УДК 621.396
DOI: 10.31673/2409-7292.2020.011117

Пуха М.С., Савченко В.А., Панадій С.В.

КОМПОНЕНТНА МОДЕЛЬ ЗАХИСТУ ПЕРЕДАЧІ ДАНИХ У СИСТЕМІ ЕЛЕКТРОННОГО УРЯДУВАННЯ

У статті розглядається компонентна модель захисту передачі даних у системі електронного урядування, яка поєднує технічні підходи та організаційні заходи. Основний підхід авторів базується на збалансованому включенні різних технологій з огляду на забезпечення цілісності, конфіденційності та доступності інформації для користувачів, забезпечення контрольованості та швидкодії роботи систем на основі довіри між користувачами та службами Е-уряду. Пропонуються основні комопненти технічного та організаційного спрямування, а також підходи щодо їх поєднання.

Ключові слова: Електронний уряд, захист інформації, компонентна модель.

Вступ

Електронне урядування (електронний уряд, Е-уряд) – це використання інструментів та сервісів інформаційно-комунікаційних технологій, заснованих на мережі Інтернет, для організації взаємодії між реальним урядом країни та її громадянами, бізнесовими та комерційними структурами та урядовими установами [1]. Запровадження "Держави у смартфоні" несе низку переваг, пов'язаних зі зниженням витрат на роботу системи державного управління та забезпеченні довіри між громадянами країни та державними інституціями. Разом з тим, існує значне коло обмежень, що впливають на ефективну взаємодію між учасниками процесу.

Постановка проблеми.

По мірі розширення використання Інтернету зростають також і ризики втручання у роботу систем, що висуває проблему захисту інформації на передній план. Зазначена проблема включає як технічну складову (безпека баз даних, додатків, хостів та Інтернету в цілому) так і соціальні ризики (психологія, етика поведінки), які потребують забезпечення конфіденційності, цілісності та доступності інформації. Зазначені складові інфомаційної безпеки є пріоритетним питанням при організації Е-урядування, оскільки:

більшість додатків Е-уряду базуються на Інтернет-технологіях, що, з одного боку, дозволяє надавати громадянам розширений перелік послуг, забезпечити легкий доступ та прозорість дій, а, з іншого, збільшує кількість уразливостей, які можуть бути використані зловмисниками;

Е-уряд зберігає значну кількість персональних даних громадян і ця інформація може бути використана зловмисниками, які можуть створювати потенційну загрозу конфіденційності, або спотворювати інформацію, порушуючи її цілісність [2].

особливо гостро стоїть питання ефективної аутентифікації користувачів, зокрема при наданні доступу до певної інформації у додатках [3], електронного голосування [4], використання електронних паспортів [5] або здійснення електронних транзакцій [6] через портали електронного уряду;

порушення безпеки може мати суттєві наслідки також при відсутності доступу до інформації, особливо зважаючи на те, що у найближчому майбутньому уся робота з громадянами перейде в режим онлайн [7,8].

Важливість забезпечення безпеки в електронному Е-уряді обумовлюється тим фактом, що у світі постійно виявляються нові уразливості безпеки TCP/IP протоколів та у системах захисту електронних ресурсів, при цьому немає стандартного механізму виявлення уразливостей, як нових, так і ще невідомих.

На рис. 1 показано необхідність безпечних відносин між громадянами та сервісами електронного уряду.

У якості основного ресурсу, за яким полюють зловмисники, як правило є інформація і розвиток нових технологій, таких як соціальні мережі, хмарні обчислення, Інтернет речей та ін. лише розширює поле діяльності для кіберзлочинності [7].

Аналіз досліджень та публікацій.

