Кудрявцев О. Ю., канд. політ. наук, доц.,
Харківський національний університет міського господарства імені О. М. Бекетова, Україна

ТРАНЗИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ВІД ЛОКАЛЬНОСТІ ДО МІЖНАРОДНОГО СПІВРОБІТНИЦТВА У СФЕРІ Е-УРЯДУВАННЯ

Повсякчасно сьогодні як держава так і приватний сектор стикаються з величезною кількістю інформаційних загроз. Враховуючи критичну значущість інформації у сучасних соціально-політичних процесах, інформаційна безпека безпосередньо пов'язана з рівнем довіри громадян до політичної влади, її можливостями адекватно протистояти інформаційним загрозам сучасності. Тож інформаційна безпека є ключовим компонентом типових державних ІС.

Інформаційна залежність «Digital Dependence» пов'язана з поширенням технологій та загальною технологічністю держави, складністю відкритих мереж передачі даних, а також загальновизнаною необхідністю забезпечення доступу громадян до інформації, в тому числі й такої, що може представляти комерційний та інші інтереси призвели до того, що ефективне управління інформаційною безпекою стала одним з найважливіших чинників успіху для державних і приватних організацій [1]. Розробка вимог та принципів ефективності управління інформаційною безпекою є необхідною умовою впровадження системи ЕУ, з метою підвищення конкурентоспроможності державних ІС, та як наслідку, підвищення рівня довіри громадян до політичної влади та конкретних політичних інститутів.

Можна прослідкувати певні закономірності у забезпеченні інформаційної безпеки базових світових моделей систем ЕУ. Проте, коли йдеться про захист безпосереднього програмного забезпечення, потрібно враховувати конкретні культурні та економічні особливості. Отже, незважаючи на узагальнений характер проблеми інформаційної безпеки, з точки зору легітимації політичної влади, її доцільно розглядати на конкретних прикладах.

Наявні дослідження демонструють зв'язок між питаннями безпеки, ЕУ та інформаційною безпекою держави загалом. [2]; [3]; [4]. Причому не меншою значущістю охарактеризовані й проблеми матеріально-технічного забезпечення діяльності ЕУ [5]. Існує велика кількість досліджень, пов'язаних із нетехнічними аспектами гарантування інформаційної безпеки державного середовища [6]. На нашу думку, у наявній відкритій літературі з приводу організаційної на національної інформаційної культури приділяється недостатньо уваги, враховуючи величезний контраст у рівні обізнаності громадян з питанньінформаційної безпеки та її ролі у забезпеченні стабільного розвитку держави та суспільства.

Отже, важливим питанням залишається аналіз концептуальних основ інформаційної безпеки, та їх вплив на рівень легітимності політичної влади. Концептуальною основою ЕУ є забезпечення доступу до державних послуг в будь-якому місці в будь-який час через відкриті мережі. Це потенційно може призвести до величезних проблем безпеки та конфіденційності у сфері

управління ІС, особливо враховуючи той факт, що управлінські процеси у державному секторі мають суттєві відмінності від аналогічних процесів у сфері приватного партнерства та виробництва.

Інформаційна безпека, з одного боку, виступає частиною концепції ЕУ, з іншого, – є значно ширшим поняттям, яке з'явилося набагато раніше досліджуваного нами явища. Питання інформаційної безпеки, що тим чи іншим чином стосуються легітимації політичної влади, можуть бути розподілені на чотири великі групи. ЕУ, як вже неодноразово наголошувалося, тут виступає у своїх інструменталістських проявах, як модель організації взаємодії держави, громадян та бізнесу на основі використання можливостей ІКТ [7]. Концептуальні основи інструменталізму як принципу відношення до ЕУ були закладені ще у середині двотисячних років [8].

Теоретична модель базується на усвідомленні критичності зв'язків між центральними владними установами та окремими користувачами, як суб'єктами політичного процесу, через що й проявляється її суб'єктність. Причому як технічні технічних так і організаційні питання повинні бути розглянуті паралельно при інтеграції державних інформаційних систем у єдину гіпер-мережу.

