостью. Исключением являются лишь некоторые шифры, например, шифр Вернама, обладающий теоретико-информационной стойкостью. При этом шифр Вернама также имеет недостаток – слишком большую длину ключа, равную длине шифруемого сообщения, что ограничивает его практическое использование.

Большинство протоколов квантовой криптографии при определенных условиях обладают теоретико-информационной стойкостью [1]. Что касается квантовых протоколов разделения секрета и так называемого "битового обязательства", то, в отличии от аналогичных по назначению классических протоколов, они позволяют обнаружить атаку не только "внутренних" нарушителей, т.е. участников процедуры разделения секрета, но и "внешних", т.е. нарушителей, пытающихся перехватить информацию, передаваемую в каналах связи между легитимными участниками.

Процедура разделения секрета предлагалась ранее для использования в системах электронного голосования [2]. Также известна схема, одновременно использующая в ходе подсчета результатов выборов разделение секрета и битовое обязательство [3]. Однако, подобные процедуры, базирующиеся на соответствующих протоколах квантовой криптографии, ранее предложены не были. **Целью** настоящей статьи является разработка схемы контроля группой уполномоченных лиц процедуры подсчета результатов выборов с использованием протоколов квантового разделения секрета и битового обязательства.

Основной материал

Рассмотрим предлагаемую схему (рис. 1). Имеется автоматическое устройство, назовем его Алиса. Предусмотрен контроль за этим устройством независимыми наблюдателями в ходе выборов. Когда избиратель голосует, Алиса направляет на другое устройство, назовем его Бобом, несколько фотонов. Устройство Боб располагается на избирательном участке, рядом с Алисой. Фотоны Алисы находятся в одном из четырех состояний поляризации, используемых в известном протоколе BB84 [4]. Голосование проводится последовательно за каждого отдельного кандидата, при этом поляризация фотонов для каждого голосования выбирается случайно из четырех возможных вариантов. Все фотоны, отправленные Алисой для голосования за каждого кандидата, достигают Боба одновременно. Когда избиратель голосует "против", устройство Боб выполняет квантовое измерение в базисе $\{|0\rangle,|1\rangle\}$, а в случае голосования "за" Боб проводит измерение в базисе $\{|+\rangle,|-\rangle\}$. Измерение проводится немедленно и одновременно для всех фотонов данного акта голосования.

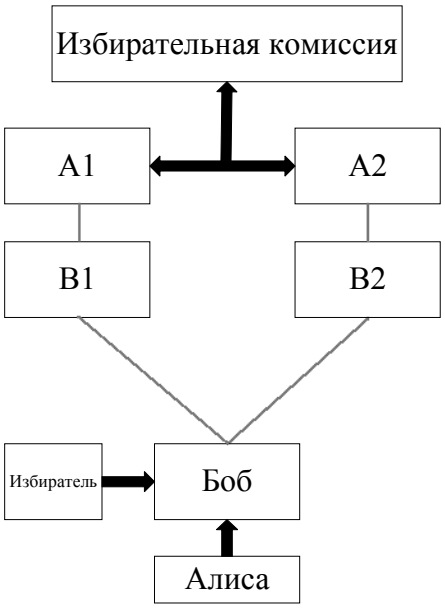

Рис. 1. Общая схема обеспечения информационной безопасности электронного голосования

Описанная последовательность должна быть выполнена для всех кандидатов из списка. Алиса должна направить группы фотонов столько раз, сколько кандидатов имеется в списке. После этого немедленно и со скоростью света Боб посылает двум своим агентам B_1 и B_2 результаты измерения. Агенты B_1 и B_2 должны быть расположены справа и слева (симметрично) от Боба на некотором расстоянии d. Обоим агентам направляется идентичная информация. Ее передача производится в зашифрованном виде. Передачу ключа для шифрования можно выполнять, например, с помощью квантового протокола распределения ключей BB84, обладающего теоретико-информационной стойкостью.

