захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних» від 6.07.2010 р. №2438-VI // Відомості Верховної Ради України. – 2010. - №46. - Ст. 542. ***5.*** *Кримінальний процесуальний кодекс України. Закон України «Про внесення змін до деяких законодавчих актів України у зв'язку з прийняттям Кримінального процесуального кодексу України»: (відповідає офіційному текстові). – К.: Алерта, 2012. - 304с.* ***6.*** *Постанова Пленуму Верховного Суду України «Про деякі питання застосування судами України законодавства при дачі дозволів на тимчасове обмеження окремих конституційних прав і свобод людини і громадянина під час здійснення оперативно-розшукової діяльності, дізнання і досудового слідства» від 28.03.2008 р. №2 //http://www.scourt.gov.ua/clients/vs.nsf.* ***7.*** *Негласні слідчі (розшукові) дії. Коментар до глави 21 Кримінального процесуального кодексу України / [кол. авт.; за заг. ред. Є.Д. Скулиша]. - К. : Наук.- вид. центр НА СБУ, 2012. - 132 с.* ***8.*** *Климчик О., Мельник Д. Реалізація положень конвенції про кіберзлочинність в законодавстві України / О. Климчук, Д. Мельник // Інформаційна безпека людини, суспільства, держави. – 2009. – № 1(1). – С. 39-43.*

УДК 004.056.5; 338.516.2

МОДЕЛЬ ЦІНОУТВОРЮЮЧИХ ЧИННИКІВ НАДАННЯ ПОСЛУГ У СФЕРІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Володимир Кононович, Юрій Копитін*, Марина Копитіна

*Одеська національна академія зв'язку ім. О. С. Попова, *КП «Обласний інформаційно-аналітичний центр» Одеської обласної ради*

Анотація: **Розкрито основні засади ведення в Україні господарської діяльності у сфері забезпечення інформаційної безпеки (СЗІБ). Побудовано модель витрат на впровадження СЗІБ у формі спіралі Архімеда. Запропоновано класифікацію послуг у СЗІБ. Відображено основні чинники, що впливають на процес ціноутворення надання послуг у СЗІБ у вигляді моделі.**

Summary: **The basic principles of doing business in Ukraine in the sector of information security (SIS) is showed. The model of the costs of implementation SIS is build. The classification of services SIS is proposed. A model of the main factors that affect the pricing of services SIS is displayed.**

Ключові слова: **Послуги у сфері забезпечення інформаційної безпеки, ціна, якість.**

І Вступ

Сучасний світ характеризується тенденціями глобалізації та інтеграції світової економіки, широким використанням інформаційно-комунікаційних технологій (ІКТ), формуванням нового типу економіки – економіки знань або інноваційної економіки, в якій основними чинниками розвитку і джерелами зростання якості життя людей є знання, високі технології та людський капітал. Генерування і впровадження ідей та інновацій, виробництво високоякісних конкурентоспроможних товарів та послуг у всіх сферах діяльності та їх споживання є сьогодні ключовою сферою економіки та фундаментом, на якому будується інформаційне суспільство.

Стрімке використання новітніх ІКТ несе в собі не лише позитивний розвиток, а й загрози інформаційної безпеки (ІБ), що створює передумови для витоку, розкрадання, втрати, спотворення, підробки, знищення, копіювання і блокування інформації і, як наслідок, веде до заподіяння шкоди. З підвищенням значущості і цінності ІКТ зростає важливість надання якісно нових послуг у сфері забезпечення інформаційної безпеки (СЗІБ).

Окремі складові даної тематики висвітлені в публікаціях Доморева В. В., Загинайлов Ю. М., Малюк А. О., Ткаченко В. В., Соколової А. О., Філіппової І. А, Баталової Н. В., Анісімова О. О. та інших. Однак, будь-яких комплексних досліджень ринку ІБ та надання послуг в СЗІБ, в тому числі процесу їх ціноутворення, в Україні та СНД не проводилося.

В зв'язку з цим, *метою статті* є висвітлення проблематики та пошук відповідей на проблемні питання процесу ціноутворення надання послуг у СЗІБ, а також представлення основних його чинників у вигляді моделі.

Для реалізації даної мети використано чинне національне законодавство, нормативно-правові акти, міжнародні та державні стандарти, світові практики щодо забезпечення ІБ та надання послуг, думки експертів, результати спеціалізованих досліджень, рекламні матеріали компаній та інші відкриті джерела інформації.