У зв'язку з цим часто звучить питання інформаційної безпеки транзакцій, забезпечення недоторканості особистих даних [9]. Через специфіку процесів в системі державного управління, моделі інформаційної безпеки повинні корелюватися з самим принципами організації цієї системи [10].

Слід зазначити, що, насправді, сама ідея ЕУ стала основним джерелом питань інформаційної безпеки у зв'язку поняттями відкритості та доступності важливих даних.

Другим важливим напрямом організації інформаційної безпеки виступають принципи управління інформацією в державному секторі, та їх трансформація з огляду на використання новітніх технологій та реальних можливостей підвищення рівня довіри громадян до політичної влади. Управління інформацією в державному секторі пов'язане з ризиками, що виникають у процесі надання державної інформації зовнішнім клієнтам. Враховуючи той факт, що уряди діють в іншому середовищі, ніж приватні організації вони, вимагають різних підходів. Питання суттєвості відмінностей інформаційних процесів у державному середовищі вже потрапляло до уваги дослідників [11]. Ними були запропоновані основі особливості, в саме: державний сектор характеризується відсутністю ринкових принципів, орієнтації на кінцевий результат, продукції. Державні асигнування знищують найменші прояви конкуренції. Така залежність створює потенційні умови для фактично необмеженого політичного впливу. У зв'язку з чим постає питання додаткових форм контролю та звітностей, які не є притаманним для приватного сектору [12]. Державне управління інформаційних системи відрізняється від звичайних ІС управління орієнтованістю на фактори навколишнього середовища, а не внутрішні характеристики організації [13]. Саме тому моделі ІС, що діють у приватному секторі, не є достатніми для впровадження секторі державного управління [14].

Організації державного сектора мають ряд специфічних особливостей, які можуть вплинути на інформаційну безпеку як таку. Перш за все маються на увазі: жорсткі ієрархії; культура; раптові зміни політичного курсу; феномени перекривання ініціатив; досить широкий спектр діяльності; специфічний персонал, через певні умови його підготовки.

Означені вище характеристики призводять до унікальності форм угод між державними організаціями та громадянами. Ще однією важливою особливістю є те, що державний сектор дуже чутливий до будь-яких компрометацій інформаційної безпеки. Хоча такі інциденти можуть бути безпосередньо не пов'язані з ЕУ, вони можуть мати потенційно негативний вплив на функціонування останнього, що в свою чергу може призвести до кризи легітимності та появи делегітимаційних явищ.

Еволюція усвідомлення критичної важливості інформаційної безпеки для суспільного та державного розвитку може бути умовно розділена на ряд стадій [15]. Хоча еволюційна модель була розроблена для розвинутих країн вона є на сьогодні корисним інструментом для аналізу розвитку ІКТ у країнах що розвиваються.

Кожна хвиля описує загальний підхід до інформаційних технологій та їх управління для певного проміжку часу. Концептуальні засади еволюції інформаційно комунікативних технологій та їх роль у менеджменті державних процесів можуть виступати сьогодні цінним інструментом оцінки зрілості ІС країн що розвиваються, побудови індексів готовності до системи ЕУ. Інформаційна безпека традиційно ґрунтується на засадах конфіденційності, цілісності та доступності. Ці властивості лежать в основі таких послуг, як аутентифікація користувача, авторизація, підзвітність та моніторинг надійності. Роботи, які стосувалися трансформації ролі інформаційної безпеки постійно з'являлися у світовій науковій думці [16].

У найбільш широкому сенсі інформаційна безпека завжди спирається на дві складові: людей, а також технології. Публікації стосовно цієї тематики ми об'єднуються під загальним напрямом організаційної культури безпеки [17]. Стандарти інформаційної безпеки широко представлені у відкритій літературі [18]. Ці стандарти намагаються описати різні процеси і елементи управління, необхідні для успішної реалізації політики інформаційної безпеки [19]. В цілому ці стандарти були розроблені на основі досвіду провідних за технологіями країн.