После того, как истекает отведенное для голосования время, начинается передача данных представителям избирательной комиссии. Агенты B_1 и B_2 выполняют передачу двум агентам A_1 и A_2 избирательной комиссии. Передача производится одновременно в фиксированный момент времени. Каждая соответствующая пара агентов A и B может находиться в недоступном для

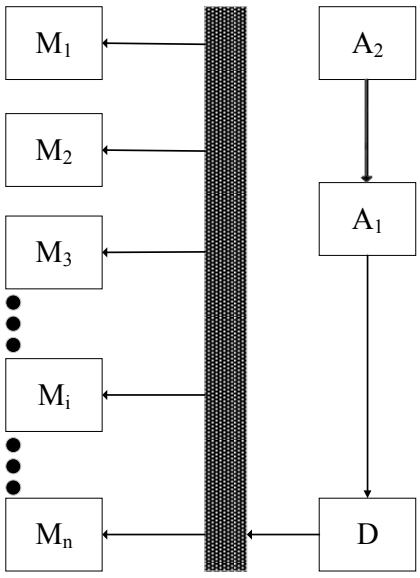

Рис.2 – Схема разделения секрета между членами избирательной комиссии. A_1, A_2 – агенты Алисы, D – дилер, M_1, M_2, …, M_n – члены избирательной комиссии

проникновения помещении.

Агенты A_1 и A_2 должны проверить, совпадает ли информация, полученная от соответствующих агентов B_1 и B_2. В случае, если информация одинакова, то попытки обмана не было. Затем агенты А проверяют – действительно ли имело место взятие обязательства в момент времени $t_0 - d/2c$, где через t_0 обозначено время, когда агенты А получают информацию, а через c – скорость света. Теперь оба агента А должны проверить соответствие поляризаций фотонов, которые ранее Алиса направляла Бобу. Такая проверка проводится на основе результатов, полученных от агентов B_1 и B_2. В итоге на основании этих данных члены избирательной комиссии получают информацию о том, какой выбор – "за" или "против" был сделан избирателем. Так как на практике в каналах связи всегда есть шум, то при проверке учитывается допустимый уровень шума. Именно для этой цели на первом этапе Алиса посылает Бобу не по одному фотону для каждого кандидата в списке, а по группе фотонов в одинаковых состояниях поляризации, что позволяет определить статистику измерений.

Описанная выше квантовая схема битового обязательства необходима для четкого фиксирования выбора избирателя. При этом любые претензии после завершения подсчета голосов будут несостоятельны.

После того, как оба агента А получат данные, необходимо выполнить разделение секрета. Для этого мы используем квантовую схему, описанную в работе [5]. Количество участников разделения секрета соответствует количеству членов избирательной комиссии. Каждая доля секрета передается одному из членов комиссии. Для определения того, какой голос был отдан избирателем, необходима взаимная демонстрация долей секрета всеми членами комиссии. Схема разделения секрета исключает альтернативное определение голоса избирателя. Таким образом, делается невозможным подсчёт голосов без взаимного контроля членами комиссии.

Остановимся на более детальном описании схемы разделения секрета (рис. 2). Итак, каждый из n членов комиссии должен получить по одной доле секрета. С этой целью необходимо приготовить состояния Гринбергера-Хорна-Цайлингера (ГЦХ):

$$|\psi\rangle_{GHZ} = \frac{1}{\sqrt{2}}\left(|000...0\rangle + |111...1\rangle\right). \tag{1}$$

Состояния $|0\rangle = |z+\rangle$ и $|1\rangle = |z-\rangle$ – это собственные состояния фотонов при измерении поляризации в вертикально-горизонтальном базисе. Обозначим такой базис через z.