При комунікації між клієнтом та агентством важливим питанням є довіра між обома сторонами процесу комунікації, яка має на меті забезпечити достовірність передачі даних. Особливо важливими аспектами у цьому сенсі є гарантування авторства інформації та запитувача інформації, тобто достовірні дані повинні бути передані авторизованому користувачеві [9]. Конфіденційність передбачає забезпечення того факту, щоб жодна стороння особа не могла отримати будь-які відомості про передані дані. Зокрема, повинні бути забезпечені основні аспекти безпеки передачі даних (захист від сторонніх підключень під час передачі) та достовірна адресація (захист від передачі даних третій стороні).

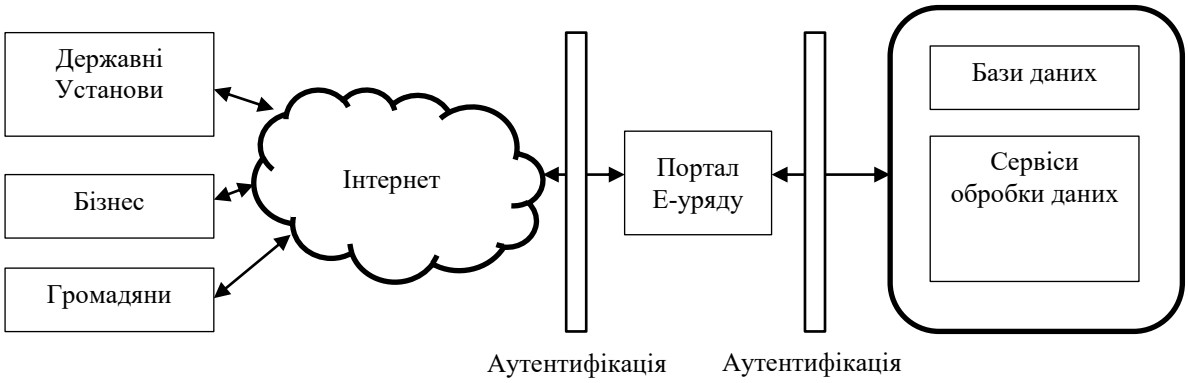

Рис. 1. Структура безпеки електронного уряду.

Особливості передачі даних у Е-уряді. Розглядаючи систему Е-уряду взагалі, як правило, звертають увагу лише на процеси обміну даними між клієнтом та агентством, тобто введення та виведення даних. Разом з тим, системи безпеки повинні охоплювати також і зв'язок (передачу даних), при цьому розрізняючи передачу від клієнта до агентства та від агентства до клієнта [9].

Електронний уряд – це онлайн система, заснована на мережевих технологіях. При цьому, на відміну від інших онлайн систем, Е-уряд обробляє багато важливої та унікальної інформації, яка повинна бути захищена від несанкціонованих користувачів. Основними проблемами безпеки для Е-уряду можуть бути впливи на:

конфіденційність – забезпечення доступу до систем та інформації лише для тих, хто має право на доступ до неї;

цілісність – забезпечення того, щоб елементи системи та дані не були підроблені (випадково чи навмисно) і перебувають у їх первинному стані;

контрольованість – гарантування того, що коли дані передаються одержувачу, ні одержувач, ні відправник не можуть заперечувати отримання або надсилання даних;

аутентифікація – забезпечення того, що суб'єкти (фізичні, апаратні чи програмні) можуть бути аутентифіковані як оригінальні та справжні сутності;

довіра – створення інфраструктурного середовища, яке базується на довірі та зрозумілих правилах для користувачів.

Основними сферами запоровадження Е-уряду є підприємництво, інновації, дослідження та розробки, дистанційне навчання, електронне здоров'я, сфера соціально-побутового обслуговування. У подальшому електронні машини для голосування стануть одними з найбільш важливих для прийняття рішень урядами країн, однак будь-який збій у виборі правильного кандидата чи рішення може призвести до катастрофічних наслідків [10]. Це може стати наслідком недосконалості роботи інтерфейсів, апаратних чи програмних помилок. Разом з тим, гарантування перевірки програмного забезпечення ще не забезпечує повну безпеку Е-уряду.

