ПУБЛІЧНЕ УПРАВЛІННЯ ТА АДМІНІСТРУВАННЯ

УДК 351.072.2:004
DOI: https://doi.org/10.26642/jen-2019-2(88)-149-155

А.О. Азарова, к.т.н., проф.
Л.М. Ткачук, к.е.н., доц.
Л.О. Нікіфорова, к.е.н., доц.
А.А. Шиян, к.ф.-м. н., проф.
Вінницький національний технічний університет
О.М. Хошаба, с.н.с.
Інституту проблем математичних машин та систем Національної академії наук України

Публічне управління та адміністрування в контексті захисту його інформаційного простору

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. Найбільш значущою і активно досліджуваною категорією публічного управління є електронне урядування, активний захист інформації в якому постає одним із першочергових завдань та вимагає вирішення. Проаналізовано стан публічного управління та адміністрування в Україні та закордоном. Виявлено проблемні питання, що потребують вирішення як на теренах України, так і в контексті його узгодження з інформаційним простором 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. Для органів публічного адміністрування особливої актуальності набуває використання проривних технологій і тенденцій, таких як Інтернет речей, хмарні технології, мобільні пристрої та контроль за ризиками, що виникають у системах електронного урядування.

Ключові слова: *публічне управління та адміністрування; електронне урядування; захист інформації.*

Актуальність теми. Новітні підходи до публічного управління та адміністрування викликають потреби створення умов для безпечного функціонування його суб'єктів, зокрема особливої актуальності набувають проблеми протидії інформаційним війнам та захист кіберпростору електронного урядування як на рівні макро-, так і на регіональному і мікрорівнях.

Дослідження наукових анналів сучасної літератури із цього питання дозволило виявити той факт, що трактування понять інформаційної безпеки у процесах публічного управління є неоднозначним. Із позиції багатоаспектних підходів визначення цього поняття нерозривно пов'язане з такими поняттями, як «потреби», «інтереси», «стійкість», «відтворення», «загрози» і «ризик». Таким чином, оцінювання інформаційної безпеки у процесах публічного управління має ґрунтуватися на комплексному методичному підході, що охоплює усі інформаційні потреби сучасного суспільства.

Тому надзвичайно важливими питаннями сьогодні є визначення основних понять, сутності та завдань захисту інформації, ознайомлення з концепцією захисту інформації в Україні, аналіз основних загроз інформаційній безпеці у процесах публічного управління та вивчення основних методів протидії їм, що надає можливість використовувати отримані знання та навички на практиці.

Аналіз останніх досліджень та публікації, на які спирається автор. Значний внесок у висвітлення питань, що стосуються інформаційної безпеки, зробили В. А. Лужецький, О. І. Барановський, В. М. Варналій, В. М. Гейць, В. І. Мунтіян, В. Т. Шлемко, О. А. Баранов, К. І. Бєлякова, В. М. Брижко, В. Д. Гавловський, Д. С. Гаврилов, О. В. Гладківська, М. В. Гуцалюк, М. В. Жулинський, Л. М. Задорожна, Я. В. Зінченко, Г. П. Лазарєв, А. І. Марущак, А. М. Новицький, С. Л. Северин, В. Г. Хахановський, В. А. Швець та ін.

Більшість наукових праць присвячується дослідженню інформаційної безпеки держави, створенню захищених окремих інформаційних систем, що застосовуються у процесах публічного управління та ін. Різні аспекти проблем інформаційної безпеки підприємницької діяльності розглянуто в наукових працях таких вітчизняних і закордонних дослідників, як В. В. Домарев, М. В. Куркін, О. М. Горбатюк, Т. М. Ткачук, О. П. Савва, Л. І. Донець, Н. В. Ващенко та ін. Проте невирішеними та проблемними залишаються численні питання, пов'язані з оцінюванням різних рівнів захисту інформації у процесах публічного адміністрування. Також потребують подальших досліджень методи захисту інформації для

забезпечення ефективної взаємодії владних структур та громади у процесах публічного управління і шляхи їх практичної реалізації.