Предположим сначала, что комиссия состоит только из двух членов. Далее мы рассмотрим разделение секрета произвольным числом членов комиссии. Один из участников разделения секрета должен являться дилером, обозначим его через D. Пусть D представляет из себя автоматическое устройство, которое связано с устройствами A_1 и A_2. В случае двух членов избирательной комиссии устройство D генерирует ГЦХ-триплеты и хранит у себя один из фотонов триплета. По одному из двух других фотонов дилер D отправляет двум членам комиссии. Обозначим их как M_1 и M_2. Затем каждый участник разделения секрета должен случайным образом выбрать один из трех взаимно несмещенных базисов для кубитов-фотонов, в котором будет измеряться их поляризация. Каждый участник должен выбрать свой базис независимо от других участников.

Собственные состояния диагонального базиса x выражаются через состояния вертикально-горизонтального базиса известным образом:

$$|0\rangle_x = |+x\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right),$$

$$|1\rangle_x = |-x\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right), \tag{2}$$

а для кругового базиса y:

$$|0\rangle_y = |+y\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + i|1\rangle\right),$$

$$|1\rangle_y = |-y\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - i|1\rangle\right). \tag{3}$$

Собственные состояния при измерениях в вертикально-горизонтальном базисе можно выразить через собственные состояния при измерениях в диагональном и круговом базисах:

$$|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_x + |1\rangle_x\right), \qquad |1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_x - |1\rangle_x\right), \tag{4}$$

$$|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_y + |1\rangle_y\right), \qquad |1\rangle = -\frac{i}{\sqrt{2}}\left(|0\rangle_y - |1\rangle_y\right). \tag{5}$$

Когда квантовые измерения проводятся в диагональном и круговом базисах, могут получаться значения 0 и 1. Это зависит от того, какая поляризация имеет место. При этом только половина из проведенных измерений может быть использована для восстановления секрета. Это обусловлено тем, что должны совпадать базисы, выбранные различными участниками. Но поскольку выбор базисов производится случайно, то совпадение базисов происходит только в 50% случаев.

Увеличим теперь число членов избирательной комиссии с двух до произвольного числа. Соответственно увеличим до произвольного числа количество участников разделения секрета. Выразим в виде последовательности $\left[b_1(j), b_2(j), ...b_i(j)...b_n(j)\right]$ набор ГХЦ-состояний, которые используются для разделения секрета. Через *j* обозначен номер ГХЦ-состояния, а нижний индекс обозначает номера частиц триплета, которые находятся у каждого члена комиссии. Самих членов комиссии обозначим через M_1, M_2, M_3 и т. д. Условимся, что когда *i*-й участник выполняет измерение в диагональном базисе, то $b_i(j) = 0$. Когда выбирается круговой базис, то $b_i(j) = 1$.

Из (4) и (5) получаем выражение для состояния $|00...0\rangle$:

$$|00...0\rangle = \prod_{i=1}^{n}\left(\sqrt{\frac{1}{2}}\left(|0\rangle_{b_i} + |1\rangle_{b_i}\right)\right). \quad (6)$$

Состояние $|11...1\rangle$, следовательно, записывается таким образом:

$$|11..1\rangle = \prod_{i=1}^{n}\left(\frac{-i}{\sqrt{2}}\left(|0\rangle_{b_i} - |1\rangle_{b_i}\right)\right). \quad (7)$$

Как следует из доказательства, приведенного в [5], разделение секрета невозможно, когда круговой базис выбран для измерения нечетным числом участников. При выборе кругового базиса четным числом участников ГХЦ-состояние можно записать следующим образом:

$$|\psi\rangle_{GHZ} = \frac{1}{2^{(n+1)/2}}\left(\prod_{i=1}^{n}\left(\sqrt{\frac{1}{2}}\left(|0\rangle_{b_i} + |1\rangle_{b_i}\right)\right)\pm\right.$$
$$\left.\pm\prod_{i=1}^{n}\left(\sqrt{\frac{1}{2}}\left(|0\rangle_{b_i} - |1\rangle_{b_i}\right)\right)\right). \quad (8)$$

Когда круговой базис выбран четным числом участников разделения секрета, результаты измерений *n*-1 члена группы однозначно определяют результат измерения дилера D. Поэтому, однозначно определить результат измерения дилера D все остальные участники могут совместно, открыв друг другу результаты своих измерений. Однако, когда до числа *n*-1 не хватает хотя бы одного члена группы, то возможности восстановить секрет они не имеют.

