УДК 681.324

НЕСТЕРЕНКО О.В. Міжнародний науковий центр
технології програмування “Технософт”

ЗАСАДИ ДЕРЖАВНОГО РЕГУЛЮВАННЯ ФОРМУВАННЯ СИСТЕМИ ЕЛЕКТРОННОГО УРЯДУ

Анотація. *Розглядаються підходи до розв’язання проблем державного регулювання створення та забезпечення взаємодії автоматизованих інформаційно-аналітичних систем органів влади як базових елементів системи електронного уряду з урахуванням питань забезпечення інформаційної безпеки.*

Ключові слова: *електронний уряд, державне регулювання, автоматизована система, взаємодія, інформаційна безпека.*

Аннотация. *Рассматриваются подходы к решению проблем государственного регулирования создания и обеспечения взаимодействия автоматизированных информационно-аналитических систем органов власти как базовых элементов системы электронного правительства с учетом обеспечения информационной безопасности.*

Ключевые слова: *электронное правительство, государственное регулирование, автоматизированная система, взаимодействие, информационная безопасность.*

Summary. *Approaches to decision of problems of government control of creation and interoperation automation information-analytical systems of government authorities as base elements of the system of electronic government taking into providing of information security are analyzed.*

Keywords: *electronic government, government control, automation system, interoperation, information security.*

Постановка проблеми. Стрімкий розвиток технологій надає небачені донині можливості для забезпечення взаємодії між комп’ютерами, мобільними пристроями та автоматизованими системами і тим самим сприяє швидкому розвитку складових інформаційного суспільства, зокрема системи електронного уряду, яку, зважаючи на виняткову роль державних органів у забезпеченні життєдіяльності країни, можна вважати “складовою № 1”. Разом з тим, розвій цих процесів веде й до швидкого збільшення загроз інформаційній безпеці взаємодіючих об’єктів.

Крім того, недостатність інформаційного забезпечення органів влади, відсутність регламентованих механізмів опрацювання інформаційних ресурсів та документів, що є наслідком відсутності в органах влади автоматизованих систем або неефективності їх створення та використання, ведуть до зниження обґрунтованості рішень та несвоєчасності їх прийняття, що, враховуючи їх державне значення, загрожує безпеці країни.

При цьому швидке утягування у процеси комп’ютеризованого обміну інформацією різних верств населення, підприємств та організацій, а також органів влади суттєво випереджає забезпечення цих процесів правовим регулюванням, що, як наслідок, зі свого боку, й ще у чималому ступені сприяє зниженню рівня інформаційної безпеки. Тому на сучасному етапі, крім інформаційних технологій, до тріади наріжних каменів інформатизації суспільства слід віднести правову підтримку та забезпечення інформаційної безпеки (Рис. 1).

Інформаційні процеси в системі електронного уряду значною мірою є процесами передачі та обробки електронних документів, тому важливим питанням є забезпечення відповідних технологій та правового регулювання – принципів, правил, заходів для

найефективнішого сполучення органів влади та їх підрозділів між собою, оптимізації їх взаємодії в часі для досягнення визначених цілей (наприклад, запобігання порушенням регламенту опрацювання документів) [1].

Рис. 1. Триада наріжних каменів інформатизації суспільства

У якості бази вирішення вказаних проблем на державному рівні у багатьох країнах, зокрема європейських, розроблені та впроваджені зведення вимог щодо сумісності державних систем, так звані e-GIF (e-Government Interoperability Framework). Ці документи мають обов’язковий статус для всіх органів державної влади, розробляються у відкритому порядку із залученням зацікавлених представників громадськості [2]. У тому або іншому вигляді в більшості таких документів, які формують регламент державного регулювання інформатизації, як правило, основний акцент робиться на описі міжсистемної взаємодії (інтероперабельності) як найбільш важливому елементі державної інформатизації, необхідному для забезпечення міжвідомчої взаємодії й взаємодії із громадянами.