Метою статті є виявлення та обґрунтування потенційних можливостей захисту інформації в процесах публічного управління та адміністрування.

Викладення основного матеріалу. Інформаційна безпека – найважливіший елемент системи безпеки публічного управління та адміністрування. Заходи із забезпечення інформаційної безпеки, з одного боку, спрямовані на охорону конфіденційної інформації (зокрема, усунення «жучків», запобігання несанкціонованому доступу до локальних комп'ютерних мереж тощо). З іншого – включають контрзаходи (пошук даних про конкурентів, партнерів і контрагентів), які сприяють розвитку довіри до владних структур з боку народу і слугують для запобігання неприємним несподіванкам.

Поняття інформації в загальному вигляді містить ст.1 закону України «Про інформацію» [1]. Відповідно до ст. 30 цього Закону інформація з обмеженим доступом поділяється на конфіденційну та таємну.

Масштабне і масове протікання процесів публічного управління, пов'язаних із проявом небезпеки та можливістю завдання збитків, виявляється у вигляді інформаційних війн, масштаби яких у наш час набули величезних розмірів і специфічних форм прояву. Разом із тим, необхідно відзначити, що відкритість суспільства, залучення до вирішення складних проблем публічного управління великої кількості людей, ресурсів цілих країн супроводжуються низкою негативних явищ, які безпосередньо пов'язані з використанням інформації, інформаційних продуктів і послуг, зокрема:

- численні порушення у фінансово-кредитній сфері (шахрайство, обман, неправомірні дії з документацією у сфері електронного документообігу, електронного урядування тощо);
- несанкціонований доступ до конфіденційної інформації;
- неправомірні зміни, що спотворюють зміст інформації, внаслідок чого вона втрачає свою юридичну значимість і цінність;
- численні явища, що призводять до значних негативних наслідків у масштабах цілої країни, які на сьогодні представляються загальною назвою «інформаційна війна».

В українському сегменті публічного управління засобами мережі Інтернет на даний момент існує більше 2500 веб-сторінок, що автоматизують цей процес на рівні державного сектора. Із них приблизно половина має виявлені ознаки компрометації, проте це лише явні ознаки, адже існує ще набагато більша частка невиявлених атак, але потенційно загрозливих.

Протягом 2 місяців 2019 року близько 8,5 тис. спланованих кібератак було виявлено в Україні на об'єктах п'яти відомств і 31 державного інформаційного ресурсу. У першу чергу це – підприємства енергетичного сектора і державні структури. Такі кібератаки, на жаль, спричинили численні негативні наслідки, незважаючи на наявність у кожної з постраждалих організацій відповідних антивірусних засобів захисту.

Особливої шкідливості набувають загрози у кіберпросторі, оскільки вони є постійно змінюваними. Відомі загрози набувають більш небезпечних, підступних та ефективних в дії типів, наприклад Advanced Persistent Threats (APT) – просунуті стійкі загрози. CERT-UA регулярно фіксує атаки на органи державної влади України які мають усі ознаки APT. Найчастіше джерелами APT є установи, що фінансуються з державних бюджетів та мають цілі, що виходять далеко за межі простої крадіжки: військова розвідка, економічний саботаж, технічний шпіонаж, фінансові махінації, політичні маніпуляції.

У той час, коли органи публічного управління все більше переводять свою діяльність у цифровий світ і створюють нові канали взаємодії з користувачами, постійні мутації кіберзагроз породжують нові ризики і нові питання у системі ефективного публічного управління.

Для органів публічного адміністрування особливої актуальності набуває використання проривних технологій і тенденцій, таких як Інтернет речей, хмарні технології, мобільні пристрої та контроль за ризиками, що виникають в системі електронного урядування.

Керівники органів публічної влади все більше усвідомлюють необхідність забезпечення передових технологій кібербезпеки. Але, щоб реагувати на інциденти, тільки усвідомлення недостатньо, питання кібербезпеки повинні бути предметом постійної уваги. Не зважаючи на інформаційно-пропагандистську роботу, що проводять ЗМІ, владні структури публічного управління недостатньо комп'ютерно грамотні і не сприймають в повній мірі такі загрози, не дотримуючись необхідних умов з реалізації заходів культури кібербезпеки.

