

ЗАХИЩЕНИЙ КОНСОЛІДОВАНИЙ ІНФОРМАЦІЙНИЙ РЕСУРС ЗАСОБІВ ЕЛЕКТРОННОГО УРЯДУВАННЯ

Вінницький національний технічний університет

Анотація

Окреслено проблеми захисту інформації у процесах електронного врядування як на адміністративному, програмному, так і процедурному рівнях. Доведено ефективність їх розв'язку шляхом створення відповідного захищеного консолідованого інформаційного ресурсу. Визначено етапи розроблення такого ресурсу та описано основні сутності його бази даних, які мають бути враховані. Даний консолідований інформаційний ресурс дозволить підвищити ефективність діяльності органів публічної влади, забезпечить зростання їх відкритості та прозорості, завдяки використанню цілісної консолідованої інформації для прийняття управлінських рішень.

Ключові слова: захищений консолідований інформаційний ресурс, електронне урядування, консолідована інформація.

Abstract

The problems of information security in e-governance processes at the administrative, program and procedural levels are identified. Their effectiveness has been proven by creating an appropriate secure consolidated information resource. The stages of development of such a resource are defined and the main essence of its database which should be considered are described. This consolidated information resource will increase the efficiency of public authorities, increase their openness and transparency by utilizing coherent consolidated information for making decisions.

Keywords: secure consolidated information resource, e-governance, consolidated information.

Вступ

Стрімкий розвиток інформаційних технологій та їх широке застосування у різних галузях діяльності суспільства спричинив появу нової форми організації публічного управління – електронного урядування, яка сприяє підвищенню ефективності, відкритості та прозорості діяльності органів публічної влади, оптимізації процесу надання публічних послуг населенню, забезпеченню участі громадян у публічному управлінні. На даний час, як свідчить зарубіжний досвід, розвиток електронного урядування є домінантним важелем успішності реформування та підвищення конкурентоспроможності країни. Досягнення необхідного рівня ефективності та результативності галузі публічного управління в сучасних умовах неможливе без широкого використання сучасних інформаційно-комунікаційних технологій. Адже саме інструменти електронного урядування здатні забезпечити значне покращення якості обслуговування фізичних і юридичних осіб та підвищення відкритості, прозорості і ефективності діяльності публічної влади, до якої належать органи державної влади та місцевого самоврядування [1].

Разом із тим, домінантною проблемою формування ефективних засад публічного управління в Україні є потреба безпечного його функціонування як на рівні адміністративному, так і на програмному і процедурному. Досконалий розвиток цих трьох рівнів публічного управління можливий за умов чіткого визначення основних понять, сутності та завдань захисту інформації, концепції захисту інформації в Україні, аналізу основних загроз інформаційній безпеці у процесах публічного управління та вивчення основних методів протидії їм, що надає можливість використовувати отримані знання та навички на практиці [2-11].

Отже, вивчення питань захисту інформації у процесах електронного врядування є надзвичайно актуальним. Тому дане дослідження присвячене створенню захищеного консолідованого інформаційного ресурсу засобів електронного урядування, який би уможливив покращення діяльності органів публічної влади, отримання консолідованої інформації для прийняття дієвих управлінських рішень.

Результати дослідження

Проблемні питання сьогодення у сфері захисту інформації у процесах публічного управління потребують розв'язання як на теренах України, так і в контексті його узгодження з інформаційним прос-

тором світової спільноти. Переведення своєї діяльності органами електронного урядування у цифровий стан створює нові канали взаємодії з користувачами, проте породжує постійні мутації кіберзагроз і появу нових ризиків, а, отже, і потребу вирішення нових питань у системі ефективного публічного адміністрування.

Системи електронного урядування працюють на основі інформаційних систем, що побудовані за принципами корпоративних комп'ютерних мережах, що і зумовлює спадковість проблем, характерних для корпоративних структур. Вони впливають як на фахівців у напрямку технічного обслуговування у сфері публічного управління, так і відповідних служб інформаційної безпеки.

Розглянемо базові аспекти, що спричиняють виникнення таких проблем [3]:

1. Складність і різноманітність програмного та апаратного забезпечення, що використовується в системах електронного урядування, які для реалізації важливих завдань використовують різні операційні системи. Робочі місця публічних службовців найчастіше оснащені операційною системою Windows, разом із тим, оброблення інформації в системах електронного документообігу та важливі інформаційні ресурси зберігаються в базах даних операційних середовищ Linux, FreeBSD, Solaris.