В Україні, як і у більшості країн, що розвиваються, подібних документів та орієнтації на такі схеми інформатизації, на жаль, ще немає. Практично відсутні й відповідні дослідження та публікації, в яких започатковано розв’язання вказаної проблеми. Окремі питання лише порушені російськими вченими у [3] та в деяких інших статтях цих авторів, оглянуті у збірці, виданій Академією народного господарства при Уряді Російської Федерації [4], а також розглянуті в деяких вітчизняних публікаціях [5 – 7]. Це, безумовно, стримує не лише хід інформатизації державних структур, а й взагалі формування інформаційного суспільства в нашій країні.

Таким чином, для забезпечення ефективної діяльності органів влади і досягнення практичних результатів щодо надання ними державних (адміністративних) послуг в електронному вигляді необхідне вироблення відповідної регуляторної політики на основі нормативно-правових актів, зокрема стосовно адаптації автоматизованих інформаційних систем органів влади з тим, що б вони могли “прозоро” взаємодіяти з ресурсами і сервісами, що можуть надаватись.

Метою статті є спроба визначити основні підходи до формування засад державного регулювання створення та сумісності цих систем як базових елементів електронного уряду.

Виклад основних положень. Основою формування в країні системи електронного уряду, що має бути головним із завдань і пріоритетів формування “електронної країни”, є створення електронної інфраструктури в державі [8]. При цьому побудова кожної зі складових цієї інфраструктури має відбуватись з урахуванням особливостей побудови інфраструктури забезпечення інформаційної безпеки (рис. 2). Водночас, слід зазначити, що базовими елементами електронної інфраструктури мають стати відповідні автоматизовані інформаційно-аналітичні системи (АІАС) органів влади, які повинні розроблятися виходячи з вимог вичерпної інформаційної підтримки аналітичної діяльності та прийняття рішень в державних структурах, активізації інформаційного обміну з населенням, забезпечення їх інтероперабельності у гетерогенному середовищі, в якому відбувається обмін інформацією між різними АІАС, системами підприємств та організацій, а також комп’ютерами та мобільними інтелектуальними пристроями громадян [5; 6].

Таким чином, враховуючи наведені вимоги, АІАС органів державної влади уявляються достатньо складними інформаційними системами, а їх створення має розглядатись як одне з пріоритетних і важливих завдань держави.

Відповідальність за процеси інформатизації, зокрема органів влади, в передових країнах, зазвичай, покладається на низку ключових міністерств, особливо в умовах, якщо інформатизація у відповідній країні ведеться за так званою стандартизованою схемою. Під такою схемою розуміється ситуація, коли більшість установ державного сектору оснащені сумісними і взаємозамінними програмно-апаратними засобами, електронні профілі користувачів-держслужбовців є незалежними з точки зору доступу з будь-якого пристрою кінцевого користувача, а аналітичні і контрольні підрозділи уряду мають структурований доступ до накопичуваної у відповідних базах органів влади інформації, включаючи елементи планування і контролю виконання розпоряджень.

Рис. 2. Інфраструктура інформаційного суспільства

В нашій країні, як свідчить досвід, ще не склалася досить висока культура проектування і розробки АІАС органів влади [5]. В цих умовах вирішити базові завдання по забезпеченню ефективності державних систем та їх сумісності може забезпечити лише запровадження державного регулювання на основі певної нормативної бази. Основним документом або комплексом документів має стати національне зведення приписів та правил створення державних автоматизованих систем (введемо для його позначення абревіатуру “НПДАС”).

Вивчення світового досвіду показує, що державна політика в цій сфері має базуватись на врахуванні архітектурних питань і вимог сумісності систем. Архітектурний підхід, більш притаманний країнам американського континенту, розглядає моделі архітектури підприємства (Enterprise Architecture, EA) та архітектури надання послуг (Service-Oriented Architecture, SOA). Європейський підхід більш пов’язаний з вимогами сумісництва систем (Government Interoperability Framework, GIF). Узагальнюючи цей досвід, можна запропонувати для НПДАС взаємопов’язану структуру документа, що враховує ці три моделі (Рис. 3).

Рис. 3. Модель НПДАС

“Архітектура органу влади” (Government Architecture, GA), спираючись на досвід розробок EA, дозволяє при проектуванні АІАС чітко співвіднести можливості інформаційних технологій функціям органу влади і процесам прийняття рішень в нових умовах діяльності та, за необхідності, провести реорганізацію органу влади (“реінжиніринг бізнес-процесів”).