Усі ці чинники доводять важливість визначення умов функціонування ефективної системи інформаційного захисту у процесах публічного управління та адміністрування.

Послуговуючись анналами українського законодавства [1-8] у питаннях захисту публічної інформації, вирішення таких проблеми на рівні держави має здійснюватися на основі:

- створення повнофункціональної інформаційної інфраструктури усіх гілок між владою та громадами і забезпечення захисту її критичних елементів;
- підвищення рівня координації діяльності державних органів щодо виявлення, оцінювання і прогнозування загроз інформаційній безпеці у процесах публічного управління, запобігання таким загрозам та забезпечення ліквідації їхніх наслідків, врахування міжнародного досвіду з цих питань;

- вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки у процесах публічного адміністрування, зокрема захисту інформаційних ресурсів електронного урядування, протидії комп'ютерній злочинності, захисту персональних даних позивачів та дописувачів, а також правоохоронної діяльності в інформаційній сфері;

- розгортання та розвитку Національної системи конфіденційного зв'язку між владою та народом як сучасної захищеної трансмісійної основи, здатної інтегрувати такі територіально розподілені інформаційні системи електронного урядування різних рівнів, в яких обробляється конфіденційна інформація.

Складність та комплексність проблем електронного урядування спричиняє залучення до вирішення проблеми інформаційної безпеки держави, яка має забезпечити наявність:

- законодавчих, нормативно-правових та нормативних актів щодо інформаційної безпеки;
- відповідність їх міжнародними стандартами ISO;
- власних розробок у напрямку безпечного електронного урядування.

Отже, для реалізації законодавчих, нормативно-правових та нормативних актів щодо інформаційної безпеки електронного урядування має бути створено відповідну потужну систему захисту інформації.

Аналіз існуючої системи захисту дозволив виявити такі державні органи інформаційної безпеки [9]:

- відповідні підрозділи спецслужб держави;
- спеціально уповноважений орган держави з питань захисту інформації: Державна служба спеціального зв'язку та захисту інформації України;
- Національний координаційний центр кібербезпеки;
- Міжвідомча комісія з питань інформаційної політики та інформаційної безпеки при Раді національної безпеки і оборони України;
- Державний центр кіберзахисту та протидії кіберзагрозам.

Специфічними службами створення інформаційної безпеки в системі електронного урядування є [9]:

- Державна агенція з питань електронного урядування України;
- Державна служба спеціального зв'язку та захисту інформації України;
- підрозділ з інформаційного забезпечення органу публічного управління, який серед інших завдань також має займатися створенням і підтриманням систем управління інформаційною безпекою та використовує комплексну систему захисту інформації у таких процесах;
- Міністерство юстиції України (в частині роботи з електронними цифровими підписами (ЕЦП)).

Одним із ефективних засобів електронного урядування є цифрове підписування, серед найбільш поширених та актуальних прикладних задач якого є такі [10, 11]:

- створення безпеки електронного документообігу;
- убезпечення електронних платіжних систем та електронної комерції;
- забезпечення авторства під час електронного голосування;
- підписування повідомлень електронної пошти;
- аутентифікація (процедура встановлення належності користувачеві інформації в системі пред'явленого ним ідентифікатора) у бездротових мережах;
- створення безпеки мобільної комерції;
- безпечність стільникового зв'язку;
- підписування цифрових сертифікатів та цифрових паспортів на базі смарт-карток.

Варто зазначити, що у Стратегії кібербезпеки України стверджує необхідність створення умов до залучення господарських суб'єктів різних рівнів, установ та організацій незалежно від форми власності до провадження ними захищеної діяльності у сфері електронного урядування. Особливо це стосується захисту інформації розпорядниками об'єктів критичної інфраструктури щодо створення кібербезпеки України. Крім того, ними має вирішуватися питання щодо обов'язковості застосування заходів із дотримання інформаційної безпеки згідно з вимогами вказаного вище чинного законодавства [1–8], а також щодо сприяння ними державним органам у виконанні завдань із забезпечення кібербезпеки.