Вже зазаз деякі країни для електронних транзакцій через портал електронного самоврядування, такі як, наприклад, отримання водійського посвідчення, вимагають конфіденційної інформації та аутентифікації, хоча такі дані також можуть бути модифіковані. У роботі [8] пропонується хороше рішення, яке зберігає автентифікацію, конфіденційність, цілісність та незмінність даних на різних рівнях як найважливіші характеристики захищених даних, однак у дослідженні розглядається лише окремий додаток, який піддається ризику, і не розглядається можливість впливу на зазначені компоненти з боку інших компонентів інфраструктури.

Ще одна загроза, яка може може впливати на електронне урядування – клонування та підроблення електронних паспортів [5]. Електронний паспорт містить інформацію, яка закладена у чіп, що зберігає особисті дані власника, біометричні характеристики та іншу інформацію. Часто процес перевірки електронного паспорта приймає документ, наприклад, у випадках використання чіпів старої версії або застосування застарілих протоколів безпеки, тому зловмисник може клонувати такий паспорт.

Щоб оцінити ступінь безпеки Е-уряду, потрібно вивчити правила та політику безпеки конкретного сервісу. В [11] визначено найважливіші загрози, з якими може зіткнутися електронний уряд. Вони поділяються на 3 класи (загрози кінцевих клієнтів, загрози каналу зв'язку та загрози на боці сервера), а також, які вимоги безпеки щодо інформаційних систем та конфіденційності застосовуються.

Оцінка безпеки Е-уряду може бути здійснена на основі матриць безпеки, які, в свою чергу, будуються з використанням відповідних моделей, а саме:

технічні моделі: модель Bell-LaPadula (фокус на конфіденційності), BibaModel (фокус на цілісність), модель Кларка-Вілсона (фокус на цілісність), Китайська стіна (фокус на конфіденційність та цілісність), Lambroudadaisis Framework Framework (доступність та автентифікація), InfosecModel (фокус на доступності, цілісності та конфіденційності) [12,13].

нетехнічні моделі та теорії: такі як Теорія розумної дії, Теорія планової поведінки, Модель прийняття технологій, Дифузія інновацій, Мотиваційна модель, Соціальна когнітивна теорія, Модель використання ПК, Уніфікована теорія прийняття та використання технологій, остання модель охоплює всі вище зазначені нетехнічні теорії.

У той же час, на сьогодні немає моделі, яка б охоплювала як технічні, так і нетехнічні питання одночасно [12].

Безпека хмарних обчислень. Хмарні обчислення – це технологія надання послуг клієнтам через Інтернет у різних моделях, зокрема: а) інфраструктура як послуга, б) програмне забезпечення як послуга і в) платформа як послуга [14,15]. Хмарні обчислення мають низку переваг, таких як зниження витрат, відсутність необхідності утримування місця для зберігання даних, масштабованість та еластичність, але перед цією технологією стоять великі проблеми в забезпеченні захисту даних. Побудова так званої Урядової хмари G-cloud зазвичай вимагає більш безпечних і надійних механізмів аутентифікації та ідентифікації [15].

У дослідженні [16] було запропоновано новий механізм шифрування баз даних з гнучкою продуктивністю та доступом до бази даних, що забезпечує конфіденційність урядових даних. Механізм спирається на алгоритм симетричного ключа AED (advanced encryption standard), який зашифровує всі дані перед зберіганням у хмарі. Також, він використовує індексування для поліпшення продуктивності запитів, що дозволяє уникнути повного сканування усієї бази [17].

Уряд у смартфоні. Mobile-Government (М-уряд). Нова тенденція BYOD (принеси власний пристрій) стає популярною у більшості компаній та асоціацій [17], де працівники використовують власні смартфони для доступу до інформаційних систем, однак це насправді лише збільшує ризики безпеки. Загальний ризик полягає в тому, що номери мобільних телефонів користувачів будуть відстежуватися, коли вони надсилають свої пропозиції та запити в уряд [18-19] і це може загрожувати конфіденційності користувача [20].