Вказані процеси можуть протікати послідовно й паралельно, бути залежними або незалежними один від одного, рівноправними або привілейованими, відкритими або захищеними, виконуватися синхронно або асинхронно тощо, тобто протікання та взаємодії процесів прийняття рішень в органах влади є багатоаспектними. Моделювання таких взаємодіючих процесів пов’язане з багатьма труднощами, адже вони визначаються не лише названими особливостями виконання процесів, а й типами локальних і розподілених об’єктів, на які ці процеси спрямовані [1].

Тому в цьому розділі документа має бути наведено не тільки опис технологічних підходів, а й порядок проектування адміністративних процесів держави, механізми контролю й фінансового заохочення. Він має містити й набір моделей, присвячених різним аспектам проектування й функціонування інформаційних систем, обробки електронних документів в органах влади.

Підхід “Архітектура АІАС” має на увазі визначення можливостей використання АІАС, її сумісності з іншими системами, використання інформаційних ресурсів з погляду на кінцеву мету – надання електронних адміністративних послуг громадянам та підприємствам. Цей підхід визначає функціональну архітектуру, що встановлює правила класифікації специфікацій і функцій, для виконання яких вони призначені. Каталог базових специфікацій, що є однією з основних частин майже всіх систем регулювання, призначений для визначення умов використання стандартів, а також їх життєвого циклу, що відповідає темпам розвитку інформаційних технологій.

Слід зазначити, що відповідним чином увага має приділятися й використанню у державних установах програмного забезпечення та його міграції на вільне/відкрите ПЗ, яке зараз розглядається як повноцінна альтернатива пропрієтарним програмам і все частіше стає основною частиною державної політики в сфері створення державних інформаційних систем, особливо в європейських державах [9].

Розділ “Правила сумісності АІАС” цілком має бути присвяченим аспектам міжсистемної взаємодії, яких слід виділити три: технічна, семантична та організаційна сумісність (Рис. 4). При цьому базою цих аспектів мають бути так звані “відкриті стандарти”, тобто такі, що розробляються незалежними спеціалізованими організаціями у відкритому процесі, а використання цих стандартів не потребує ліцензійних відрахувань.

Рис. 4. Аспекти міжсистемної взаємодії

Технічна сумісність (або технологічна) передбачає визначення інтерфейсів взаємодії, єдиних форматів даних та загальні вимоги до метаданих. Семантична сумісність (іноді має назву інформаційної) пов’язана з однозначною інтерпретацією і обробкою даних як системами, так і користувачами. Нарешті, одноманітність процесів обробки даних та електронних документів в органах влади визначає організаційна сумісність.

Розглянемо деякі приклади можливого представлення положень НПДАС. Одним з них може бути вирішення проблеми інтероперабельності шляхом напрацювання рекомендацій з програмної організації підтримки інформаційно-аналітичної діяльності (так званих компонентів бізнес-логіки) та доступу до даних. Традиційно у методах автоматизації управлінської діяльності є “клієнтська” орієнтація бізнес-процесів, коли дані зберігаються на сервері, а на комп’ютері користувача встановлюється програма-клієнт, що отримує дані з сервера, опрацьовує їх та подає результати користувачу

(“товстий клієнт”). Таке рішення, окрім проблем з необхідністю оновлень клієнтського ПЗ та підтримки, потребує врахування вимог до форматів даних. Тому традиційна схема безпосереднього доступу компонентів до даних вважається недосконалою та пов’язаною з проблемами уніфікації програмного забезпечення та структур даних.

Сучасна схема, що рекомендується, передбачає створення ПЗ проміжного шару (*middleware*), що уможливлює незалежність бізнес-компонентів від компонентів доступу до даних, а також застосування веб-інтерфейсу (“тонкий клієнт”). Засоби проміжного шару, за рекомендаціями Євросоюзу, для АІАС різних органів влади мають бути основною ланкою їх взаємодії, що забезпечують мережну підтримку, захищену передачу даних та різні механізми доступу залежноі від рівня користувача е-уряду (Рис. 5).