Держава має сприяти залученню наукових установ, навчальних закладів, організацій, громадських об'єднань і громадян до розроблення та реалізації заходів із кібербезпеки і кіберзахисту [9].

Найбільш ефективним рівнем протидії загрозам і створення інформаційної безпеки є саме законодавчий. Розроблення та впровадження відповідних законодавчих актів створює умови для безпечного використання сучасних інформаційних технологій, захищеного доступу до інформації, захисту її від несанкціонованого доступу та витоку технічними каналами. Крім того, важливим питанням для державотворення є захист громадян, суспільства і владних структур від неправдивої інформації, реалізації усіх складових інформаційної безпеки.

Найбільш практично значимим з точки зору використання технології інформаційної безпеки в системах електронного урядування є Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [6], який регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Він чітко окреслює об'єкти захисту в системі та суб'єкти відносин, порядок доступу до інформації в системі, відносини між власником

інформації, власником інформаційно-телекомунікаційної системи та користувачами, відповідні умови забезпечення захисту інформації в системі, повноваження державних органів та відповідальність за порушення законодавства, міжнародні договори та прикінцеві положення.

Закон України «Про Національну програму інформатизації» [3] визначає загальні засади формування, виконання та коригування Національної програми інформатизації. Пріоритетними завданнями цієї програми є формування правових, науково-технічних, організаційних, фінансових та гуманітарних засад регулювання процесу її формування та виконання. Вона визначає стратегію вирішення проблем забезпечення інформаційних потреб та інформаційної підтримки публічного управління та адміністрування в напрямках соціальному, економічному, екологічному, науково-технічному, оборонному, національно-культурному та інших сферах загальнодержавного значення. Зокрема, Національна програма інформатизації містить:

- Концепцію Національної програми інформатизації;
- сукупність державних програм з інформатизації;
- галузеві програми та проекти інформатизації;
- регіональні програми та проекти інформатизації;
- програми та проекти інформатизації органів місцевого самоурядування.

Національна програма інформатизації формується, виходячи з довгострокових пріоритетів соціально-економічного, науково-технічного, національно-культурного розвитку країни з урахуванням світових напрямів розвитку та досягнень у сфері інформатизації і спрямована на розв'язання найважливіших загальносуспільних проблем – державного управління та адміністрування, забезпечення розвитку освіти, науки, культури, охорони довкілля та здоров'я людини, національної безпеки, оборони держави і демократизації суспільства та створення умов для інтеграції України у світовий інформаційний простір відповідно до сучасних тенденцій інформаційної геополітики [9].

Процеси інтеграції України до світового інформаційного простору викликають особливу потребу в опрацюванні нових підходів [12–16] до захисту інформації в задачах публічного управління та адміністрування. Разом із тим, врахування закордонного досвіду розбудови системи захищеного публічного управління та адміністрування є надзвичайно важливим для України.

Практика впровадження систем електронного урядування в різних країнах світу існує понад два десятиліття. За цей час накопичено істотний як позитивний, так і негативний досвід. Раціональне застосування цих узагальнених результатів дозволяє суттєво економити ресурси, як фінансові, так і людські, скоротити кількість помилок, вирішити проблеми стандартизації, уніфікації та взаємодії національної системи електронного урядування з міжнародними.

Європейський Союз (ЄС) надає особливу увагу проблемам становлення захищеного інформаційного суспільства, зокрема, Серія документів ISACA про впровадження європейської кібербезпеки, подає загальний огляд впровадження передового досвіду в галузі кібербезпеки згідно з діючими законами, стандартами та іншими настановами. У цих документах зазначено, що, виходячи з європейського досвіду, кібербезпека вимагає, щоб у всіх державах-членах та асоційованих країнах застосовувалися загальноприйняті визначення та основні положення [9]. Крім того, в Серіях документів ISACA визначено, що кібербезпека – це не тільки захист організації та її інформаційних ресурсів. У багатьох випадках реструктуризація певних частин чи всього корпоративного середовища інформаційних технологій у певній організації приводить до посилення кібербезпеки.