ІІ Опис проблеми

На сьогоднішній день в Україні юридичними та фізичними особами активно ведеться господарська діяльність у СЗІБ, пов'язана з виробництвом (виготовленням) продукції, торгівлею, виконанням робіт, наданням послуг. Перш ніж перейти до розкриття особливостей ведення такої діяльності, визначимо сутність понять забезпечення інформаційної безпеки та надання послуг у сфері забезпечення інформаційної безпеки.

Під забезпеченням інформаційної безпеки будемо розуміти систему заходів правового, організаційно-технічного та організаційно-економічного характеру з виявлення загроз інформаційній безпеці, запобігання їх реалізації, припинення та ліквідації наслідків реалізації таких загроз [1].

Під наданням послуг у СЗІБ будемо вважати господарську діяльність, спрямовану на забезпечення інформаційної безпеки, виконану постачальником послуг на замовлення споживача згідно з договором на платній або безоплатній основі.

Відповідно до ст. 9 закону України (ЗУ) «Про ліцензування певних видів господарської діяльності» ліцензуванню підлягають наступні види господарської діяльності у СЗІБ [2]:

- *надання послуг у галузі криптографічного захисту інформації* (крім послуг електронного цифрового підпису), торгівля криптосистемами і засобами криптографічного захисту інформації, а саме:
- складання конструкторської та іншої технічної документації до криптосистем і засобів криптографічного захисту інформації;
- монтаж (встановлення), налаштування, технічне обслуговування (супроводження) криптосистем і засобів криптографічного захисту інформації [3];
- *надання послуг у галузі технічного захисту інформації*, а саме:
  - оцінювання захищеності інформації;
  - виявлення закладних пристроїв [4].

Більшість компаній надають послуги, які входять в межі зазначених вище ліцензійних умов ведення діяльності. Однак значна кількість ІТ-компаній та компаній з суміжних областей реалізують продукти та надають послуги в сфері ІБ в обхід зазначених ліцензійних умов або взагалі без них, оскільки такі умови відсутні, що несе значний вплив на процес ціноутворення. Основною причиною такої ситуації є відсутність чіткого визначення понять інформаційно-комунікаційні технології, інформаційна безпека, захист інформації та надання послуг у СЗІБ. У зв’язку з цим, майже неможливо виокремити, чи пов’язана дана діяльність з послугами у СЗІБ. В цілому, серед всіх проектів, реалізованих на українському корпоративному ринку в 2011 році, на ІТ-інфраструктуру припала частка в 40%, на корпоративні інформаційні системи - 25%, на ІТ-безпеку - 10% [5].

Взагалі ринок надання та споживання послуг у СЗІБ є закритим та непрозорим. Не всі компанії погоджуються брати участь в рейтингах та надавати дані про свою діяльність. Об'єктивно оцінити обсяг цього ринку складно і через те, що він не має загальноприйнятої термінології, а також затвердженої класифікації та сегментації, внаслідок чого провести чітку грань між продуктами, рішеннями та послугами іноді досить важко та коректно визначити частку безпосередньо послуг практично неможливо.

У ході ведення господарської діяльності особливо важливим та одним з найважчих є процес формування та встановлення цін, іншими словами процес ціноутворення.

Законодавство про ціни і ціноутворення процесу надання послуг у СЗІБ ґрунтується на Конституції України та складається з Цивільного кодексу України, Господарського кодексу України, Податкового кодексу України, законів України «Про ціни і ціноутворення», «Про природні монополії», «Про захист економічної конкуренції» та інших нормативно-правових актів.

На поточний момент під час провадження господарської діяльності у СЗІБ суб’єкти господарювання використовують як самостійне формування цін за згодою суб’єктів (вільні ціни), так і державне регулювання цін [6].

Державне регулювання застосовується до послуг конфіденційного зв’язку, які мають істотну соціальну значущість, шляхом встановлення граничних тарифів на їх надання [7]. На всі інші послуги ціна формується на ринку надання послуг у СЗІБ.

В умовах ринкової економіки прейскуранти цін на послуги в СЗІБ встановлюються підприємствами самостійно відповідно до загальних принципів ціноутворення. Однак, більшість компаній не афішують прейскуранти на надання послуг у СЗІБ, у зв'язку з чим неможливо провести порівняльний аналіз тарифів на послуги, що надаються.