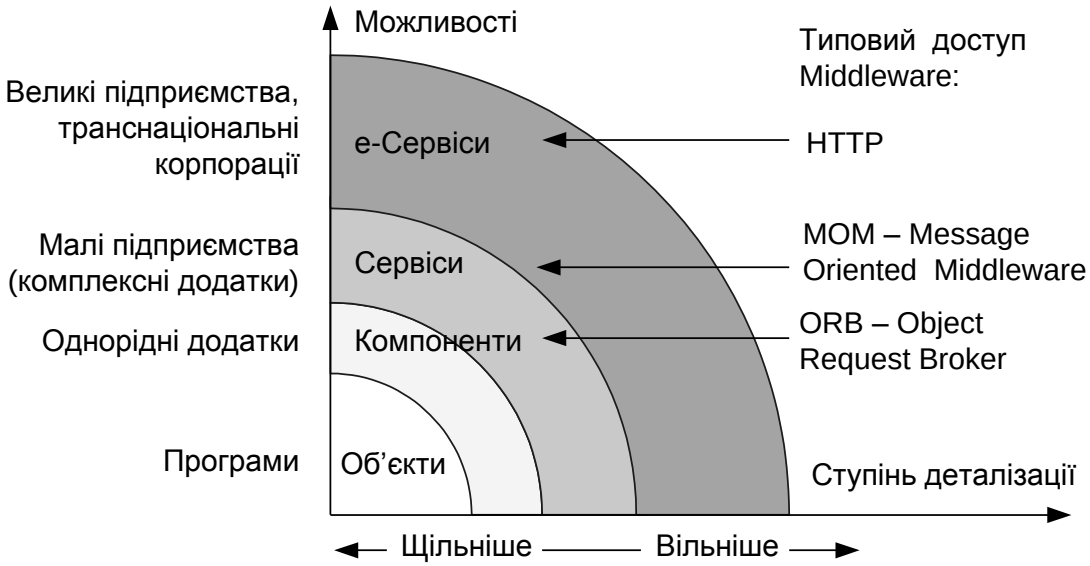

Рис. 5. Механізми доступу до системи електронного уряду

При цьому для взаємодії з громадянами доцільне використання єдиного урядового порталу доступу, а взаємодія з підприємствами передбачає безпосередній доступ їх бізнес-додатків до сервісів інтегрованої системи органів влади.

Ще одним прикладом вирішення проблем інтероперабільності є забезпечення інформаційної безпеки та захисту інформації в автоматизованих системах. Враховуючи, що схема обробки інформації в АІАС має бути зорієнтованою на Інтранет/Інтернет технології та використання портальних технологій, з точки зору безпеки важливе значення має побудова систем з захищеним поділом на дві зони – так званого переднього краю (*Front-end*), що підтримує взаємодію з зовнішніми користувачами через веб-портал, та заднього (*Back-end*), зорієнтованого на обслуговування працівників органу влади.

У цих умовах створення та актуалізація комплексної системи безпеки інформації має забезпечуватись реалізацією багатостадійного процесу інтеграції окремих складових АІАС до єдиної системи зі створенням засобів захисту телекомунікаційного середовища з дотриманням існуючих міжнародних рекомендацій щодо організації не лише безпосередньо засобів безпеки, а й засобів Front-end та Back-end [10 – 12] (Рис. 6).