Метою даної статті є формування компонентної моделі захисту передачі інформації у системі електронного урядування.

Компонентна модель захисту передачі даних у системі електронного урядування

Надання безпечного сервісу електронного урядування є критичним питанням для підтримки довіри уряду та користувачів до системи. Без сумніву, компонентна модель має охоплювати всі фактори, які впливають на послуги електронного уряду, оскільки служби електронного уряду постійно стикаються з багатьма проблемами безпеки, такими як: крадіжка персональних даних, злом та відмова в обслуговуванні, або проблеми, пов'язані з недобросовісними користувачами електронного уряду. Отже, захист конфіденційності, цілісності та доступності інформації є важливим аспектом Е-урядування, однак усі ці аспекти пов'язані з суто технічними проблемами, у той же час, залишається важливою ще низка питань соціального чи соціотехнічного спрямування.

Соціальна інженерія, яка розглядається як нетехнічна загроза, використовується для компрометації безпеки технічних систем за допомогою людського фактора, коли зловмисник використовує обман, переконання та впливає на авторизованих користувачів для отримання інформації. В результаті цих загроз зловмисник отримує несанкціонований доступ для вчинення диверсій та вандалізму чи шпигунства та зловживань урядовою інформацією. Таким чином, іншим важливим блоком компонентної моделі має бути блок нетехнічних засобів, який захищатиме систему саме від соціотехнічних атак.

Блок технічного захисту компонентної моделі захисту передачі інформації у системі електронного урядування має включати наступні компоненти.

Безпека мережі. Доступ до Інтернету є ключовим аспектом використання сервісів Е-урядування. Відсутність доступу до Інтернету або його висока вартість є першою загрозою для Е-уряду в цілому.

Ідентифікація. Усі учасники Е-урядування мають бути надійно та унікально ідентифіковані.

Забезпечення конфіденційності. Захист системи має убезпечувати від розкриття конфіденційної інформації та несанкціонованого доступу до приватних даних громадянина.

Контроль доступу. Це технологія, орієнтована на користувача, яка поєднує питання ідентифікації, автентифікації та авторизації. Іншими словами, захист системи має забезпечити механізми контролю доступу при обміні інформацією між урядом та громадянами.

Електронна аутентифікація. Щоб побудувати ефективну систему електронного урядування, важливо запропонувати високонадійну індивідуальну ідентифікацію як для приватного, так і для державного сектору. При цьому інфраструктура відкритих ключів (PKI) – це технологія, визнана найкращою аутентифікацією для електронного уряду.

Обмін інформацією. Обмін інформацією між державними установами завжди був пов’язаний з певними складнощами. Цей обмін необхідний, щоб урядові установи реалізовували процес електронного обслуговування. Разом з тим, побудова надійної і ефективної системи зв’язку залишається актуальною проблемою.

Структуризація даних. Структуризація даних – це процес сортування даних на основі номінальних значень відповідно до їх чутливості щодо безпеки (у залежності від дії чинного законодавства та правил). Дані та інформаційні ресурси структуризуються на основі ризику несанкціонованого доступу, наприклад, щодо втрати чи викраденя. Дані з високим рівнем ризику класифікуються як конфіденційні, для яких потрібен більш високий рівень захисту, тоді як дані з меншим ризиком можуть вимагати пропорційно меншого захисту.

Організація процесів обробки. Процеси обробки даних – це технології, що використовуються для управління процесами обробки даних під час фаз планування, виконання та оцінки в системі електронного урядування. Наприклад, вони можуть характеризуватися успішністю обробки веб-заявки окремою особою чи організацією, що дуже важливо для електронного уряду.