І нарешті один з основних аспектів при аналізі потенційних можливостей легітимації політичної влади за допомогою впровадження системи ЕУ може бути умовно названий як суспільний контекст, або культурні та соціально-економічні особливості того чи іншого суспільства.

Мається на увазі є особливості країни, де явище розгорнуте і працює. За загальною класифікацією країною, що розвивається, як правило, вважають ту , яка має душу населення валовий національний продукт менше 2000 доларів США [20]. Майже 80% населення у світі живе в країнах, що розвиваються. Проте це не означає, що всі вони мають однакові проблеми на шляху до е-готовності. Кожна країна має свою унікальну атмосферу, політичні та

економічні обмеження. І саме ці особливості і будуть диктувати різноманітні обмеження на впровадження означеної системи та її реальні можливості по підвищенню рівня довіри громадян до політичної влади.

В деяких випадках можна зустріти і контраргументи, що нібито, якби було менше ініціатив у сфері е-демократизації та створення е-готовності, було б значно менше проблем з порушенням конфіденційності та недоторканості персональних даних [20]. Тому необхідно мати чітке уявлення про культурні аспекти, які охоплюють як організаційні та національної особливості загального контексту, в якому ЕУ функціонує або планується.

Згідно з наявними даними 35% програм у сфері ІКТ, серед яких і ЕУ в країнах, що розвиваються, визнані безуспішними та класифікуються як загальні невдачі і 50% визнані частково впровадженими [240]. Безпека завжди була визначена в якості одного з важливих компонентів ІС. Сучасний менеджмент інформаційного забезпечення визнає за необхідне, широке включення максимальної кількості людей і процесів до розробки питань технології безпеки. В значній мірі технологічні рішення для більшості проблем безпеки були розроблені раніше. Однак, є ще багато проблем у сфері програмного забезпечення, людей і процесів управління компонентами, забезпечення безпеки інформації. Це все обумовлює необхідність наявності не лише технологічних, а й соціокультурних аспектів у теоретичних моделях систем ЕУ країн що розвиваються.

ІКТ в країнах, що розвиваються, як правило, недостатньо описані загальнодоступною не технічною мовою у загальнодоступній літературі. Враховуючи виключне значення ІТ, зокрема, ЕУ для країн, що розвиваються, актуальність їх потреб, часто пов’язаних з недоліком власних економічних ресурсів, вельми корисним для розуміння сутності проблем є національно-культурні фактори. Проте, існує досить невелика кількість опублікованих емпіричних досліджень, які безпосередньо стосуються цього питання. Згадані аспекти пов’язують концепцію ЕУ та інформаційної безпеки у ширшому контексті з соціально-організаційною теорією. [21]. Концепція соціально-технічного детермінізму будується на припущенні, що розвиток ІС включає в себе велику частину погоджувальної роботи, де ІС повинна бути сумісна з навколишнім середовищем (стандарти інтероперабельності) [22]. Це означає, що соціально-технічна модель повинна об’єднати функції ІС, профілі користувача і формат навколишнього середовища, водночас як технічні та організаційні системи є однаково важливими і відсутність відповідності між соціальними і технічними системами є основною причиною проблем ІС [23].

З точки зору легітимації політичної влади цікавими є кілька моделей інформаційної безпеки в які представлені в літературі, та спираються на концепції соціально-технічного детермінізму. Модель безпеки на основі консенсусу запропонував Дікард [24]. Сутність її полягає у намаганні поєднати соціально-технічні системи, забезпечивши юзабіліті дизайну ІС. Дослідники стверджують, що система управління інформаційною безпекою складається з багатьох аспектів, таких як політичні рішення, стандарти, керівні принципи, норми і правила, технології, людські ресурси, правові та етичні питання.