Публічні службовці використовують такі портативні мобільні пристрої (планшети, смартфони), які працюють у середовищах Android та iOS, що ускладнює технічне обслуговування (управління конфігураціями і оновленнями програмних засобів) та проведення стандартних, базових заходів у напрямку інформаційної безпеки.

2. Велика кількість вузлів у системах електронного урядування. Велика кількість вузлів, об'єднаних до корпоративних мереж системи електронного урядування, обробляє важливу інформацію, проте їх розгалуженість і віддаленість (різні міста, регіони або країни), а також відсутність часу на контроль необхідних налаштувань програмних засобів, не дозволяє технічному персоналу своєчасно контролювати діяльність і безпеку користувачів.

3. Зовнішній доступ до системи електронного урядування є надзвичайно важливою проблемою, що виникає під час її експлуатації, оскільки підключення зовнішніх користувачів (підприємств, організацій, окремих громадян) до відкритих сервісів та надання прав персоналу органу публічного управління щодо віддаленої роботи з внутрішніми інформаційними ресурсами призводить до збільшення загальної кількості небезпек, що постійно з'являються у корпоративній мережі. Такі «слабкі місця» програмного забезпечення процесів електронного урядування уможливають несанкціонований доступ до інформаційних ресурсів, що і пояснює необхідність застосування різних механізмів і засобів створення безпеки, налаштування яких залежить від технології інформаційного оброблення, яка застосована у системах публічного адміністрування.

4. Функціонування груп технічного обслуговування та інформаційної безпеки. У процесах електронного урядування група технічного обслуговування переважно вирішує питання системного і мережевого адміністрування. Фахівці з інформаційної безпеки займаються питаннями, пов'язаними з інформаційною безпекою на усіх рівнях, зокрема адміністративному, організаційному, технічному. Це спричиняє проблему чіткого розмежування функціональних обов'язків персоналу цих двох груп. Наприклад, обслуговування віддаленого доступу користувачів до інформаційних ресурсів системи електронного урядування; робота з основними службами і сервісами корпоративної мережі: DNS, електронна пошта; прикладні системи; електронний документообіг тощо.

Використання інструментів електронного урядування зумовлює появу значної кількості інформації та даних, які здебільшого різняться за форматом, сферою діяльності, джерелами та системами, використаними засобами електронного урядування тощо. Оскільки, зазначена інформація є важливою для діяльності органів публічної влади, для успішного вироблення та прийняття на її основі управлінських рішень, то постає проблема в її консолідації, а у зв'язку з тим, що дана інформація може мати вплив на функціонування держави в цілому, то виникає ще один аспект проблеми захисту даної інформації. Таким чином, під час створення та використання системи електронного урядування необхідним є комплексне вирішення складних проблем щодо її технічного обслуговування та інформаційної безпеки шляхом розроблення відповідного захищеного консолідованого інформаційного ресурсу.

Враховуючи те, що консолідована інформація – це одержані з кількох джерел та системно інтегровані різнотипні інформаційні ресурси (знання), які в сукупності наділені ознаками повноти, цілісності, несуперечності та складають адекватну інформаційну модель проблемної області з метою її опрацювання та ефективного використання в процесах підтримки прийняття рішень, то процес консолідації полягає саме в об'єднанні, інтеграції різнотипної інформації. Це вимагає розроблення меха-

нізму захисту під час створення консолідованого інформаційного ресурсу засобів електронного урядування на основі бази даних різних інформаційних ресурсів засобів електронного урядування, яка буде зберігати та обробляти інформацію з даних ресурсів.

Розроблення захищеного консолідованого інформаційного ресурсу зумовлює виконання таких етапів [9]:

- 1) проектування бази даних (БД) за методом «сутність–зв’язок»;
- 2) розроблення нормалізованої БД консолідованого інформаційного ресурсу;
- 3) формування звітів для відображення консолідованих даних;
- 4) захист інформації у БД створеного консолідованого ресурсу.

Розглянемо процес проектування бази даних за методом «сутність–зв’язок». Одним із базових етапів створення консолідованого інформаційного ресурсу є розроблення структури моделей даних. Створення моделей даних – це визначення сутностей, атрибутів та їх зв’язків. Потрібно визначити, яка інформація стане зберігатися в певній сутності або атрибуті. Сутність можна задати як об’єкт, концепцію або подію, інформацію про яку необхідно зберегти. Об’єкти повинні мати назви з точним смисловим значенням, називатися іменником в однині [12].

