

management of information security. Existing typologies of social institutions are based mainly on the external characteristics to them. The formal and informal institutions, development and predatory institutions, social and economic, etc. are described. Such typologies of social institutions are mainly used for problems of economic, political, and social security. Known tools cannot directly to use these typologies to problems of information security. The typology is developed for coding of individuals for carrying out activities within the framework of a social institution, using the methods of their training in methods and standards of individual and collective activity, as well as infrastructures, which within the social institution responsible for their training. It is shown that there are three types of social institutions for the encoding of the individual in methods of activity: personality-nominal, professional-nominal and universal-conceptual. The developed typology can describe the important information security features of social institutions, such as institutions of corruption, mafia, terrorism, law, higher education, and

information characteristics for interaction between social institutions, which are the different types. The developed typology uses only information characteristics, which describe the activities of man, society and the state.

Keywords: social institution, knowledge, activity, individual, information security.

Шиян Анатолій Антонович, кандидат фізико-математичних наук, доцент, доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет.

E-mail: aa_shiyan@mail.ru

Шиян Анатолій Антонович, кандидат физико-математических наук, доцент, доцент кафедры менеджмента и безопасности информационных систем, Винницкий национальный технический университет.

Shiyan Anatoliy A., PhD in Physics, Associate Professor, cathedra of management and information systems security, Vinnitsa National Technical University.

УДК 621.396.39 (045)

МЕТОДИКА ВИБОРУ ПРОЕКТНОГО РІШЕННЯ ДЛЯ РОЗГОРТАННЯ ЗАХИЩЕНОЇ МЕРЕЖІ LTE

Георгій Конахович, Роман Одарченко, Вадим Ткаченко

Для підтримання високошвидкісних додатків, користування новими послугами, підтримки постійного мобільного доступу до мережі Інтернет телекомунікаційним операторам необхідно розробляти плани щодо впровадження новітніх технологій та оновлення вже існуючих підприємств зв'язку з урахуванням загальних тенденцій науково-технічного й інноваційного розвитку. Великий попит на ринку надання послуг зв'язку компенсується наявністю ще більших обсягів пропозицій. Часто замовник телекомунікаційного рішення за величезної кількості пропонованих йому найрізноманітніших послуг на яку відрізняються на порядки цінами не може сам зробити правильний вибір. Саме ґрунтуючись на цьому положенні необхідно запропонувати методику, мета якої полягатиме в узгодженні споживчих запитів до системи зв'язку, заснованої на передачі пакетних даних через канали сучасних стільникових систем зв'язку четвертого покоління. В роботі запропоновано покрокову методику вибору проектного рішення для розгортання мережі LTE із урахуванням потреб захисту інформації. Розглянуто основні вимоги користувачів до мереж нового покоління, проаналізовано яким чином вони впливають на вибір обладнання для побудови мережі. Запропоновано та обґрунтовано опис матриці вибору рішення, на базі якої в кінцевому результаті відбувається вибір проектного рішення, згідно із вимогами користувачів.

Ключові слова: *стільникові мережі зв'язку, базова станція, LTE, матриця вибору рішення, проект, вимоги користувачів, архітектура рішення.*

Вступ. Стан розвитку зв'язку у чималому ступені визначає економічний рівень будь-якої держави. Особливо актуальною проблемою є розвиток телекомунікацій для нашої країни. Існуючі мережі зв'язку вже не можуть задовольнити потреби ринку за якістю та ефективністю обміну інформацією. З іншого боку, розвиток мобільного зв'язку передбачає величезні інвестиції в економіку країни, підвищення рівня інтеграції зі сві-

товим співробітництвом, розвиток малого і середнього бізнесу, розвиток інфраструктури зв'язку загального користування України. Ці обставини обґрунтовують актуальність розробки прогнозів щодо прогнозування перспектив оновлення стільникових операторів України шляхом інвестиційного планування і реалізації такого проекту, як мережа технології Long Term Evolution (LTE). Такі прогнози були розроблені в [6, 7].