У загальному вигляді ціна на послуги у СЗІБ складається з собівартості витрат, пов’язаних з наданням послуг, прибутку виробника та податків. Найбільш важливим під час формування ціни є процес визначення собівартості, яка є найбільшою величиною в її структурі, зміна якої в ту або іншу сторону веде до зростання або зниження абсолютної величини прибутку. Собівартість послуг, що надаються підприємствами у СЗІБ,

являє собою сукупність поточних трудових, матеріальних і фінансових витрат, виражених у грошовій формі. Правильна класифікація витрат та їх облік мають суттєве значення для аналізу й планування собівартості послуг та виявлення джерел економії. Враховуючи все вище зазначене, процес розрахунку собівартості послуг в СЗІБ має стати темою окремого спеціалізованого дослідження.

Виходячи із мети статті, в даній роботі зупинимось на висвітленні проблематики та визначенні основних чинників, що впливають на процес ціноутворення послуг у СЗІБ.

ІІІ Основні засади впровадження процесу надання послуг у СЗІБ в організації

В опублікованій доповіді Комісії ООН щодо широкосмугового зв'язку, підготовленому під егідою ЮНЕСКО й Міжнародного союзу електрозв'язку, говориться, що сьогодні 2,26 мільярди осіб у світі мають доступ до Інтернету. За оцінками МСЕ, до 2015 року щонайменше половина населення Землі буде мати доступ до контенту й засобів широкосмугового зв'язку [8]. Згідно з даними компанії InMind [9] на початок другого півріччя 2012 року 17,6 млн. жителів України старше 15 років регулярно користуються Інтернетом (рідше разу на місяць), що становить 45% від дорослого населення країни. При цьому щодня користуються Інтернетом 12,2 млн. українців без урахування дітей.

На сьогоднішній день компаніями Kaspersky, Symantec, ESET, McAfee, які є світовими лідерами в СЗІБ, фіксується кількісне та якісне зростання загроз, інцидентів, кібератак, в яких об’єктами нападу стають не лише окремі фізичні або юридичні особи, а й цілі держави. В зв’язку з цим, в сучасних умовах особливо важливим є забезпечення безпеки об'єктів критичної інформаційної інфраструктури.

Враховуючи викладені вище тенденції будь-яка організація для ефективного ведення господарської діяльності повинна регулярно переглядати та підвищувати рівень інформаційної безпеки шляхом виділення коштів на впровадження та постійну модернізацію засобів ІБ. Такий підхід до побудови системи управління інформаційною безпекою (СУІБ) викладено у міжнародному стандарті ISO/IEC 27001 у вигляді процесної моделі «Плануй – Виконуй – Перевіряй – Дій» («Plan-Do-Check-Act») [10], яку застосовують для структуризації всіх процесів СУІБ.

Представимо залежність витрат на впровадження системи забезпечення ІБ від рівня ІБ за допомогою моделі у вигляді спіралі Архімеда (рис. 1), яка класично використовується під час виконання креслень, що застосовуються в машинах-автоматах.

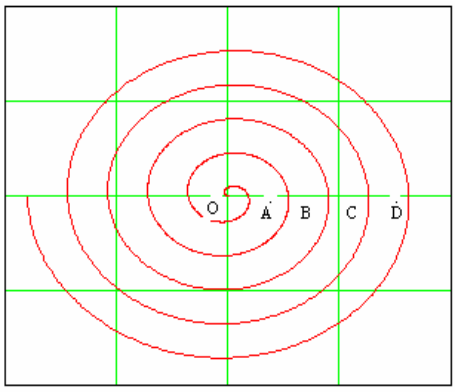

Рисунок 1 – Модель витрат на впровадження системи ІБ

Точка О характеризує відсутність системи захисту і витрат на її побудову. Точки А, В, С, D і т. д. характеризують досягнутий рівень ІБ. Витрати на впровадження захисних механізмів, потрібних для досягнення необхідного рівня безпеки, характеризуються довжиною відповідної дуги (дуга ОА, АВ, ВС, CD і т. д.). Загальна вартість витрат дорівнює сумі довжин дуг, які характеризують витрати кожного рівня. Наприклад, для досягнення мінімального рівня безпеки (точка А) необхідно впровадити організаційні заходи і антивірусний захист та налаштувати брандмауери. Для досягнення наступного рівня (точка В) необхідно впровадити систему захисту від шкідливого програмного забезпечення (ШПЗ), яка включає механізми захисту попереднього рівня, а також впровадження мережевої та локальної систем виявлення вторгнень, механізмів відновлення інформації та лікування комп’ютерів після впливу ШПЗ. Для досягнення ще вищого рівня безпеки (точка С) слід впровадити систему управління ІБ й т. д.