Вернемся к случаю трех участников: дилер D и два члена избирательной комиссии M_1 и M_2. Когда, например, результат квантового измерения есть $|100\rangle$, то значение "1" результата измерения дилера D рассчитывается следующим образом:

$$l_D = l_1 = l_2 \oplus l_3 \oplus 1. \quad (9)$$

Здесь через l_1 и l_2 обозначены результаты измерений кубитов членов комиссии M_1 и M_2 соответственно, и в приведенном случае оба они имеют значение "0".

Теперь обобщим формулу (9) на произвольное количество членов комиссии. Рассмотрим все те, и только те случаи, когда количество участников, выбравших круговой базис, равно 2(2*k*+1), где *k* является целым неотрицательным числом:

$$l_D = l_1 = l_2 \oplus l_3 \oplus ... \oplus l_n \oplus 1. \quad (10)$$

Если же число членов группы, выполнивших измерение в круговом базисе, выражается как 4*k*, то:

$$l_D = l_1 = l_2 \oplus l_3 \oplus ... \oplus l_n \otimes. \quad (11)$$

Выводы

Предложенная в работе схема криптографической защиты системы электронного голосования использует протоколы квантовой криптографии, как разделения секрета, так и битового обязательства. Несмотря на существующие в настоящее время технологические сложности в реализации, квантовые криптосистемы превосходят по многим показателям классические. Так, квантовые протоколы разделения секрета защищены не только от нечестных действий участников протокола, но и от действий "внешних" злоумышленников, пытающихся перехватить информацию в каналах связи. Используемый же в предложенной схеме квантовый протокол битового обязательства обладает теоретико-информационной стойкостью. Поэтому, предложенная в работе схема защиты системы электронного голосования с использованием протоколов квантовой криптографии обладает большей криптографической стойкостью, чем известные схемы, использующие не квантовые протоколы.

Литература

1. Korchenko O. Quantum Secure Telecommunication Systems / Korchenko O., Vorobiyenko P., Lutskiy M., Vasiliu Ye., Gnatyuk S. // Telecommunications Networks – Current Status and Future Trends (Edited by J.H. Ortiz**).** – InTech, 2012. – P. 211–236.

2. Schoenmarkers B. A. Simple Publicly Verifiable Secret Sharing Scheme and Its Application to

Electronic Voting / B. A. Schoenmarkers // Lecture Notes in Computer Science. – 1999. – Vol. 1666. – P. 148-164.

3. Смарт Н. Криптография / Н. Смарт. – М.: Техносфера, 2005. – 528 с.

4. Lunghi, T. Experimental Bit Commitment Based on Quantum Communication and Special Relativity / T. Lunghi, J. Kaniewski, F. Bussieres, R. Houlmann, M. Tomamichel, A. Kent, N. Gisin, S. Wehner, H. Zbinden // Physical Review Letters. – 2013. – Vol. 111. – 180504.

5. Xiao, L. Efficient Multiparty Quantum-Secret-Sharing Schemes / L. Xiao, G.L. Long, F.G. Deng, J.W. Pan // Physical Review A. – 2004. – Vol. 69. – 052307.

References

1. Korchenko O. Quantum Secure Telecommunication Systems / Korchenko O., Vorobiyenko P., Lutskiy M., Vasiliu Ye., Gnatyuk S. // Telecommunications Networks – Current Status and Future Trends (Edited by J.H. Ortiz). – InTech, 2012. – P. 211–236.

2. Schoenmarkers B. A. Simple Publicly Verifiable Secret Sharing Scheme and Its Application to Electronic Voting / B. A. Schoenmarkers // Lecture Notes in Computer Science. – 1999. – Vol. 1666. – P. 148-164.