На сьогоднішній день питання розгортання LTE є досить нагальним, одразу ж може виникнути резонне питання – чи будуть затребувані масовим ринком «гіпершвидкості» і «суперпослуги» і чи не ляжуть в результаті інвестиції оператора в модернізацію мережі вантажем на плечі рядових користувачів, яких цілком влаштовує доступ до мобільної мережі через GPRS або EDGE. Чи випідно для операторів капіталовкладення в такий проект?

Крім цього, кожен користувач будь-якої мережі (в тому числі і 4G) прагне забезпечити конфіденційність передаваних даних та унеможливити спроби мережових атак на мобільні пристрої. Конфіденційну інформацію у сфері господарської діяльності можна визначати умовно розділити на три сектори:

1. Ділова інформація суб'єкта господарювання;
2. Інформація, що стосується безпосередньо фактичних даних суб'єкта господарювання (інформація персонального характеру);
3. Ноу-хау – так звані секрети виробництва.

Кожен вид інформації може мати різну цінність як для абонентів мереж, так і для зловмисників. Тому, як і в інших видах мереж, в 4G використовуються певні засоби захисту. Тому під час проектування даного типу мереж необхідно обов'язково оцінювати необхідність впровадження механізмів захисту інформації та їх доцільність.

Аналіз досліджень та публікацій. Мета й механізми впровадження нових телекомунікаційних технологій досліджені в опублікованих працях Балабанова І., Галкіна З., Голдовського І., Зуєва А., Іванова Ю., Інджикяна Р., Кобелева О., Коржова В., Курицького А., Мясникова А., а також у декількох захищених в останні роки кандидатських дисертаціях, наприклад, М. Кульченко й Р. Русаковського. Цьому ж присвячені публікації ряду закордонних учених, серед яких дисертант виділяє таких авторів, як Барроу К., Бейлі З., Гревал Р., Козяче Д., Мак-Івор Р., Позначка Р., Ріган К., Стенфілд ІЗ, Уоллес У.Д., Чен К., Шультц Д.Є.

Дослідженню технології LTE присвячено праць багатьох іноземних та вітчизняних авторів (В.О. Тихвінський, С.В. Терентьев, А.Б. Юрчук та інші) [1, 4, 8], були зроблені припущення щодо кількості абонентів в світі в найближчі роки, проте методики прогнозування не розроблялося і не розраховувалась можлива кількість користувачів в Україні. Ці припущення щодо вітчизняних перспектив технологій четвертого покоління були зроблені в [2, 3, 6, 7]. Разом з тим автори не ставили перед собою сформульовані нижче мету й за-

вдання даного дослідження, які в остаточному підсумку й визначають наукову новизну останнього.

Постановка завдання. Великий попит на ринку надання послуг зв'язку компенсується наявністю ще більших обсягів пропозиції. Часто замовник телекомунікаційного рішення за величезної кількості пропонованих йому найрізноманітніших послуг на яку відрізняються на порядки цінами не може сам зробити правильний вибір.

Саме ґрунтуючись на цьому положенні необхідно запропонувати методику, мета якої полягатиме в узгодженні споживчих запитів до системи зв'язку, заснованої на передачі пакетних даних через канали сучасних стільникових систем зв'язку четвертого покоління.

Виклад основного матеріалу дослідження. Традиційно замовник рішення формулює досить конкретне завдання на технічну реалізацію, і компанія-проектувальник пропонує йому найбільш ефективну систему, здатну забезпечити всі споживчі запити. У процесі вибору технічної реалізації також може відбуватися з'ясування потреб замовника шляхом проведення серії досить дорогих переговорів і узгодження всіх особливостей проекрованої системи.

Відмінністю запропонованої методики від звичайних техніко-економічних розрахунків полягає в тому, що на практиці організація – замовник або простий абонент має свої інформаційні потоки, які залежать від технічних можливостей системи зв'язку, кількість і якість яких впливає на дохід компанії, або зручність користування кінцевими послугами. А у зв'язку з переведенням багатьох елементів сучасного ведення справ у віртуальний інформаційний простір ця залежність стає все більш значущою.