У багатьох країнах, які послуговуються європейськими стандартами на управління кібербезпекою в галузі публічного адміністрування існують різні вимоги, зокрема:

- захист і конфіденційність інформації в системі електронного урядування;
- фінансовий контроль та пов'язана з ними система внутрішнього управління, включаючи фінансову звітність;
- державні та місцеві постанови про секретну інформацію (наприклад, про службові таємниці);
- збереження та оброблення інформації третіми сторонами тощо.

До найважливіших закордоном нормативно-правових актів у сфері становлення публічного управління, що діють на цей час, відзначають Резолюцію 64/211 ООН «Створення глобальної культури кібербезпеки щодо захисту найважливіших інформаційних інфраструктур» від 21 грудня 2009 року19 та Резолюцію 64/25 ООН «Досягнення в сфері інформатизації та телекомунікацій в контексті міжнародної безпеки» від 2 грудня 2009 року [9].

Серед загальних проблем, з якими зіткнулися країни ЄС під час впровадження електронного урядування були різні підходи до вирішення різних складних ситуацій в напрямку публічного адміністрування. Так, зокрема, для багатьох країн європейської спільноти домінантною проблем було забезпечення сумісності різнорідних інформаційних систем публічного адміністрування, що створювалися у різні часи, на основі різних принципів та технологічних платформ.

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:

1. Складність і різнорідність 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 уможливлюють 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 розмежовування 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.

Таким чином, під час створення та використання системи електронного урядування необхідним є вирішення складних проблем щодо її технічного обслуговування та інформаційної безпеки.

Висновки та перспективи подальших досліджень. Глобалізаційні процеси, в умовах яких існує сучасне українське суспільство, кидають нові виклики до існуючої системи публічного управління та адміністрування в аспекті її захищеності. Внутрішні суперечності як на рівні інформаційного, технічного та організаційного забезпечення систем електронного урядування стикаються із додатковими труднощами невідповідності закордонним механізмам захисту та провадження.

Складність і різнорідність програмного та апаратного забезпечення, що використовують у процесах публічного як вітчизняного, так і закордонного адміністрування; наявність в системах електронного урядування потужної розгалуженості вузлів комутації широких мас користувачів та зовнішнього доступу до таких систем, як і складнощі у функціональному поділі обов'язків різних груп обслуговуючого їх персоналу, спричиняють нагальну потребу у розробленні на теренах українського інформаційного простору уніфікованої системи публічного адміністрування, впорядкованої за загальними принципами європейських стандартів.

Визначення протидії загрозам безпеки в інформаційних системах становить комплексну проблему, для вирішення якої необхідно поєднання заходів на законодавчому, адміністративному, процедурному і

програмно-технічному рівнях інформаційної безпеки.

Упровадження нормативно-правових актів у напрямку безпечного публічного адміністрування дозволить захищене використання інформаційно-комунікаційних технологій, доступ до інформації, її захист від несанкціонованого доступу та витоку технічними каналами.

На адміністративному рівні захисту інформації в системі публічного управління вирішується визначення керівних документів і стандартів, підходів до управління ризиками та сертифікація на відповідність стандартам інформаційної безпеки.

Іншим рівнем для забезпечення захисту у процесах електронного урядування є процедурний, що регламентує відповідні організаційні заходи. Важливим аспектом процедурного та програмного рівнів протидії загрозам інформаційної безпеки у таких процесах є формування політики безпеки, яка в

організаціях, підключених до систем електронного урядування, є сукупністю принципів, правил, процедур і практичних рішень у галузі інформаційної безпеки, які регулюють керування, захист та розподіл інформації, що захищається.