Для того, щоб визначити ключові фактори інформаційної безпеки в громадських контекстах, має бути присутня концептуальна основа, що допомагає класифікувати фактори і зрозуміти, їх важливість для навколишнього середовища. Сукупний аналіз запропонованої у світовій політичній думці системи аналізу базується на чотирьох аспектах, а саме: власне концепції ЕУ, теорії управління інформаційною безпекою, управління інформаційними технологіями у державному секторі, а також контекстах суспільств. Ґрунтуючись на Вергез, можна виділити чотири компоненти, які суттєво впливають на інформаційну безпеку державної електронної системи: культура безпеки, культура управління, інфраструктури інформаційної безпеки та технології управління змінами [25].

Концептуально ми маємо говорити про взаємозв'язок між ефективністю безпеки системи ЕУ з точки зору основних критеріїв (наявність, цілісність, конфіденційність та звітності) і структурними особливостями компонентів, таких як культура безпеки, управлінські та інформаційна інфраструктура. Ці взаємопов'язані елементи виступають у якості пропозицій, які можуть представити розвинуті країни тим, що розвиваються.

Одним з елементів, що пов'язує інформаційну безпеку, рівень довіри громадян до політичної влади та культурні особливості конкретного соціуму є поняття культури безпеки.

Культура безпеки являє собою певне ставлення до принципів організації безпечного інформаційного середовища. Нормативне втручання особливо важливе при розробці правил використання і захисту інформаційних активів. Ці фактори впливають на формат законодавчих і нормативних рамок, а також національних і організаційних культур.

У деяких дослідженнях культура безпеки була віднесена до структури національної культури [26], тоді як в інших було особлива увага приділяється організаційним формам культури безпеки, як самостійним елементам [22]. Практичні навички інформаційної безпеки в організаційній культурі позитивно позначаються на щоденних операціях, і відповідно мають позитивний вплив на усю організацію. Важливим є також зв'язок організаційної та національної культури. Відмінності в національній культурі можна пояснити відмінностями в ефективності управління інформаційною безпекою на організаційному рівні визначили п'ять аспектів національної культури: дистанція влади, уникнення невизначеності, індивідуалізм, маскулінність і орієнтація часу. Фріман прийшов до висновку, що національна культура мала значний вплив на те, як сприймались суспільством новітні технології, яким саме чином вони використовувалися і адаптувалися [27]. Наприклад, національні культури розвинених країн, таких як Австралія, Сполучені Штати і Великобританія мають багато схожого в питаннях інформаційної безпеки з країнами, що розвиваються, такими, як у Перській затоці (Саудівська Аравія, Бахрейн, Кувейт, Катар ОАЕ і Оман), що може корелюватися з культурними відмінностями [28]. Країни, що розвиваються, стикаються з культурними і соціальними перешкодами при спробі трансферу та адоптації технології, створеної за кордоном, у себе вдома [29].

Д. Томпсон стверджував, що соціально-культурне середовище в країнах, що розвиваються, в порівнянні з розвиненими країнами, є відносно стабільним у питаннях уникнення невизначеності та дистанції влади, і відносно низькому рівні індивідуалізму. Ці фактори, як правило, підсилюють прагнення до впровадження до ІКТ у країнах, що розвиваються [30].

Отже, сучасні погляди на легітимацію політичної влади за допомогою впровадження систем ЕУ виходять з наступного:

- громадянська організаційна культура може мати вплив на ефективність та безпеку ЕУ;
- національна культура має безпосередній вплив на ефективність та безпеку ЕУ.

Вагоме значення для легітимації політичної влади має також нормативне забезпечення та законодавча база організації безпеки системи ЕУ. Закони мають стати основою для забезпечення належного рівня дотримання міжнародних норм і домовленостей. Підвищений попит з боку суспільства на захист приватного життя та персональних даних змусило провідні країни, наприклад, розробляти свої власні закони про приватне життя [31].