Забезпечувати необхідний рівень інформаційної безпеки організація може як власними силами (традиційний підхід), так і шляхом використання послуг у СЗІБ, які надаються суб’єктами господарської діяльності (сервісний підхід) [11]. Враховуючи той факт, що система забезпечення ІБ має відповідати

принципам системності, комплексності, неперервності захисту, достатності механізмів і заходів захисту та їхньої адекватності загрозам, гнучкості керування системою захисту, простоти і зручності її використання, більш оптимальним є другий варіант.

Основними перевагами сервісного підходу над традиційним є:

- вища надійність впроваджених механізмів ІБ;
- кращий рівень кваліфікації фахівців сторонньої компанії завдяки їх спеціалізації на цій роботі;
- здійснення витрат виключно за використані в поточний момент функції, при цьому не потрібно робити інвестиції в інфраструктуру;
- концентрація уваги організації на своїх безпосередніх функціях, оскільки відсутня проблема в навчанні та утриманні фахівців з інформаційної безпеки;

Основним проблемами другого варіанту є:

- відсутність 100% довіри до співробітників, що надають послуги;
- неможливість оцінити повноту послуг, оскільки відсутні критерії та стандарти якості послуг у СЗІБ.

Під час замовлення послуг у СЗІБ слід враховувати залежність між трьома пов'язаними з ними критеріями: рівнем захищеності, часом надання послуг та ціною. Підвищення вимог до рівня ІБ або підвищення швидкості надання послуг збільшує ціну впровадження механізмів безпеки.

З метою вибору оптимального постачальника послуг у сфері ІБ організація має дотримуватися наступного алгоритму.

1. Встановити, які послуги у СЗІБ необхідні шляхом визначення переліку активів, що потребують захисту та імовірних джерел загроз ІБ, тобто, перш ніж почати аналізувати ринок ІБ, організація повинна мати повне уявлення про те, навіщо потрібно забезпечувати захист.

2. На ринку ІБ обрати множину постачальників необхідних послуг у СЗІБ та провести їх аналіз за наступними критеріями: наявність ліцензії на ведення діяльності у сфері технічного та криптографічного захисту інформації, наявність спеціалізованих сертифікатів щодо надання необхідної послуги, досвід роботи постачальника на ринку ІБ (поточні та виконані проекти), наявність відповідних кваліфікованих фахівців та періодичність підвищення їх компетенції, наявність публікацій фахівців організації в профільних виданнях.

3. Укласти договір, в якому буде визначено: чітке найменування та кількість послуг, якість їх надання, ціну та порядок здійснення оплати, місце та термін надання послуг, права, зобов'язання та відповідальність обох сторін, поведінку у випадку настання обставин непереборної сили, порядок вирішення суперечок та строк його дії.

4. Після укладення договору організації необхідно проводити періодичний аналіз послуг відповідно до їх поточних потреб згідно п. 1, а також, якості їх надання обраними постачальниками. У випадку їх неякісного надання обрати альтернативного постачальника на підставі критеріїв п. 2.

IV Модель ціноутворюючих чинників надання послуг у сфері забезпечення інформаційної безпеки

Однією з основних проблем, пов'язаних із наданням послуг у СЗІБ**,** є відсутність методології розрахунку цін. У зв'язку з цим, для кращого розуміння процесу ціноутворення представимо всі складові, пов'язані з наданням послуг у СЗІБ, у вигляді трирівневої моделі (рис. 2). Перший рівень моделі складають фундаментальні чинники ціноутворення на послуги у СЗІБ, другий рівень – самі послуги у СЗІБ, третій рівень – критерії формування цін на певну послугу.

Опис першого рівня. В Україні можна виділити такі види організацій, що здійснюють діяльність у СЗІБ:

- вендори;
- розробники продуктів (програмних і апаратних);
- системні інтегратори рішень з ІБ;
- дистриб'ютори продуктів ІБ;
- консультанти з ІБ;
- аудитори в сфері ІБ;
- компанії, що надають тренінги з ІБ;
- страхові компанії в сфері ІБ;
- мас-медіа та інформаційні ресурси в сфері ІБ [12].
- Ринок постачальників послуг у сфері ІБ складають вітчизняні постачальники послуг та філії міжнародних компаній. Зазначимо, що ціна та якість однакових послуг може досить суттєво відрізнятися. Недостатня координація діяльності з боку професійних спілок у СЗІБ та регуляторів призвела до того, що реалізувати прозоре та зрозуміле ціноутворення в Україні майже неможливо.