Сертифікація обміну. Урядові відомства використовують інфраструктури відкритих ключів (PKI) для здійснення внутрішніх процесів і транзакцій, впроваджуючи для

забезпечення безпеки передачі інформації віртуальні приватні мережі (VPN). Для забезпечення загальноприйнятого підходу "єдиного вікна", більшість урядових відомств пов'язані також з іншими урядовими департаментами та відомствами. Якщо ці взаємодіючі відомства використовують свої внутрішні засоби безпеки то вкрай необхідним є аміністрування їх корпоративних PKI, хоча такі корпоративні PKI можуть бути реалізовані на різній архітектурі, політиках безпеки та криптографічних протоколах.

Захист від DoS атак на рівні хостів. Зловмисник може спричинити втрату мережевої здатності операційної системи або і її пошкодження шляхом надсилання значної кількості запитів на порти даних окремого хоста.

Захист від DoS атак на рівні локальної мережі. Відмова в обслуговуванні на рівні локальної мережі виникає, коли зловмисник надсилає до локальної мережі підроблені IP-пакети, або велику кількість стандартних UDP пакетів, внаслідок чого система перестає реагувати.

Раціональна мережева інфраструктура. Відсутність належного встановлення мережевих брандмауерів, конфігурації мережевої безпеки, вразливості інтернет-протоколів та Інтернет-залежність – основні проблеми, які впливають на безпеку електронного уряду.

Захищена Інтернет-інфраструктура. Серйозні атаки включають не лише конкретні системи в Інтернеті, а й елементи Інтернет-інфраструктури. Наприклад, постачальники мережевого доступу, сервери мережевих імен та баз даних, від яких залежить велика кількість користувачів. Усі ці об’єкти також можуть бути атаковані, що може серйозно затримати щоденну роботу багатьох сайтів.

Захист від шкідливого програмного забезпечення. Шкідливе програмне забезпечення має на меті нанесення шкоди данним або знищення комп'ютерної системи. Це, у свою чергу, призводить до втрати конфіденційності або неправильного використання та отримання несанкціонованого доступу до активів системи.

Застосування систем контролю. Важливим аспектом є застосування мережевих аналізаторів, які застосовуються для діагностики проблем, пов'язаних з мережею. Однак, слід мати на увазі, що цей інструмент може також використовувати і зловмисник для збору паролів чи уразливостей мережі і спричинити серйозні порушення в захищеній передачі даних.

Трасування. Це дія, яка використовується для перевірки з'єднання між двома точками. Наприклад, щоб дізнатися, що точка прийому дійсно існує, може бути надіслане порожнє повідомлення. Зловмисник може використати цю інформацію під час незаконного підключення, щоб встановити конфігурацію та інші параметри мережі.

Нейтралізація загроз каналам зв'язку. Зазвичай повідомлення передаються через Інтернет від джерела до місця призначення різними маршрутами. У такому випадку досить важко гарантувати, що кожен вузол в Інтернеті, через який передаються повідомлення, є надійним, безпечним і неворожим.

Нейтралізація серверних загроз. Сервер є однією з основних частин мережі. Він є однією з найбільш уразливих ланок і зловмисники будуть намагатися заподіяти щонайбільшої шкоди саме цій інфраструктурі.

Використання брандмауерів. Брандмауер - це сукупність пов'язаних програм або апаратних засобів, розташованих на сервері мережевого шлюзу, який захищає активи мережі від користувачів. Застосування брандмауерів має бути підпорядковане загальній політиці безпеки системи.

Таким чином, з технічної точки зору компонентна модель має забезпечити достатньо значний перелік заходів та технологій, які забезпечать захищеність даних та інформації у системі Е-урядування стосовно трьох основних аспектів захисту: конфіденційності, цілісності та доступності.

Однак розуміння загроз та протидії їм з технічної точки зору ще недостатньо для забезпечення повної безпеки Е-уряду. Існує також значне коло нетехнічних впливів, яким має протидіяти система.

Блок організаційного захисту компонентної моделі захисту передачі інформації у системі електронного урядування має включати наступні компоненти.