Залишається ще багато нерозглянутих питань щодо наявності відповідного законодавства, пов'язаного з управлінням інформаційною безпекою, прийняттям законів, які криміналізують кібератаки і дозволяють правоохоронним органам адекватно розслідувати та переслідувати в судовому порядку такі дії. Крім того, багато країн не мають відповідного законодавства у сфері захисту приватного життя, які були б покликані перешкоджати різноманітним зловживанням, потенційно можливим при наявності в державі системи ЕУ. Незважаючи на технологічність та інноваційність такої системи, на жаль, можливості для означених зловживань знаходяться з насторожливою періодичністю. Тобто, мова йде про те, що багато країн, що розвиваються фактично не мають дієвого інструментарію та суттєво обмежені у вживанні заходів проти порушників з метою не лише захисту своїх інформаційних активів, а також запобіганню використання інформаційної мережі своєї країни в якості бази для виконання незаконної діяльності в глобальному масштабі. Цей вид загроз є основним питанням у еру інформації, що представляє ще одну фундаментальну відмінність між країнами, що розвиваються, і розвиненими країнами з погляду існування і відсутності необхідних норм і законів, здатних забезпечити більш високий рівень відповідності.

Забезпечення недоторканості даних також залежить від правил управління, відповідальності, обізнаності та прихильності вищого керівництва і користувачів, до відповідних політик. Ці фактори залежать від цілого ряду питань, таких, як наявного бюджету, стандартів управління інформаційною безпекою та кваліфікацією персоналу.

Держава, так само як і приватні організації можуть уникнути втрат, пов'язаних з порушеннями інформаційної безпеки, якщо більш відповідально ставитимуться до наявних реальних інформаційних загроз. Організаційна свідомість є складовим елементом організаційної культури, проявляється на управлінському рівні в якості основних детермінант організаційної

прихильності. Ключ до успіху в процесі планування зобов'язань, полягає у контексті об'єктивних умов. Ефективний розвиток програми інформаційної безпеки здійснюється на основі договірних відносин між зацікавленими сторонами організації (керівництво, технічний персонал, користувачі, треті особи). Для того, щоб визначити ефективні методи реалізації управління інформаційною безпекою, важливо, щоб всі зацікавлені сторони зробили свій внесок у програму інформаційної безпеки. Адекватна політика, чітко визначені цілі, процедури, процеси, обов'язки є пріоритетними напрямками співробітництва для усіх зацікавлених сторін. Завдяки цьому існує можливість на ранніх етапах уникнути неузгодженості дій.

У багатьох країнах, що розвиваються, нині, як і раніше існує необхідність покладати більше зусиль щодо політики у сфері розвитку ІКТ. Наприклад, відсутність політики безпеки у сфері ІКТ та її практичних впроваджень розглядається в якості однієї з основних причин фрагментації правил і процедур основних програм інформаційної безпеки. Це дозволяє припустити, що ймовірність порушення інформаційної безпеки може бути більша в країнах, що розвиваються, де спостерігається низький рівень організаційної культури.

СПИСОК ДЖЕРЕЛ

1. Ковалевський В. Інформаційна демократія як політична категорія / В. Ковалевський // Наукові записки Інституту політичних і етнонаціональних досліджень імені І. Ф. Кураса НАН України. – К. : Інститут політичних і етнонаціональних досліджень імені І. Ф. Кураса НАН України, 2003. – Вип. 22. – С. 214 – 222.
2. West D. M. State and Federal E-government in the United States [Електронний ресурс]. / Darrell West // Taylor Nelson Sofres. – 2006. – Режим доступу : www.InsidePolitics.org/egovetdata.html.
3. Yan L. Exploring success factors for web-based e-government services: behavioral perspective from end users / L. Yan, Y. Chen, C. Zhou. // Information and Communication Technologies, 2006. – №1. – С. 937–942.
4. Zhao J. ICT4D: internet adoption and usage among rural users in China / Jinqiu Zhao. // Knowledge, Technology and Policy, 2008. – №21. – С. 9–18.
5. Yao M. K. The Digital Divide Still An Issue [Електронний ресурс]. / Marc Kouadio Yao // University of Regensburg, 2007. – Режим доступу : http://epub.uni-regensburg.de/10713/1/The_Digital_Divide_Still_An_Issue.pdf.
6. Vandenberg A. Citizenship and Democracy in a Global Era / Andrew Vandenberg. – New York : St. Martins Press, 2000. – 887 с.
7. Tsagarousianou R. Cyberdemocracy: Technology, Cities, and Civic Networks / R. Tsagarousianou, T. Damian, B. Cathy. – London and New York: Routledge, 1998. – 324 с.
8. Thierer A. D. How Free Computers are Filling the Digital Divide / Adam Thierer. – New York : The Heritage Foundation Backgrounder, 2000. – 225 с.
9. The New E-Government Equation [Електронний ресурс] // Council for Excellence in Government. – 2003. – Режим доступу : www.excelgov.org
10. Ozaltinordu G. From digital divide to use-divide. [Електронний ресурс]. / Gultekin Ozaltinordu // International Trade Center, 2006. – Режим доступу : http://www.digitaldivide.net/articles/view.php?ArticleID=548.
11. Todd L. Webbing Governance: Global Trends Across National-Level Public Agencies / L. Todd, D. Chris, C. Friis. // Communications of the ACM, 2001. – №44. – С. 63–67.
12. Servon L. J. Bridging the Digital Divide: Technology, Community, and Public Policy / Lisa J. Servon. – Malden : Blackwell Publishers, 2002. – 520 с.