3. Smart N. Kriptigrafia / Smart N. – M.: Tehnosfera, 2005. – 528 s.

4. Lunghi, T. Experimental Bit Commitment Based on Quantum Communication and Special Relativity / T. Lunghi, J. Kaniewski, F. Bussieres, R. Houlmann, M. Tomamichel, A. Kent, N. Gisin, S. Wehner, H. Zbinden // Physical Review Letters. – 2013. – Vol. 111. – 180504.

5. Xiao, L. Efficient Multiparty Quantum-Secret-Sharing Schemes / L. Xiao, G.L. Long, F.G. Deng, J.W. Pan // Physical Review A. – 2004. – Vol. 69. – 052307.

Рецензія/Peer review : 12.1.2015 р. Надрукована/Printed :24.1.2015 р.
Стаття рецензована редакційною колегією

УДК 004.82:681.18

А.А. ШИЯН, Ю.Є. ЯРЕМЧУК, Л.О. НІКІФОРОВА, В.Х. КАСІЯНЕНКО
Вінницький національний технічний університет

МОДЕЛЬ СТВОРЕННЯ АВТОМАТИЗОВАНИХ СИСТЕМ УПРАВЛІННЯ ТЕХНОЛОГІЧНИМ ПРОЦЕСОМ З ВИКОРИСТАННЯМ МАТЕМАТИЧНИХ ОПЕРАТОРІВ У ІНФОРМАЦІЙНОМУ ПРОСТОРІ

Поставлено задачу розробки моделі створення автоматизованих систем управління технологічним процесом, який у рамках одного математичного апарату дозволяє описати як технічну, так і людську складові. З використанням операторів, що діють в інформаційному просторі задачі з управління технологічним процесом, побудовано основні елементів теорії автоматичного управління. Це дозволило розробити алгоритм для створення автоматизованих систем управління технологічним процесом, який використовує тільки такі оператори.

Ключові слова: автоматизована система управління, технологічний процес, формування, інформаційний простір задачі, оператор.

A.A. SHIYAN, IU.E. IAREMCHUK, L.O. NIKIFOROVA, V.H. KASIANENKO
Vinnytsia national technical university, Vinnytsia, Ukraine

MODEL FOR CREATING OF AUTOMATED CONTROL SYSTEMS FOR TECHNOLOGICAL PROCESSES WITH USING OF MATHEMATICAL OPERATORS IN THE INFORMATION SPACE

Abstract – The problem on elaboration of a model for the creation of automated control systems for technological process, which in the frame of the same mathematical apparatus allows describing both technical and human components, is developed. With the using of operators, which operate in the information space of problem on management of technological process, the basic elements of the theory of automatic control are constructed. This made it possible to develop an algorithm for the creation of automated control systems for technological process, which only uses such operators.

Keywords: automated control system, technological process, create, information space of problem, mathematical operator.

Вступ. Управління технологічними процесами вимагає значної автоматизації. Важливою обставиною при цьому є те, що необхідність приймати рішення та здійснювати вибір вимагає включення структури управління також і людини. Людина здійснює різноманітну діяльність: від здійснення так званого «управління вручну», до підготовки баз даних для використання в автоматичних системах.

Однак сьогодні все ще існує розбіжність у методах, які використовуються для опису технічної та людської компонент автоматизованих систем управління. Якщо для опису функціонування технічних пристроїв існують добре розвинені математичні методі, то опис людини все ще залишається за межами необхідної математичної формалізації. Найчастіше для цього використовують описові методи психології, теорії прийняття рішень та теорії ігор.

Таким чином, розробка універсальних методів формалізації для моделювання функціонування автоматизованих систем управління технологічними процесами, які на однакому рівні математичного апарату могли б описати і технічну, і людську компоненту, залишається актуальною науковою проблемою.

Аналіз останніх досліджень та публікацій. Сучасні системи автоматичного управління детально описано в [1], де наведено велику кількість прикладів застосування загальних методів теорії автоматичного управління до широкого кола наукових та практичних задач. Показано, що важливою особливістю теорії