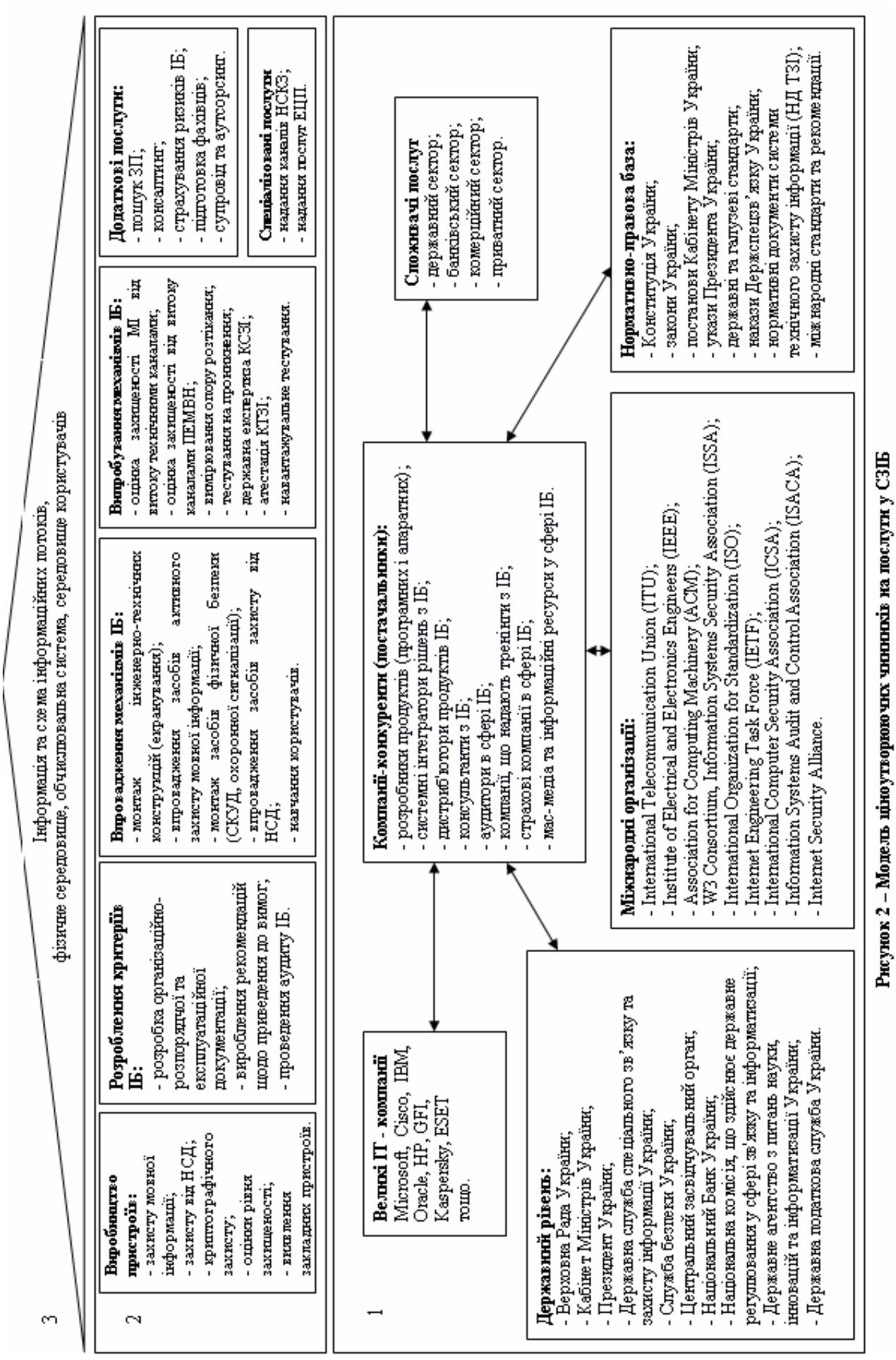

Рисунок 2 – Модель ціноутворюючих чинників на послуги у СЗІБ

Також загострює ситуацію відсутність виробленої державної політики, спрямованої на стимулювання науково-дослідної і впроваджувальної діяльності з надання послуг у сфері забезпечення інформаційної безпеки (СЗІБ) та концепція організації системи контролю за їх якістю на рівні уряду.

Споживачів послуг у сфері забезпечення інформаційної безпеки за сегментами ринку можна розподілити наступним чином:

- державний сектор (органи державної влади та місцевого самоврядування, військові формування, державні та комунальні підприємства, установи та організації тощо);
- банківський сектор (банківські та інші фінансові установи);
- комерційний сектор (підприємства різних форм власності та секторів економіки);
- приватний сектор (фізичні особи для власних потреб).