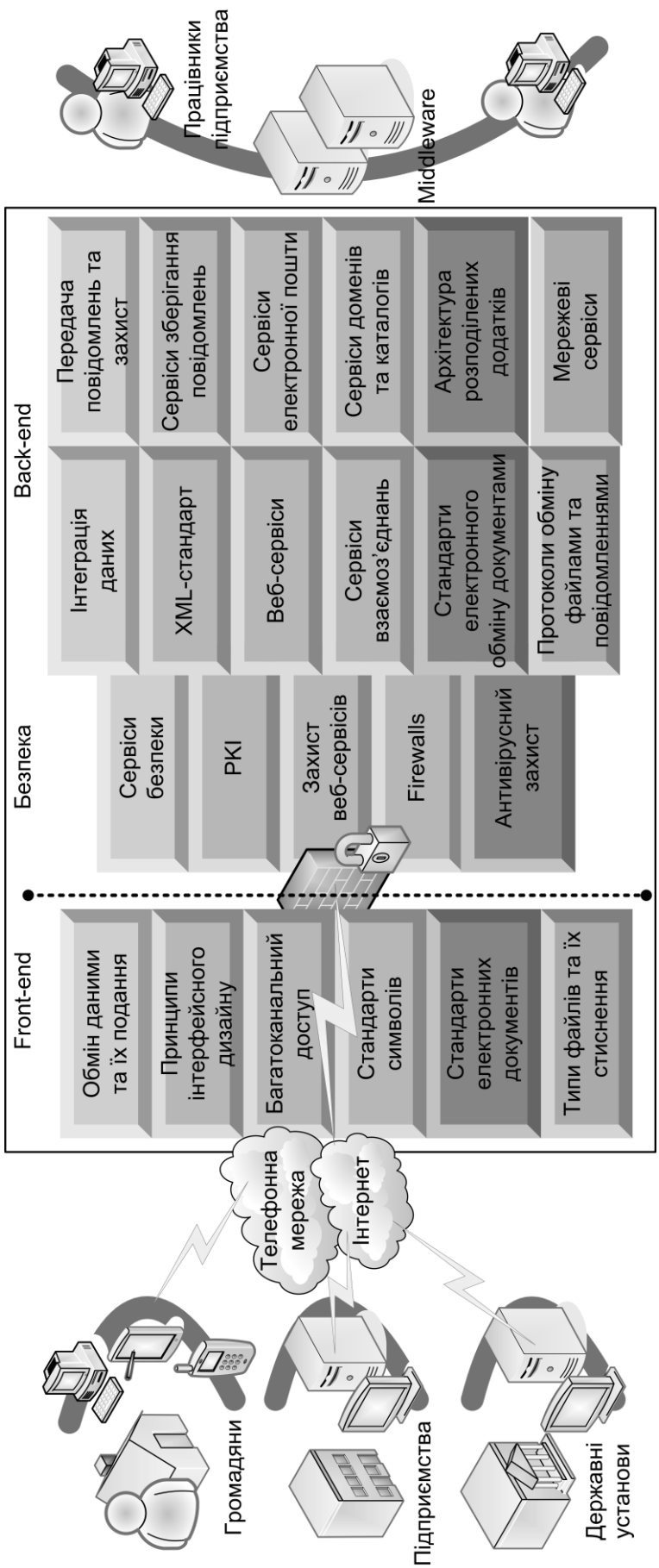

Рис. 6. Імплементація міжнародних рекомендацій щодо створення комплексної системи інформаційної безпеки в АІАС

Отже, ця концепція безпеки електронної інфраструктури органів влади передбачає реалізацію технологій захисту інформації на всіх рівнях інформаційної системи та забезпечує:

1) автентифікацію суб’єктів;

2) контроль доступу до об’єктів;

3) підтвердження цілісності документів із застосуванням електронного цифрового підпису (ЕЦП);

4) захист інформації за допомогою засобів шифрування.

Реалізація цих вимог значною мірою пов’язана із застосуванням засобів інфраструктури відкритих ключів (*PKI*) ЕЦП, що забезпечує захист персональної інформації, захист конфіденційної та таємної інформації, гарантії конфіденційності й ідентифікації, цілісності даних і автентичності.

Висновки та пропозиції.

Стрімкий розвиток інформаційних технологій, тенденції відкритості діяльності державних установ та збільшення її ефективності вимагають створення в органах влади автоматизованих інформаційно-аналітичних систем та вирішення проблем їх інтероперабельності. Тому невідкладним завданням для органів влади, що є відповідальними за вказані процеси, вбачається започаткування розгортання робіт у напрямі підготовки проекту національного зведення приписів та правил створення державних автоматизованих систем, проведення його всебічного обговорення, імплементації та забезпечення процедур впровадження.

Підхід до створення такого документа має базуватись на моделях архітектури органу влади, архітектури надання послуг та сумісності державних систем. Такий підхід має дозволити державній владі швидко розгорнути АІАС та модифіковувати їх у відповідності до змін у структурі органів державної влади та інших обставин, а також створити умови для суттєвого підвищення рівня інформаційної безпеки. Водночас слід мати на увазі, що розробка такого документа та його впровадження потребують значних політичних зусиль, а також налагодження координації зусиль державних осіб, науковців та технічних фахівців.