Під час розроблення бази даних необхідно орієнтуватися на кінцевого користувача, аналітика, який буде приймати рішення на основі поданої інформації. Це дозволяє ще на етапі розроблення бази даних обрати необхідні дані для повного відображення потрібної інформації [13].

Проектування за методом «сутність–зв’язок» виконується у такій послідовності, як визначити: сутності, зв’язки, атрибути, ключі сутностей, ступені зв’язку, класи належності.

Отже, автори пропонують базу даних такого консолідованого ресурсу представляти у вигляді ER-моделі, яка дозволяє описувати концептуальні схеми предметної області за допомогою узагальнених конструкцій-блоків. Вона уможливило виділення ключових сутностей і чітке окреслення зв’язків, які можуть встановлюватися між цими сутностями.

Визначимо такі основні сутності бази даних, які мають бути враховані під час побудови консолідованого інформаційного ресурсу засобів електронного урядування:

- орган публічної влади;
- відділи органу публічної влади;
- публічні послуги;
- звернення;
- запити;
- публічні обговорення;
- публічне голосування.

Наступним етапом є розроблення нормалізованої БД консолідованого інформаційного ресурсу. Для систематизації отриманої інформації та детального аналізу галузі авторами дослідження було розроблено базу даних засобами СУБД MS SQL та JavaScript. Було обрано для роботи мову Java, фреймворки Spring, Hibernate та MySQL. Hibernate дозволяє автоматичне створення таблиць баз даних на основі класів Java [9]. Кожен клас, що має зберігатися у базі даних, супроводжується спеціальними анотаціями, які визначають правила збереження класів у таблиці БД та задає зв’язки між ними. Завдяки використанню цього фреймворка необхідність ручного налаштування бази даних зводиться до мінімуму [14]. Для перегляду автоматично створеної структури БД було використано MySQL Workbench.

Захист інформації у базі даних створеного консолідованого ресурсу відбувається за рахунок застосування MS SQL, що є сервером високого класу, який забезпечує управління розробленою БД, її безпеку і стабільність роботи та гарантує найвищий рівень захисту даних. Крім того, для захисту особистих даних користувача використовується SSL сертифікат – криптографічний протокол, що встановлює безпечне з’єднання клієнта і сервера [15, 16]. Протокол створює конфіденційний обмін даними між клієнтом і сервером, що використовують протокол TCP/IP, а для шифрування авторами роботи використовується асиметричний алгоритм з відкритим ключем.

Висновки

Окреслено проблеми захисту інформації у процесах електронного урядування як на адміністративному, програмному, так і процедурному рівнях. Доведено ефективність розв’язку таких проблем шляхом створення відповідного захищеного консолідованого інформаційного ресурсу.

Визначено етапи розроблення такого захищеного консолідованого інформаційного ресурсу та описано основні сутності його бази даних, які мають бути враховані.

Захищений консолідований інформаційний ресурс повинен відповідати вимогам визначених функціональних характеристик, техніко-економічних показників, надійності, цілісності, технічного захисту інформації. Захист інформації у базі даних створеного консолідованого ресурсу відбувається за рахунок застосування MS SQL, що є сервером високого класу, який забезпечує управління розробленою БД, її безпеку і стабільність роботи та гарантує найвищий рівень захисту даних. Крім того, для захисту особистих даних користувача використовується SSL сертифікат – криптографічний протокол, що встановлює безпечне з'єднання клієнта і сервера.