У зв'язку з цим, ключовим елементом методики є можливість вибору замовником рішення на основі аналізу власних інформаційних потоків або потоків своєї організації та побудови залежностей отримання додаткового доходу від споживчих властивостей проектового телекомунікаційного рішення.

Після цього за допомогою запропонованої методики проводиться підбір і вартісна оцінка всіх можливих технічних реалізацій систем зв'язку з різними споживчими характеристиками, відбувається порівняння цих оцінок з фінансовими можливостями організації – замовника і вибирається рішення, яке дає організації – замовнику найбільший прибуток або найбільшу ефективність від вкладених в нову систему інвестицій. Таким чи-

ном, самі технічні характеристики системи відходять у пропонованій методиці на другий план.

Для досягнення мети автором проводився аналіз розвитку інформаційного суспільства та участь України в цих процесах, проводяться технічні розрахунки з обґрунтування та узгодженням побудови широкосмугових ліній зв'язку, а також архітектури можливих мереж LTE, наводяться методики інвестиційного, техніко-економічного аналізу та аналізу рішення на наявність шкідливих факторів, що виникають при експлуатації мережі, і в разі їх появи, забезпечення їх усунення. Всі ці елементи в результаті дозволяють побудувати алгоритм вибору телекомунікаційного рішення по споживчому запиту.

Опис матриці вибору рішення і її графічного представлення. Матриця вибору рішення являє собою 4-вимірну матрицю. 3 виміри матриці являють собою фактори споживчих переваг:

- пропускна здатність каналу зв'язку;
- надійність роботи всієї системи зв'язку (в тому числі і захищеність передаваних даних);
- якість в каналі зв'язку (визначається ймовірністю помилки).

Четвертим виміром матриці є відношення «вартість системи зв'язку/дохід від експлуатації нового телекомунікаційного рішення». У разі розгляду дискретного варіанту методики (розглянуто далі) осередки матриці розбиваються по дискретним значенням факторів споживчих переваг. У відповідність їм ставиться додатковий дохід, одержуваний організацією від впровадження рішення з такими характеристиками. Таким чином, кожна технічна реалізація телекомунікаційного рішення вводиться в матрицю відповідно з найближчими споживчими характеристиками. Навпроти свого номера в клітинці ставиться повна вартість створення системи з урахуванням усіх необхідних витрат та приведення всіх фінансових витрат до початкового моменту часу.

Поля матриці виглядають наступним чином:

1. Перерахування значень факторів споживчих переваг в стільникових системах зв'язку;
2. Пронумерований ряд вартісних виразів технічних реалізацій телекомунікаційних рішень мереж LTE;
3. Значення додаткового доходу від впровадження телекомунікаційного рішення з відповідними споживчими характеристиками.

Графічне подання матриці засноване на таких основних елементах:

- побудова тривимірної системи координат;
- дискретність значень;

– побудова четвертого виміру шляхом виділення дискретних елементів різними кольорами.

Реалізуючи ці постулати, отримуємо тривимірну систему координат, осями якої є:

- пропускна здатність;
- якість в каналі зв'язку;
- вартість системи зв'язку/дохід від експлуатації нового телекомунікаційного рішення.

Четвертий вимір – надійність телекомунікаційного рішення – буде реалізовуватися в системі координат шляхом внесення позначень всіх рішень з одним рівнем надійності одним кольором. Причому дохід від експлуатації при цьому рівні надійності також буде виділений цим же кольором. На графіку це може бути, зокрема, реалізовано у вигляді кольорових крапок з крупною точкою – доходом від експлуатації нового рішення.

Таким чином, алгоритм роботи методики (дискретний варіант) наступний:

4. На основі аналізу інформаційних потоків організації замовник телекомунікаційного рішення заносить у клітинку матриці вибору рішення, приведені до початкового моменту часу за методикою інвестиційного аналізу додаткові доходи, одержувані в результаті впровадження рішення з відповідними споживчими характеристиками, а також експлуатаційні платежі нинішньої системи, виключаються з витрат організації після впровадження нового рішення.