Нормативно-правову базу з питань надання послуг у сфері інформаційної безпеки складають Конституція України, ЗУ «Про інформацію», ЗУ «Про доступ до публічної інформації», ЗУ «Про захист персональних даних», ЗУ «Про захист інформації в інформаційно-телекомунікаційних системах», ЗУ «Про ліцензіювання певних видів господарської діяльності», постанови Кабінету Міністрів України, укази Президента України, державні та галузеві стандарти, накази Держспецзв'язку України, нормативні документи системи технічного захисту інформації (НД ТЗІ), міжнародні стандарти та рекомендації.

Більшість з цих документів стосуються регламентування процесу забезпечення інформаційної безпеки в державному секторі. Однак частина документів системи технічного захисту інформації прийняті без змін ще з часів Радянського Союзу і є цілком відсталими від сучасних потреб. Міжнародні нормативні документи в органах державної влади носять рекомендаційний характер, що значно впливає на рівень цін, оскільки компаніям-виконавцям доводиться забезпечувати захист одних і тих самих активів за різними стандартами. У зв'язку з цим, доволі складно визначити остаточний перелік послуг, необхідних для забезпечення інформаційної безпеки.

Питання забезпечення банківської таємниці та інформаційної безпеки банківського сектору регламентуються Конституцією та Законами України, постановами Правління Національного Банку України, а також прийнятими для цих цілей міжнародними стандартами. Законодавство даного сектору є найбільш адаптованим до сучасних умов.

Однак майже повністю неврегульованим є забезпечення інформаційної безпеки комерційного та приватного секторів. Телекомунікаційні установи можуть виступати як постачальники послуг, так і споживачі. Частково врегульованою є діяльність у сфері телекомунікацій (як постачальники послуг), оскільки оператори та провайдери зобов'язані відповідно до законодавства вживати заходи:

- із забезпечення таємниці телефонних розмов, іншої інформації, що передається телекомунікаційними мережами, а також із захисту відомостей про споживача, отриманих під час укладання договору, наданих чи замовлених ним послуг, іншої інформації з обмеженим доступом;
- щодо недопущення несанкціонованого доступу до телекомунікаційних мереж, технічних засобів провайдерів та інформації, що передається ними.

Оператори та провайдери зобов'язані вживати відповідно до законодавства технічні та організаційні заходи із захисту телекомунікаційних мереж, технічних засобів телекомунікацій, інформації з обмеженим доступом про телекомунікаційні мережі та інформації, що передається такими мережами [13].

Також певний вплив на комерційний сектор здійснюють вимоги міжнародного регулятора в особі Комітету по безпеці індустрії платіжних карт PSI SSC, міжнародних біржових структур, що вимагають виконувати вимоги нормативних актів SOX 404, Basel II або міжнародних стандартів ISO 27001, PCI DSS тощо.

Майже повністю не врегульованими є страхування ризиків інформаційної безпеки [14] та аудиту інформаційної безпеки. Також чітко не визначено, які послуги відносяться до ІТ, а які до сфери інформаційної безпеки. Законодавчо не забезпечені належні умови для розробки і швидкого впровадження ефективних інноваційних послуг на ринку ІБ.

Відповідно до вимог ст. 75, 116 Конституції України, ст. 9, 106 ЗУ «Про основи національної безпеки України», ст. 3 ЗУ «Про Державну службу спеціального зв'язку та захисту інформації України», ст. 2 ЗУ «Про Службу безпеки України», ст. 3 ЗУ «Про державну податкову службу в Україні», ст. 7 ЗУ «Про Національний банк України» основними регуляторами процесу ціноутворення на послуги у СЗІБ є Верховна Рада України, Кабінет Міністрів України, Президент України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Центральний засвідчувальний орган, Національний Банк України, Національна комісія, що здійснює державне регулювання в сфері зв'язку та інформатизації, Державне агентство з питань науки, інновацій та інформатизації України, Державна податкова служба України.

Зазначені вище структури:

- забезпечують встановлення та контроль за додержанням рівня цін;
- провадять контроль за сплатою податків;
- проводять ліцензування діяльності з надання послуг у СЗІБ та послуг, пов'язаних із забезпеченням охорони державної таємниці;
- визначають вимоги до захисту державних інформаційних ресурсів, банківської таємниці та споживачів телекомунікаційних послуг;
- встановлюють умови функціонування засвідчувальних центрів органів виконавчої влади або інших державних органів та центрів сертифікації ключів;
- тощо.