Даний консолідований інформаційний ресурс дозволить підвищити ефективність діяльності органів публічної влади, забезпечить зростання їх відкритості та прозорості, завдяки використанню цілісної консолідованої інформації для прийняття управлінських рішень.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Методичні вказівки до проведення практичних занять та до виконання самостійної й індивідуальної роботи з дисципліни „Основи науково-дослідної роботи для студентів напрямів підготовки 6.030601 – „Менеджмент та 6.170103 – „Управління інформаційною безпекою / Укладачі: А. О. Азарова, В. В. Карпінєць. Вінниця: ВНТУ, 2013. 44 с.
2. Азарова А. О., Гаврилова О. В. Розробка методики визначення економічної безпеки підприємства. *Збірник наукових праць «Економіка: проблеми теорії та практики»*. Дніпропетровськ: ДНУ, 2004. Вип.191, т. III. С. 719–727.
3. Азарова А. О., Ткачук Л. М., Хошаба О. М. Шляхи створення інституційних засад муніципального управління засобами публічного врядування на основі соціальної рефлексії. *Державне будівництво*. 2019. №1. С. 1–11. URL : <http://db.journal.kharkiv.ua/index.php/db/article/view/32/30>.
4. Азарова А. О., Ткачук Л. М., Нікіфорова Л. О., Шиян А. А., Хошаба О. М., Каплун І. С. Шляхи удосконалення публічного управління регіональним розвитком на основі сучасних ІТ-технологій. *Інвестиції: практика та досвід*. 2019. №10. С. 88–98.
5. Азарова А. О., Ткачук Л. М., Нікіфорова Л. О., Шиян А. А., Хошаба О. М. Публічне управління та адміністрування в контексті захисту його інформаційного простору. *Вісник Житомирського державного технічного університету*. 2019. № 2 (88). С. 149–155.
6. Нікіфорова Л. О., Азарова А. О., Ткачук Л. М., Шиян А. А., Хошаба О. М. Управління стратифікацією суспільства засобами електронної демократії. *Публічне управління і адміністрування в Україні*. 2019. №11. С. 122–126.
7. Азарова А. О., Шиян А. А., Нікіфорова Л. О., Ткачук Л. М. Моделювання взаємодії суспільства та влади в контексті електронної демократії та публічного управління і адміністрування. *Університетські наукові записки*. 2019. № 1–2 (69–70). С. 156–166.
8. Shyian A. A., Azarova A. O., Nikiforova L. O., Tkachuk L. M. The modeling of communication between the community and authorities in the process of implementing the social projects as e-democracy and public administration. *Економічні горизонти*. 2019. №1(8). С. 89–98.
9. Shyian A., Mironova Y., Shturma L. The development of secured consolidated information resource of activity analysis of the poultry industry in Ukraine. *Technology audit and production reserves*. 2019. №6/2(50). Р. 14–18.
10. Автоматизация процессов публичного управления и администрирования на основе СППР / Азарова А. А., Ткачук Л. М., Каплун И. С., Тямушева В. М. Коллект. науч. монография «Вопросы современной науки» / под ред. А. А. Еникеева. Москва : Изд. «Интернаука», 2019. Т. 39. 122 с. С. 82 – 97.
11. Публічне управління та адміністрування : навч. посібник / [Азарова А. О., Ткачук Л. М., Шиян В. В., Нікіфорова Л. О., Хошаба О. М., Міронова Ю. В., Небава М. І.]. Вінниця : ВНТУ, 2019. 181 с.
12. Берко А. Ю. Системи управління базами даних та знань. К. : Магнолія. 2006, 680 с.
13. Лобок О. П. Організація баз даних та знань. Теоретичні основи проектування, реалізації та використання баз даних. К. : НУХТ, 262 с.
14. Bootstrapping Hibernate 5 with Spring. *Baeldung*. URL: <https://www.baeldung.com/hibernate-5-spring>. (дата звернення: 05.03.2020)
15. Матвієнко О. В. Консолідована інформація: навч. посіб. / П. І. Матвієнко, М. Н. Цивін. К. : «Центр учбової літератури», 2014. 134 с.
16. Ситник Н. В., Краснюк М. Т. Проектування баз і сховищ даних: навч. посіб. К. : КНЕУ, 2015. 264 с.

Азарова Анжеліка Олексіївна – к.т.н., проф. каф. МБІС, заст. декана Факультету менеджменту та інформаційної безпеки з наукової роботи та міжнародного співробітництва Вінницького національного технічного університету, м. Вінниця, e-mail: azarova.angelika@gmail.com.

Ляхович Людмила Миколаївна – студентка групи КІНз-19мз, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: lyakhovich.ludmila@gmail.com.

Anzhelika Azarova – PhD., Professor, Deputy dean of the Faculty of management and information security by scientific work and international cooperation Vinnytsia National Technical University, Vinnytsia, e-mail: azarova.angelika@gmail.com

Liudmyla Liakhovych — student of group KINz-19mz, Faculty of management and information security, Vinnytsia National Technical University, Vinnytsia, e-mail: lyakhovich.ludmila@gmail.com.