5. Вводяться вихідні дані про координати розташування базових станцій мереж LTE, їх необхідну кількість.

6. Згідно представленого алгоритму (рис. 1) відбувається оцінка зони радіо покриття мережі за технологією LTE.

7. Вибирається архітектура рішення побудови опорного сегмента мережі LTE (з урахуванням вимог до систем безпеки).

8. Розраховується ступінь шкідливості впливу електромагнітного випромінювання працюючої базової станції і в разі перевищення встановлених норм виключається з подальшого розгляду.

9. Розраховується надійність системи зв'язку на основі значень надійності роботи всіх її елементів.

10. Розраховується вартість кожної технічної реалізації будівництва системи зв'язку з відповідними компонентами та споживчими характеристиками.

11. Проводиться оцінка повної вартості будівництва мережі з урахуванням використання позикових коштів і приведенням до початкового

моменту часу результатів на основі методики інвестиційного аналізу.

12. Отримані значення відносин порівнюються зі значеннями у відповідній таблиці і заносяться в комірку з відповідними споживчими характеристиками матриці вибору рішення під номерами.

13. Значення повної вартості будівництва мережі кожної можливої технічної реалізації в кожному осередку матриці вибору рішення з відповідними споживчими характеристиками порівнюються з наведеним до початкового моменту часу додатковим доходом від використання рішення з відповідними осередку матриці споживчими характеристиками.

14. Вибирається мінімальне значення вартості технічної реалізації в осередку матриці з відповідними споживчими характеристиками.

15. Обчислюється значення ефекту і ефективності від реалізації кожного найкращого рішення в кожному осередку з відповідними споживчими характеристиками матриці вибору рішення.

16. З усіх осередків вибирається технічна реалізація з найбільшим ефектом/ефективністю (вибирається замовником рішення).

17. Конфігурація технічної реалізації виводиться замовнику телекомунікаційного рішення.

це, ведеться споживачем на підставі одного з критеріїв:

- максимізація загального економічного ефекту, одержуваного від впровадження нової телекомунікаційної системи або послуги,

- максимізація економічної ефективності від вкладення коштів у реалізацію проекту.

Показник економічного ефекту на всіх етапах реалізації системи визначається як перевищення вартісної оцінки сукупних витрат ресурсів за весь строк здійснення проекту. Відмінність систем зв'язку від багатьох інших видів вкладення засобів відрізняється тим, що зв'язок є інфраструктурною одиницею діяльності організації (за винятком самих підприємств зв'язку). Тому вкладення коштів в телекомунікації самі по собі не приносять великого доходу, однак ефект від впровадження нововведень проявляється в підвищенні ефективності технологічного процесу створення продукту або послуги, таким чином впливаючи на збільшення прибутковості всього підприємства в цілому.

Показник економічної ефективності проекту визначається як співвідношення сумарних доходів від реалізації проекту за вирахуванням загальних витрат за проектом в цілому до величини цих витрат. Цей показник також може повною мірою відображати реальну картину в організації тільки при обліку всіх додаткових доходів, одержуваних організацією від впровадження нової телекомунікаційної системи.

Саме з цих причин у пропонованій методиці не ведеться прямий розрахунок описаних показників на основі певного технічного проекту, а проводиться багатокритерійний вибір.

За загальним визнанням, основними критеріями вибору телекомунікаційного рішення в корпоративному середовищі і користувача середовищі є: пропускна здатність каналу зв'язку, надійність, якість в каналі зв'язку, можливість зв'язку в єдину мережу всі підрозділи, відсутність шкідливого впливу обладнання на співробітників, конфіденційність цілісність та доступність передаваних даних. Для визначення обґрунтованих потреб у модернізації обладнання зв'язку необхідно проводити аналіз інформаційних потоків організації.