Окремим чинником, що впливає на процес ціноутворення, є наявність міжнародних організацій, що діють у сфері інформаційної безпеки та здійснюють істотний вплив на функціонування глобальних інформаційних систем та діяльність всього інформаційного суспільства. До найбільш відомих об'єднань відносяться: International Telecommunication Union (ITU), Institute of Electrical and Electronics Engineers (IEEE), Association for Computing Machinery (ACM), W3 Consortium, Information Systems Security Association (ISSA), International Organization for Standardization (ISO), Internet Engineering Task Force (IETF), International Computer Security Association (ICSA), Information Systems Audit and Control Association (ISACA), Internet Security Alliance [15].

Кожна з них, у свою чергу, має свої специфічні організаційні особливості, проте всі вони, як правило, вирішують завдання розробки, погодження та подальшого поширення загальних для всього співтовариства користувачів інформаційних систем технічних і організаційних рішень, таких як:
- протоколи глобальних мереж;
- архітектура, алгоритми, протоколи публічних засобів шифрування даних;
- правила побудови глобальних мереж обміну даними та інших елементів глобальної інфраструктури інформаційної безпеки.

Значний внесок у процес ціноутворення на послуги в сфері ІБ здійснюють великі міжнародні компанії (виробники засобів захисту інформації), оскільки саме вони встановлюють ціни на апаратні, програмні та програмно-апаратні засоби захисту інформації. До таких компаній відносяться Microsoft, Cisco, IBM, Oracle, HP, GFI, Kaspersky, ESET тощо.

Опис другого рівня. На сьогоднішній день існує широке різноманіття послуг в СЗІБ. Це пов'язано з особливостями організації кіберсередовища, яке включає користувачів, Інтернет, комп'ютерні пристрої, які підключені до нього, всі програми, служби та системи, які можуть прямо або опосередковано підключатися до Інтернету, та середовище мереж наступних поколінь, доступних для загального і приватного використання. У кіберсередовище входить програмне забезпечення, яке працює в комп'ютерних пристроях, інформація, яка зберігається та передається в цих пристроях, або інформація, яка створюється цими пристроями. В зв'язку з використанням технології VoIP, стаціонарний телефон також став частиною кіберсередовища. Ізольовані пристрої є також частиною кіберсередовища, оскільки вони можуть користуватися інформацією спільно з комп'ютерними пристроями, що підключаються за допомогою змінних носіїв. Обладнання та будівлі, в яких розташовані ці пристрої, також є його частиною. Всі ці елементи повинні прийматися в розрахунок кібербезпеки [16].

Однак, до поточного моменту не створено загальновизнаної системи класифікації та каталогізації послуг у СЗІБ. В КВЕД-2010, ДК 016:2010, ДК 003:2010 не в повному обсязі виділені види економічної діяльності, продукція та послуги, професійні назви робіт, які надаються суб'єктами господарювання СЗІБ.

Проаналізувавши вимоги чинного законодавства, каталоги компаній постачальників послуг та потреби споживачів автори спробували виділити наступні класи послуг: виробництво пристроїв, розробка критеріїв ІБ, впровадження механізмів ІБ, додаткові та спеціалізовані послуги.

До послуг виробництва пристроїв відноситься виготовлення засобів захисту мовної інформації, захисту від НСД, криптографічного захисту, оцінки рівня захищеності, виявлення закладних пристроїв (ЗП).

Послуги щодо розробки критеріїв ІБ включають: розробку організаційно-розпорядчої та експлуатаційної документації, вироблення рекомендацій щодо приведення до вимог, проведення аудиту ІБ.

До послуг впровадження механізмів ІБ відносяться: монтаж інженерно-технічних конструкцій (екранування), впровадження засобів активного захисту мовної інформації, монтаж засобів фізичної безпеки (СКУД, охоронна сигналізація), впровадження засобів захисту від НСД, навчання користувачів. Впровадження засобів захисту від НСД включає налаштування: системи захисту від шкідливого програмного забезпечення, захисту периметру мережі, захисту від інсайдерів (DLP-системи), систем контролю мережевого трафіку (IDS/IPS), корпоративної інфраструктури відкритих ключів (PKI), системи ідентифікації та автентифікації, механізмів захисту мобільних пристроїв, системи управління інцидентами ІБ, захищеної електронної пошти, захищеного Інтернет порталу, засобів контролю цілісності, засобів захисту бездротового

зв’язку, системи управління оновленнями, каналів захищеного зв’язку (VPN), захисту систем віртуалізації, захищеного відеоконференцзв’язку.

До послуг випробування механізмів ІБ віднесемо: оцінку захищеності мовної інформації (МІ) від витоку технічними каналами, оцінка захищеності від витоку каналами ПЕМВН, вимірювання опору розтікання, тестування на проникнення, державна експертиза КСЗІ, атестація КТЗІ, навантажувальне тестування.