Список використаної літератури:

1. Закон України «Про інформацію» від 02.10.1992 р. № 2657- XII, із змінами. – Режим доступу: zakon2.rada.gov.ua/laws/ show/2657-12.
2. Закон України «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» від 09.01.2007 №537-16 // [Електронний ресурс] – Режим доступу: http://zakon2.rada.gov.ua/laws/show/537- 16.
3. Закон України «Про Національну програму інформатизації» від 01.08.2016р. № 74/98-ВР. // [Електронний ресурс] – Режим доступу: http://zakon2.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80.
4. Закон України «Про електронні документи та електронний документообіг» від 22.05.03 № 851-IV // [Електронний ресурс] – Режим доступу: http://sfs.gov.ua/diyalnist-/zakonodavstvo-pro-diyalnis/zakoniukraini/53715.html.
5. Закон України «Про електронний цифровий підпис» від 22.05.2003 № 852-IV // [Електронний ресурс] – Режим доступу: http://zakon0.rada.gov.ua/laws/show/852-15.
6. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР // [Електронний ресурс] – Режим доступу: http://zakon2.rada.gov.ua/laws/show/80/94- %D0%B2%D1%80.
7. Положення про технічний захист інформації в Україні: Указ Президента України від 27.09.1999 р. № 1229/99. – Режим доступу: zakon3.rada.gov.ua/laws/show/1229/99. – Назва з екрану.
8. Концепція технічного захисту інформації в Україні: постанова Кабінету Міністрів України від 08.10.1997 р. № 1126, із змінами. – Режим доступу: zakon3. rada.gov.ua/laws/show/1126-97-п. – Назва з екрану
9. Хошаба О. М. Електронне урядування та електронна демократія: навч. посіб.: у 15 ч. / за заг. ред. А. І. Семенченка, В. М. Дрешпака. – Частина 13: Захист інформації в системах електронного урядування. – К. : ФОП Москаленко О. М., 2017. – 72 с.
10. Азарова А. О. Електронний цифровий підпис як засіб захисту інформації на вітчизняних підприємствах / А. О. Азарова, Роїк О. М., Года К. О. / Збірник наукових праць «Економічний простір». – № 60. – Дніпропетровськ: ПДАБА, 2012. – С.258–263.
11. Азарова А. А. Электронная цифровая подпись как средство защиты информационной модели предприятия / А. А. Азарова, К. В. Ивчук, М. И. Кукуруза // Экономика, социология и право : журнал научных публикаций. – Москва : Изд-во «Спецкнига». – № 2. – 2014. – С.7–9.
12. Азарова А. О. Управління та адміністрування захистом інформації шляхом локалізація закладних пристроїв на основі індикатора електромагнітних випромінювань [Електронний ресурс] / А. О. Азарова, В. О. Гудзь, В. О. Блонський // Матеріали XLVIII науково-технічної конференції підрозділів ВНТУ, Вінниця, 13-15 березня 2019 р. – Електрон. текст. дані. – 2019. – Режим доступу: https://conferences.vntu.edu.ua/index.php/all-fm/all-fm-2019/paper/view/7335.
13. Азарова А. О. Управління інформаційною безпекою в державних установах на основі біометричної аутентифікації відбитків пальців для захисту інформації від несанкціонованого доступу [Електронний ресурс] / А. О. Азарова, В. О. Гудзь, В. О. Блонський // Матеріали XLVIII науково-технічної конференції підрозділів ВНТУ, Вінниця, 13-15 березня 2019 р. – Електрон. текст. дані. – 2019. – Режим доступу: https://conferences.vntu.edu.ua/index.php/all-fm/all-fm-2019/paper/view/7429.
14. Азарова А. О. Електронні засоби політики інформаційної безпеки на державних підприємствах [Електронний ресурс] / А. О. Азарова, В. Ф. Хісматулліна // Матеріали XLVIII науково-технічної конференції підрозділів ВНТУ, Вінниця, 13-15 березня 2019 р. – Електрон. текст. дані. – 2019. – Режим доступу: https://conferences.vntu.edu.ua/index.php/all-fm/all-fm-2019/paper/view/6889.
15. Азарова А. О. Метод захисту процесів електронного урядування шляхом квантування [Електронний ресурс] / А. О. Азарова, Я. В. Чайковська // Матеріали XLVIII науково-технічної конференції підрозділів ВНТУ, Вінниця, 13-15 березня 2019 р. – Електрон. текст. дані. – 2019. – Режим доступу: https://conferences.vntu.edu.ua/index.php/all-fm/all-fm-2019/paper/view/7946.
16. Азарова А. О. Розробка методики визначення економічної безпеки підприємства / А. О. Азарова, О. В. Гаврилова // Збірник наукових праць «Економіка: проблеми теорії та практики». – Дніпропетровськ : ДНУ, 2004. – Вип. 191, Т. ІІІ. – С. 719–727.