Висновки. Таким чином, в роботі було запропоновано методику вибору проектного рішення для розгортання мережі LTE із урахуванням потреб захисту інформації. Користувачів в мережах нового покоління передусім цікавлять пропускна здатність каналу зв'язку, надійність, якість в каналі зв'язку та захищеність передаваних даних. На основі цих потреб було запропоновано

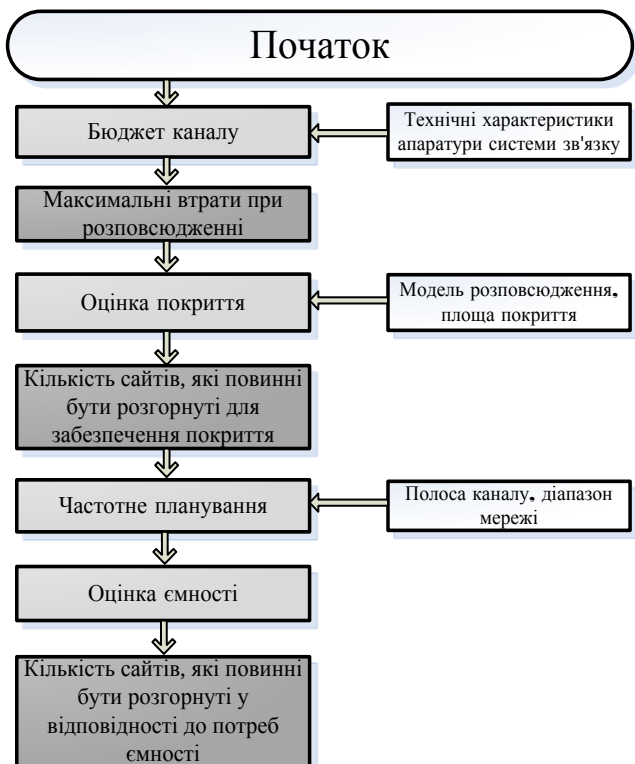


Рис.1 Алгоритм планування мережі LTE

Аналіз споживчих уподобань. Остаточний вибір телекомунікаційного рішення зі всього пропонованого спектру, як вже було згадано ви-

та обґрунтовано опис матриці вибору рішення, на базі якої в кінцевому результаті відбувається вибір проектного рішення, згідно із вимогами користувачів та потребами операторів зв'язку.

В подальших дослідженнях планується визначити найбільш затребувані послуги для користувачів, які можуть бути впроваджені в мережах LTE та оцінити економічний ефект від їх впровадження.

ЛІТЕРАТУРА

- [1]. Вишне夫斯基 В. М. Энциклопедия WiMAX: Путь к 4G / В. М. Вишне夫斯基, С. А. Портной, И. В. Шахнович – М.: Техносфера, 2009. – 472 с.
- [2]. Одарченко Р. С. Аналіз перспектив технології WiMAX в Україні / Р. С. Одарченко, Ю. О. Петрова // Політ-2011. Сучасні проблеми науки : міжнародна науково-практична конференція молодих учених і студентів, 7–9 квітня 2010 р. : тези доп. – К. : НАУ, 2011. – С. 29.
- [3]. Перспективи та рекомендації по впровадженню стільникового зв'язку 4-го покоління / В. В. Ткаченко, Р. С. Одарченко, В. С. Повхліб, Т. Р. Андрійченко // Проблеми навігації та управління рухом : Всеукраїнська науково-практична конференція молодих учених і студентів; м. Київ, 21–22 листопада 2011 р. : тези доповідей / редкол. : М. С. Кулик та ін. – К. : НАУ, 2011. – С. 122.
- [4]. Тихвинский В. О. Сети мобильной связи LTE: технологии и архитектура / В. О. Тихвинский, С. В. Терентьев, А. Б. Юрчук. – М.: Эко-Трендз, 2010. – 284 с.: ил.
- [5]. Ткаченко В. В. Вітчизняні перспективи розвитку технології LTE / В. В. Ткаченко, І. О. Дударчук, К. В. Дружиніна // Проблеми навігації та управління рухом : Всеукраїнська науково-практична конференція молодих учених і студентів; м. Київ, 23–24 листопада 2010 р. : тези доповідей / редкол. : М. С. Кулик та ін. – К. : НАУ, 2010. – С. 105.
- [6]. Ткаченко В. В. Методи прогнозування попиту на послуги мереж LTE / В. В. Ткаченко, Р. С. Одарченко, Ю. О. Петрова // Політ-2011. Сучасні проблеми науки : міжнародна науково-практична конференція молодих учених і студентів, 7–9 квітня 2010 р. : тези доп. – К. : НАУ, 2011. – С. 30.
- [7]. Конахович Г. Ф. Аналіз залежності кількості абонентів стільникових мереж від доходів населення / Г. Ф. Конахович, І. О. Козлюк, В. В. Ткаченко, Р. С. Одарченко // Наукоємні технології. – 2012. – №. 3 (15). – С. 48–51.
- [8]. Тихвинский В. О., Терентьев С. В. Управление и качество услуг в сетях GPRS/UMTS. – М.: Эко-Трендз, – 2007. – 400 с.