На завершення слід зазначити, що аналіз підходів і методів вирішення проблеми інтероперабельності АІАС органів влади приводить до висновку про необхідність зміни парадигми вирішення проблем взаємодії систем у масштабах країни з переходом від транспарентності обміну повідомленнями через забезпечення семантичної інтероперабельності до головного – створення цілісної моделі інформаційно-аналітичного середовища управління, як державного, так і господарського. Досягнення цієї мети дозволить створити модель знань не лише в окремому органі влади чи на підприємстві, а й модель “загальнонаціональної інтелектуальної системи” для колективного – у масштабах країни – розв’язання задач і обґрунтування прийняття рішень.

Використана література

1. Нестеренко О.В. Моделі інформаційного навантаження при опрацюванні документів в автоматизованих інформаційно-аналітичних системах органів державної влади / О.В. Нестеренко, І.Є. Нетесін // Реєстрація, зберігання і обробка даних. – 2011. – Т. 13. – № 1. – С. 39 – 55.

2. e-Government Interoperability Framework / Version 6.1.18. – March 2005. – Cabinet Office e-Government Unit, London. – 2005. – 34 p. – Режим доступу : http://www.govtalk.gov.uk/schemas standards/egif.asp

3. Батоврин В.К. Обеспечение интероперабельности – основная тенденция в развитии открытых систем / В.К. Батоврин, Ю.В. Гуляев, А.Я. Олейников // Информационные технологии и вычислительные системы. – 2009. – № 5. – С. 7 – 15.

4.Интероперабельность информационных систем : сборник материалов. – М. : INFO-FOSS.RU, 2008. – 128 с.

5. Нестеренко О.В. Безпека інформаційного простору державної влади : технологічні основи / О.В. Нестеренко. – К. : Наукова думка, 2009. – 352 с.

6. Нестеренко О.В. Організаційно-технологічні підходи до забезпечення інформаційної безпеки державної влади / О.В. Нестеренко // Національна безпека: український вимір : щокв. наук. зб. / Рада нац. безпеки і оборони України, Ін-т пробл. нац. безпеки ; редкол. Горбулін В.П. (голов. ред.) та ін. – К., 2009. – Вип. 4 (23). – С. 41 – 50.

7. Нестеренко О.В. Інтероперабельність автоматизованих інформаційно-аналітичних систем органів державної влади / О.В. Нестеренко : *матеріали Міжнародного наукового конгресу з розвитку інформаційно-комунікаційних технологій та розбудови інформаційного суспільства в Україні*, (Київ, 17 – 18 листопада 2011 р.). – К.: Український науковий центр розвитку інформаційних технологій, 2011. – С. 79 – 80.

8. Нестеренко О.В. Проблеми формування національної інформаційної інфраструктури та забезпечення її безпеки / О.В. Нестеренко // Реєстрація, зберігання і обробка даних. – 2010. – Т. 12. – № 2. – С. 216 – 226.

9. Будько М.М. Стратегія застосування відкритих програм для забезпечення інформаційної безпеки держави / М.М. Будько, О.В. Нестеренко, І.Є. Нетесін // Національна безпека: український вимір: щокв. наук. зб. / Рада нац. безпеки і оборони України, Ін-т пробл. нац. безпеки ; редкол. Горбулін В.П. (голов. ред.) та ін. – К., 2009. – Вип. 6 (25). – С. 72 – 81.

10. Guide for Assessing the Security Controls in Federal Information Systems / NIST Special Publication 800-53A. – National Institute of Standards and Technology, Gaithersburg, July 2008. – 381 p.

11. European interoperability framework for pan-european egovernment services / Luxembourg: Office for Official Publications of the European Communities, 2004. – 26 p. – Режим доступу : http://europa.eu.int/idabc

12. Architecture guidelines For Trans-European Telematics Networks for Administrations Version 7.1 Enterprise DG Brussels, September 2004. – 39 p.

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~