Взаємосумісність. Здатність систем або бізнес-процесів працювати спільно задля досягнення загальної мети залишається одним з ключових факторів безпеки. Ефективність спілкування між владою, бізнесом та громадянами потребує того, щоб продукт, який вони використовують, був здатен обмінюватися даними незалежно від платформ, які використовуються. Відсутність семантичної сумісності через відсутність відповідних стандартів та різних систем класифікації інформації руйнівно впливатимуть на ефективність електронного уряду.

Практичність використання. Діяльність розробників зосереджена на створенні програм та служб, які будуть простими у користуванні. Завдання практичності базується на безпеці використання і тому, чим вищим є рівень безпеки, тим більшим є потенціал використання системи.

Стандарти безпеки. Ці стандарти стосуються керівних органів, які визначають політику безпеки електронного уряду для забезпечення безпечного робочого середовища. Особливо це стосується електронного голосування, електронної демократії, цифрового підпису та інших угод між урядом, користувачами та іншими зацікавленими сторонами.

Політика безпеки - це план визначення основних ресурсів установи з детальним поясненням прийняття чи неприйняття раціональної поведінки громадян та інших зацікавлених сторін з метою ефективного гарантування інформаційної безпеки. Цей план повинен супроводжувати рівень ефективності електронного уряду. Цей показник повинен бути оцінений для виконання заходів безпеки.

Правова база включає такі аспекти, як закони та підзаконні акти, які створюють чимало проблем, пов'язаних зі злочинами у сфері безпеки та загрозами безпеці. Відсутність законів та правил щодо інформаційної безпеки негативно впливає на довіру до влади. Для ефективного Е-урядування необхідно приймати закони та інші нормативні акти для регулювання взаємовідносин, а отже, і робити рішення електронного уряду юридично обов'язковими.

Конфіденційність спілкування. Передові технології мають використовуватись не лише для підвищення ефективності державного управління, але і для зміцнення довіри громадян до Е-уряду через забезпечення конфіденційності та прозорості між громадянами та державними установами. Так, хоча інформаційні системи державних органів мають перешкоджати несанкціонованому доступу до даних, ці персональні дані повинні бути доступними самим їх власникам.

Культура інформаційної безпеки зазвичай сприймається як частина національної культури і полягає в усталених в суспільстві нормах та правилах використання та захисту інформаційних ресурсів.

Інформованість – це здатність людини відчувати, спостерігати та усвідомлювати, що відбувається навколо неї, а також розуміти значення інформації для особистого існування. Поінформованість про інформаційну безпеку має вирішальне значення для розуміння особистої безпеки, яка використовується в цьому плані.

Довіра. Довіра відіграє важливу роль у використанні послуг електронного урядування. Довіра до влади з боку громадян в залежить переважно від відносин між органом електронного уряду та іншими урядовими установами, а також від того, наскільки переконливою є урядова інфраструктура, Інтернет-провайдери та інші державні установи. Щоб отримати високий рівень довіри важливо мати високий рівень інформаційної безпеки. Цього вдасться досягти, залучивши державних службовців до вивчення політики безпеки, архітектури, компетенцій, цілей безпеки та оперативних процедур в державних установах. Довіра до влади гарантує, що транзакції можуть бути здійснені лише автентифікованою особою, після чого їх не можна буде відмінити.

Висновки

Отже, розробка та впровадження систем безпеки є ключовим елементом побудови ефективного Е-урядування. Найбільш доцільним способом організації захисту передачі даних у Е-уряді є комбінування існуючих технічних та нетехнічних підходів. Запропонована модель безпеки може стати основою для Е-урядування ще на етапі розробки концепції та її розбудови. При цьому, метою такого захисту має стати надійне та довірливе спілкування між громадянами та урядом. Крім того, такий підхід сформує ефективне поле для розвитку електронної комерції та бізнесу.