REFERENCES

- [1]. V. Vyshnevskyy, S. Portnoy, I. Shakhnovich, Encyclopedia WiMAX: Road to 4G, Moscow: Technosphere, 2009, 472 p.

- [2]. R. Odarchenko Analysis of the prospects for WiMAX technology in Ukraine Flight 2011. Challenges of Science: International Scientific and Practical Conference of Young Scientists and Students, April 7-9, 2010: Abstracts ext, K.: NAU, 2011, P. 29.
- [3]. V. Tkachenko, R. Odarchenko, V. Povhlib, T. Andriychenko Perspectives and recommendations on the introduction of cellular 4th Generation, Issues Navigation and Traffic Management, National Scientific Conference young scientists and students, Kyiv, November 21-22, 2011: abstractsredkol. MS Kulik et al., K.: NAU, 2011, P. 122.
- [4]. V. Tikhvinsky Sets mobylnoy connection LTE: Technology and Architecture / V. Tikhvinsky, S. Terentev, A. Yurchuk, Moscow: Eco-Trendz, 2010, 284 p.
- [5]. V. Tkachenko Domestic perspectives of technology LTE / V. Tkachenko, I. Dudarchuk, K. Druzhynina, Issues Navigation and Motion Control: National Scientific Conference of young scientists and students, Kyiv, 23-24 November 2010: abstracts/redkol: MS Kulik et al., K.: NAU, 2010, P 105.
- [6]. V. Tkachenko Methods of forecasting demand for network LTE / V. Tkachenko, R. Odarchenko, Y. Petrova, Flight 2011. Challenges of Science : International Scientific and Practical Conference of Young Scientists and Students, April 7-9, 2010: Abstracts ext, K.: NAU, 2011, P. 30.
- [7]. G. Konahovich Analysis of the number of subscribers of cellular networks on income / G. Konahovich, I. Kozlyuk, V. Tkachenko, R. Odarchenko, science-intensive technology, 2012, №. 3 (15), P. 48-51.
- [8]. V. Tikhvinsky, S. Terentev The quality of services and Management in setyah GPRS/UMTS, Moscow: Eco-Trendz, 2007, 400 p.

МЕТОДИКА ВЫБОРА ПРОЕКТНОГО РЕШЕНИЯ ДЛЯ РАЗВЕРТЫВАНИЯ ЗАЩИЩЕННОЙ СЕТИ LTE

Для поддержания высокоскоростных приложений, пользования новыми услугами, поддержания постоянного мобильного доступа к сети Интернет телекоммуникационным операторам необходимо разрабатывать планы по внедрению новейших технологий и обновление уже существующих предприятий связи с учетом общих тенденций научно - технического и инновационного развития. Большой спрос на рынке предоставления услуг связи компенсируется наличием еще больших объемов предложения. Часто заказчик телекоммуникационного решения из-за огромного количества предлагаемых ему самых разнообразных услуг по отличающимся на порядки ценам не может сам сделать правильный выбор. Именно основываясь на этом положении необходимо предложить методику, цель которой будет заключаться в согласовании потребительских запросов к системе связи, основанной на передаче пакетных данных через каналы современных сотовых систем связи четвертого поколения. В работе предложено пошаговую методику вы-

бора проектного рішення для розгортання мережі LTE з урахуванням потреб захисту інформації. Розглянуті основні вимоги користувачів до мереж нового покоління, проаналізовані, як вони впливають на вибір обладнання для побудови мережі. Представлено і обґрунтовано опис матриці вибору рішення, на основі якої в кінцевому підсумку відбувається вибір проектного рішення, згідно з вимогами користувачів.