References:

1. Zakon Ukrai'ny (1992), ««Pro informaciju», 02.10.1992 r. № 2657-XII, iz zminamy», available at: zakon2.rada.gov.ua/laws/ show/2657-12, (accessed 20.03.2019).
2. Zakon Ukrai'ny (2007), ««Pro osnovni zasady rozvytku informacijnogo suspil'stva v Ukrai'ni na 2007–2015 roky», 09.01.2007 №537-16», available at: http://zakon2.rada.gov.ua/laws/show/537- 16, (accessed 20.03.2019).
3. Zakon Ukrai'ny (2016), ««Pro Nacional'nu programu informatyzacii'», 01.08.2016 r. № 74/98-VR», available at: http://zakon2.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80, (accessed 20.03.2019).
4. Zakon Ukrai'ny (2003), ««Pro elektronni dokumenty ta elektronnyj dokumentoobig» vid 22.05.2003 № 851-IV», available at: http://sfs.gov.ua/diyalnist-/zakonodavstvo-pro-diyalnis/zakoniukraini/53715.html, (accessed 20.03.2019).
5. Zakon Ukrai'ny (2003), ««Pro elektronnyj cyfrovyj pidpys», 22.05.2003 № 852-IV», available at: http://zakon0.rada.gov.ua/laws/show/852-15, (accessed 20.03.2019).
6. Zakon Ukrai'ny (1994), ««Pro zahyst informacii' v informacijno-telekomunikacijnyh systemah», 05.07.1994 № 80/94-VR, available at: http://zakon2.rada.gov.ua/laws/show/80/94- %D0%B2%D1%80, (accessed 20.03.2019).