13. Schlosberg D. Digital democracy: Authentic or virtual? / D. Schlosberg, J. S. Dryzek. // Organization and Environment, 2002. – №3. – С. 332–337.

14. Riley T. Electronic Governance: Living and Working in the Wired World. / T. Riley. – New York : Oxford University Press, 1999. – 148 с. 279

15. Pateman C. Participation and Democratic Theory / Carole Pateman. – London : Cambridge University Press, 1970. – 228 с.

16. Bimber B. The Internet and citizen communication with government: does the medium matter. The Political Communication / B. Bimber – [Електронний ресурс]. – Режим доступу: https://www.researchgate.net/publication/231381849_The_Internet_and_Citizen_Communication._With_Government_Does_the_Medium_Matter

17. Carter L. The utilization of e-government services: citizen trust, innovation and acceptance factors [Електронний ресурс] / L. Carter // Blackwell Publishing Ltd, 2005. – Режим доступу : http://csel.eng.ohio-state.edu/productions/intel/research/trust/utilization%20of%20e-government%20services.pdf

18. Badri M. A. A path analytic model and measurement of the business value of e-government: and international perspective [Електронний ресурс] / M. A. Badri, K. Alshare // International Journal of Information Management, 2008. – Режим доступу : http://www.sciencedirect.com/science/article/pii/S0268401208000133

19. Babbie E. R. The Practice of Social Research / Earl Babbie. – Belmont : Wadsworth, 1989. – 624 с.

20. ClickZ Stats Staff. E-Government May Not Mean Efficiency [Електронний ресурс]. – Режим доступу : http://www.clickz.com/clickz/news/1703726/e-government-may-not-mean-efficiency

21. Cooper T. Citizenship and Professionalism in Public Administration. Public Administration Review / T. Cooper. // Public Administration Review. – 76. – №66. – С. 76–88.

22. Curtin G. The World of E-Government / G. Curtin, M. Sommer, V. Vis-Sommer. – Binghamton, New York: Haworth Press, 2004. – 255 с.

23. De Leon P. Democracy and the Policy Sciences. / Peter De Leon. – Albany : State University of New York Press, 1997. – 270 с.

24. Dickard N. Federal Retrenchment on the Digital Divide: Potential National Impact / Norris Dickard. — Washington, DC : Benton Foundation, 2002. – 470 с. – (Policy Brief No. 1).

25. Електронна демократія: сподівання та проблеми / Джоан Кедді, Крістіан Вергез [та ін.] ; [пер. з англ. С. Соколик, О. Оржель, К. Гомма]. – К. : Центр адаптації державної служби до стандартів Європейського Союзу, 2009. – 164 с.