Ключевые слова: сотовые сети связи, базовая станция, LTE, матрица выбора решения, проект, требования пользователей, архитектура решения.

METHODOLOGY FOR THE SELECTION OF DESIGN SOLUTIONS FOR THE DEPLOYMENT OF SECURE LTE NETWORK

To maintain high-speed applications, the use of new services, support continuous mobile access to the Internet, telecom operators need to develop plans for the implementation of new technologies and update existing business communications with the general trend of scientific and technological innovation and development. Strong demand in the market of communication services is offset by the presence of even greater demand. Often the customer telecommunication solutions to the huge amount offered him a variety of services for which prices vary by orders of magnitude is unable to make the right choice. It is based on this position you must offer a technique whose purpose will be to harmonize consumer requests to the communication system based on packet data through the channels of modern mobile communication systems fourth generation. The paper presents a step by step methodology for selecting design solution for LTE network deployment, taking into account the need to protect information. The basic user requirements to next generation networks and analyzes how they affect the selection of equipment for the construction of the network. A reasonable description and selection decision matrix, based on which the final result is the choice of design solution, according to the requirements of users.

Keywords: cellular networks, base station, LTE, choice of matrix solution, project, user requirements, architecture decisions.

Одарченко Роман Сергійович, кандидат технічних наук, доцент кафедри телекомунікаційних систем інституту аеронавігації Національного авіаційного університету.

E-mail: odarchenko.r.s@mail.ru

Одарченко Роман Сергеевич, кандидат технических наук, доцент кафедры телекоммуникационных систем института аэронавигации Национального авиационного университета.

Roman Odarchenko, Ph.D., Associate Professor of Telecommunication Systems department of Institute of Air Navigation of the National Aviation University.

Ткаченко Вадим Валерійович, аспірант кафедри телекомунікаційних систем інституту аеронавігації Національного авіаційного університету.

E-mail: vtkauchenko@mts.com.ua

Ткаченко Вадим Валерьевич, аспирант кафедры телекоммуникационных систем института аэронавигации Национального авиационного университета

Vadim Tkachenko, a graduate student of Telecommunication Systems department of Institute of Air Navigation of the National Aviation University.

Конахович Георгій Філімонович, доктор технічних наук, професор, завідувач кафедри телекомунікаційних систем інституту аеронавігації Національного авіаційного університету.

E-mail: tks@nau.edu.ua

Конахович Георгий Филимонович, доктор технических наук, профессор, заведующий кафедрой телекоммуникационных систем института аэронавигации Национального авиационного университета.

George Konahovich, prof., Head of Telecommunication Systems department of Institute of Air Navigation of the National Aviation University.

УДК 681.3.067

АЛГЕБРАЇЧНІ МОДЕЛІ АСИМЕТРИЧНИХ КРИПТОГРАФІЧНИХ СИСТЕМ

Юрій Яремчук

Моделювання криптографічних методів на рівні алгебраїчних структур дає можливість глибше зрозуміти принципи їх побудови, особливості функціонування, дослідити їх властивості. Існуючи на сьогодні алгебраїчні моделі асиметричних криптографічних систем не забезпечують в повній мірі можливості їх використання. В роботі розглянуто алгебраїчну модель відкритого розподілу секретних ключів, а також запропоновано алгебраїчні моделі асиметричного шифрування, автентифікації сторін взаємодії та цифрового підписування як багатоосновні універсальні алгебри. На основі представлених алгебр розглянуто моделі існуючих криптосистем, а також запропоновано моделі розподілу секретних