Перелік посилань

1. Погребняк І. Є. Електронний уряд (E-government) і електронне урядування (E-governance): поняття та принципи функціонування // Право та інновації № 3 (7) 2014. 26-35.
2. Електронне урядування та електронна демократія: навч. посіб.: у 15 ч. / за заг. ред. А.І. Семенченка, В.М. Дрешпака. – К., 2017. Частина 13: Захист інформації в системах електронного урядування / [О.М. Хошаба]. – К.: ФОП Москаленко О. М., 2017. – 72 с.
3. Національна стратегія електронної ідентифікації України. Біла книга з електронного урядування. Під редакцією О. Потія та Ю. Козлова // – К: НАДУ, 2015. – 145 с.
4. Соломко Ю. Електронне урядування: поняття, сутність, принципи та напрями розвитку // Ефективність державного управління. 2018. Вип. 2 (55). Ч. 1. – С. 135-143.
5. Luca Calderoni, Dario Maio, (2014) Cloning and tampering threats in e-Passports, Expert Systems with Applications 41 5066–5070.
6. Рощук М. Розвиток електронного урядування в Україні: правовий аспект забезпечення безпеки інформації // Ukrainian Scientific Journal of Information Security, 2018, vol. 24, issue 1, p. 17-22.
7. J. Jang-Jaccard, S.Nepal, (2014) A survey of emerging threats in cyber security", Journal of Computer and System Sciences 80 973–993.
8. Choi M., Lee J. and Hwang K. Information Systems Security (ISS) of E-Government for Sustainability: A Dual Path Model of ISS Influenced by Institutional Isomorphism // Sustainability 2018, 10, 1555.
9. Malik F. Saleh, (2011) Information Security Maturity Model , International Journal of Computer Science and Security (IJCSS), Volume (5) : Issue (3)
10. Adeel Javaid Electronic Voting System Security // SSRN Electronic Journal · January 2014. 1-18.
11. Mohammad Hazza Zu'bi, Hamdan Hasan AL-Onizat, (2012) E-government and security requirements for information systems and privacy (performance linkage), Journal of management research, Vol 4, No.4.
12. Ali, Omar & M.Wahby, Talaat & Osman, Izzeldin. (2016). E-government Security Models. International Journal of Computer Applications Technology and Research. 5. 439-442.
13. Deven C. Pandya1 , Dr. Narendra J. Patel. Study and analysis of E-Governance Information Security (InfoSec) in Indian Context. IOSR Journal of Computer Engineering (IOSR-JCE). Volume 19, Issue 1, Ver. IV (Jan.-Feb. 2017), PP 04-07.
14. Nanos, Ioannis & Misirlis, Nikolaos & Manthou, Vicky. (2017). Cloud Computing Adoption and E-government. 6th International Symposium and 28th National Conference on Operational Research, At Thessaloniki, Greece. June 2017.
15. Almarabeh, Tamara & Majdalawi, Yousef & Mohammad, Hiba. (2016). Cloud Computing of E-Government. Communications and Network. 08. 1-8.
16. Danielsen, Frank & Flak, Leif & Ronzhyn, Alexander. (2019). Cloud Computing in eGovernment: Benefits and Challenges. ICDS 2019 : The Thirteenth International Conference on Digital Society and eGovernments, At Athens, Greece.
17. Ali M. Al-Khouri, (2013) Technological and Mobility Trends in E-Government, Business and Management Research, Vol. 2, No. 3. 132-139.
18. El-Bakry, Hazem. (2015). Cloud Computing in E-Government: A Survey. International Journal of Advanced Research in Computer Science & Technology. Vol. 3, Issue 2 (Apr. - Jun. 2015)
19. Hassan R.G., Khalifa O.O. E-Government - an Information Security Perspective // International Journal of Emerging Trends & Technology in Computer Science. 2016. 36(1):1-9.
20. Shareef M. Shareef. Enhancing Security of Information in E-Government // Journal of Emerging Trends in Computing and Information Sciences. Vol. 7, No. 3 March 2016. 139-146.

Надійшла: 15.01.2020 Рецензент: д.т.н., професор Кожухівський А.Д.