26. Еноксен Дж.-А. Що таке електронний уряд? [Електронний ресурс] / Дж.-А. Еноксен // Матеріали проекту «Розбудова демократії та можливостей державної служби в Україні». – Режим доступу : http://www.google.com.ua/url?url=http://derzhava.in.ua:8081/egov/Shared%2520Documents/E-Government_01.doc&rct=j&q=&esrc=s&sa=U&ei=ISFXVfrGKIassgHCuYDACw&ved=0CBMQFjAA&sig2=WEbUt8k3BWSzR3cvdI2dJQ&usg=AFQjCNGGzjBhD00-3WrZe-A4RbW8DJp-iw.

27. Ferdinand P. The Internet, Democracy, and Democratization / Peter Ferdinand. — London and Portland : Frank Cass, 2000. – 365 с.

28. Grossman L. K. The Electronic Republic: Reshaping Democracy in the Information Age / Lawrence Grossman. – New York : Viking, 1995. – 152 с.

29. Hague B. Digital Democracy: Discourse and Decision Making in the Information Age / B. Hague, B. Loader. – London and New York : Routledge, 1999. – 258 с.

30. Thompson D. V. The business value of e-government for small firms / D. V. Thompson, R. T. Rust, J. Rhoda. // International Journal of Service Industry Management, 2005. – №16. – С. 385–407.

31. Європейська Хартія місцевого самоврядування / Страсбург, 15 жовтня 1985 р. : Хартію ратифіковано Законом № 452/97-ВР від 15.07.1997. [Електронний ресурс]. – Режим

доступу : http://zakon1.rada.gov.ua/laws/show/994_036.

Луб А. І., аспірант, УФЕБ
Харківський національний університет міського господарства ім. О. М. Бекетова, Україна

СИСТЕМА ФІНАНСОВОЇ БЕЗПЕКИ ПІДПРИЄМСТВА ЯК СПОСІБ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ МІСТА

Розгляд поняття «система фінансової безпеки підприємства», як одного із можливих способів забезпечення безпеки міста.

В основі побудови системи фінансової безпеки кожного підприємства знаходиться цілком індивідуальний підхід. Об'єм та дієвість такої системи визначаються прийнятою на території певної держави законодавчою базою, обсягом наявних матеріально-технічних та фінансових ресурсів підприємства, розповсюдження серед працівників інформації щодо значення сприяння безпеці бізнесу, а також від досвіду роботи та кваліфікації керівного складу служби безпеки підприємств.

Так, згідно з визначенням, запропонованим Т. В. Ганущак, система фінансової безпеки підприємства включає комплекс зовнішніх та внутрішніх суб'єктів сприяння фінансовій безпеці суб'єкта господарювання, що базуються на єдиних задачах, цілях, методах, організаційно-правовому та фінансово-економічному забезпеченні, єдиній політиці та визначених організаційною структурою та кадровим забезпеченням і направленістю виробничо-господарської діяльності, єдиним механізмом управління [1].

У статті І. Ю. Кадникової та А. Ф. Самігуліної система фінансової безпеки визначається як сукупність управлінських, економічних та правових заходів, що здійснюються керівництвом підприємства з метою захисту фінансових інтересів організації від реальних або потенційних загроз, що можуть призвести до втрати основних ресурсів [2].

В. Т. Сусіденко, Р. П. Підлипна, Е. Ф. Югас визначають систему фінансової безпеки підприємства як сукупність взаємопов'язаних елементів (спеціальних структур, засобів, методів і заходів), здатних забезпечити захист ведення бізнесу від внутрішніх і зовнішніх загроз [3].

Отже, система фінансової безпеки підприємства представляє собою сукупність спеціальних заходів, методів, засобів та суб'єктів, головної метою яких виступає захист фінансових інтересів підприємства від внутрішніх та зовнішніх загроз.

Головною проблемою сучасних міст і підприємств, які знаходяться в ньому, є те, що не всі керівники підприємств в повній мірі оцінюють потребу в надійній системі фінансової безпеки. На мою думку складність цього полягає в визначенні конкретних дій, які повинні бути направленні для захисту життєво важливих ресурсів. Саме тому, більшість керівництва обмежуються лише створенням на підприємстві простої охорони, а це майже повністю виключає