7. Ukaz Prezydenta Ukrai'ny (1999), «Polozhennja pro tehnichnyj zahyst informacii' v Ukrai'ni, 27.09.1999 r. № 1229/99» available at: zakon3.rada.gov.ua/laws/show/1229/99, (accessed 20.03.2019).
8. Postanova Kabinetu Ministriv Ukrai'ny (1997), «Koncepcija tehnichnogo zahystu informacii' v Ukrai'ni, 08.10.1997 r. № 1126, iz zminamy», available at: rada.gov.ua/laws/show/1126-97-p, (accessed 20.03.2019).
9. Hoshaba, O.M. (2017), «Zahyst informacii' v systemah elektronnogo urjaduvannja», in Semenchenka, A.I., Dreshpaka V.M. (Ed.), *Elektronne urjaduvannja ta elektronna demokratija*, FOP Moskalenko O. M., Kyi'v, 72 p.
10. Azarova, A.O., Roi'k O.M. and Goda K.O. (2012), «Elektronnyj cyfrovyj pidpys jak zasib zahystu informacii' na vitchyznjanyh pidpryjemstvah», *Zbirnyk naukovyh prac' «Ekonomichnyj prostir»*, vol 60, pp. 258-263.
11. Azarova, A. A., Yvchuk K.V. and Kukuruza M.Y. (2014). «Эlektronnaja cyfrovaja podpys' kak sredstvo zashhyty ynformacyonnoj modely predpryjatyja», *Эkonomyka, socyologyja y pravo : zhurnal nauchnыh publykacyj*, vol 2, pp. 7–9.
12. Azarova, A.O., Gudz', V.O. and Blons'kyj, V.O. (2019), «Upravlinnja ta administruvannja zahystom informacii' shljahom lokalizacija zakladnyh prystroi'v na osnovi indykatora elektromagnitnyh vyprominjuvan'», *Materialy XLVIII naukovo-tehnichnoi' konferencii' pidrozdiliv VNTU*, March 13-15, 2019, Vinnycja, available at: https://conferences.vntu.edu.ua/index.php/all-fm/all-fm-2019/paper/view/7335, (accessed 23.03.2019).
13. Azarova, A.O., Gudz', V.O. and Blons'kyj, V.O. (2019), «Upravlinnja informacijnoju bezpekoju v derzhavnyh ustanovah na osnovi biometrychnoi' autentyfikacii' vidbytkiv pal'civ dlja zahystu informacii' vid nesankcionovanogo dostupu», *Materialy XLVIII naukovo-tehnichnoi' konferencii' pidrozdiliv VNTU*, March 13-15, 2019, Vinnycja, available at: https://conferences.vntu.edu.ua/index.php/all-fm/all-fm-2019/paper/view/7429, (accessed 23.03.2019).
14. Azarova, A.O. and Hismatullina V.F. (2019), «Elektronni zasoby polityky informacijnoi' bezpeky na derzhavnyh pidpryjemstvah», *Materialy XLVIII naukovo-tehnichnoi' konferencii' pidrozdiliv VNTU*, March 13-15, 2019, Vinnycja, available at: https://conferences.vntu.edu.ua/index.php/all-fm/all-fm-2019/paper/view/6889, (accessed 23.03.2019).
15. Azarova, A.O. and Chajkovs'ka, Ja.V. (2019), «Metod zahystu procesiv elektronnogo vrjaduvannja shljahom kvantuvannja», *Materialy XLVIII naukovo-tehnichnoi' konferencii' pidrozdiliv VNTU*, March 13-15, 2019, Vinnycja, available at: https://conferences.vntu.edu.ua/index.php/all-fm/all-fm-2019/paper/view/7946, (accessed 23.03.2019).
16. Azarova, A.O. and Gavrylova, O.V. (2004), «Rozrobka metodyky vyznachennja ekonomichnoi' bezpeky pidpryjemstva», *Zbirnyk naukovyh prac' «Ekonomika: problemy teorii' ta praktyky»*, vol 191, pp 719-727.

Азарова Анжеліка Олексіївна – кандидат технічних наук, професор, заступник декана Факультету менеджменту та інформаційної безпеки з наукової роботи та міжнародного співробітництва Вінницького національного технічного університету

Наукові інтереси:
- захищені засоби публічного управління та адміністрування;
- публічне управління на основі СППР та математичного моделювання.

ORCID: 0000-0003-3340-5701

Ткачук Людмила Миколаївна – кандидат економічних наук, доцент, заступник декана Факультету менеджменту та інформаційної безпеки з навчально-методичної роботи Вінницького національного технічного університету

Наукові інтереси:
- захищені засоби публічного управління та адміністрування;
- регіональні аспекти публічного управління та адміністрування.

ORCID: 0000-0001-9770-7851

Нікіфорова Лілія Олександрівна – кандидат економічних наук, доцент, вчений секретар факультету менеджменту та інформаційної безпеки Вінницького національного технічного університету

Наукові інтереси:
- електронні засоби публічного управління та адміністрування.

ORCID: 0000-0002-7034-607X

Шиян Анатолій Антонович – кандидат фізико-математичних наук, професор кафедри менеджменту та безпеки інформаційних систем факультету менеджменту та інформаційної безпеки Вінницького національного технічного університету.

Наукові інтереси:
- електронні засоби публічного управління та адміністрування.

ORCID: 0000-0002-5418-1498

Хошаба Олександр Мирославович – кандидат технічних наук, доцент, старший науковий співробітник Інституту проблем математичних машин та систем Національної академії наук України.

Наукові інтереси:
- захищені засоби публічного управління та адміністрування;
- продуктивність обчислювальних систем

ORCID: 0000-0001-5375-62809

Стаття надійшла до редакції 29.03.2019.