Додаткові послуги включають: пошук ЗП, консалтинг, страхування ризиків ІБ, підготовка фахівців, супровід та аутсорсинг.

Спеціалізовані послуги складають: надання каналів національної системи конфіденційного зв’язку (НСКЗ), надання послуг електронного цифрового підпису (ЕЦП).

Опис третього рівня. Враховуючи те, що кожна організація має унікальну за своїм складом інформацію та технологію її обробки, майже неможливо попередньо чітко визначити ціну більшості з послуг у СЗІБ. Всеосяжний обсяг вимог до безпеки, який має важливе значення під час формування ціни, повинен враховувати: залучені сторони; ресурси, що потребують захисту; загрози, від яких необхідно захистити ці ресурси; вразливі елементи, пов'язані з цими ресурсами; загальні ризики, яким ці загрози та вразливі елементи піддають ресурси.

Перш за все, на процес ціноутворення впливає інформація, що може бути представлена в усному або документованому вигляді, та технологія її обробки. В першому вигляді вона може бути оголошена безпосередньо людиною (тобто об’єктом захисту є мова людини), у другому вигляді – надрукована або зберігатися в електронному вигляді (тобто об’єктами захисту є документи, а також, електронні носії інформації – комп’ютери, флеш-носії, диски, дискети). Від категорії інформації, відповідно до нормативно-правових вимог, залежить вибір необхідних механізмів безпеки. Ціна послуг також залежить від особливостей обігу електронних документів, оскільки від схем інформаційних потоків і середовища, через які вони передаються, залежить складність забезпечення інформаційної безпеки.

По-друге, на ціну впливають характеристики фізичного середовища, а саме: територіальне розміщення, наявність охорони території та перепускний режим, наявність категорійованих приміщень, захищеність від засобів технічної розвідки, наявність елементів комунікацій, систем життєзабезпечення і зв’язку, що мають вихід за межі контрольованої зони, наявність та технічні характеристики систем заземлення, умови зберігання магнітних, оптико-магнітних, паперових та інших носіїв інформації. Ці характеристики визначають перелік інженерно-технічних засобів та склад робіт щодо їх налаштування або монтажу.

По-третє, на ціноутворення впливають особливості обчислювальної системи, а саме:

- перелік і склад обладнання, технічних і програмних засобів, їхні зв'язки, особливості конфігурації, архітектури й топології, програмні і програмно-апаратні засоби захисту інформації, взаємне розміщення засобів тощо;
- види і характеристики каналів зв'язку;
- особливості взаємодії окремих компонентів, їх взаємний вплив один на одного;
- можливі обмеження щодо використання засобів.

Від особливостей обчислювальної системи залежить остаточний склад апаратних, програмних та програмно-апаратних засобів, необхідних для забезпечення безпеки, а також необхідні роботи щодо їх налаштування. На думку аналітиків IDC, основною рушійною силою ринку ІБ в подальшому стануть мобільні та хмарні технології [17].

Четвертим чинником є середовище користувачів, оскільки від їхніх функціональних обов’язків та рівня кваліфікації, повноважень щодо допуску до відомостей, а також рівня можливостей, що надаються, залежить потреба в їх консультуванні та додатковому навчанні.

V Висновки

Проведений аналіз ціноутворюючих чинників процесу надання послуг у СЗІБ свідчить про недостатній розвиток нормативно-правової бази, відсутність критеріїв оцінки якості послуг, недостатній стимулюючий вплив регуляторів і, як наслідок, низьку конкурентоспроможність вітчизняних постачальників послуг. Побудована модель, це лише один із кроків вирішення проблем, пов’язаних з наданням послуг у СЗІБ, та в подальшому може бути відправною точкою для розрахунку собівартості надання послуг.

Для вирішення зазначених в статті проблем необхідно:

- розробити та впровадити ефективну державну політику, спрямовану на стимулювання науково-дослідницької та впроваджувальної діяльності з надання послуг у сфері забезпечення інформаційної безпеки
- розробити концепцію організації системи державного контролю якості надання послуг у СЗІБ та виробити критерії оцінки якості їх надання;
- розробити та прийняти державні стандарти щодо надання послуг у СЗІБ та оцінки їх якості;

- створити узгоджений понятійний апарат і єдину термінологію з надання послуг у СЗІБ, яка буде зрозумілою постачальникам та споживачам послуг;
- створити загальновизнану систему класифікації послуг у СЗІБ, що дозволить забезпечити єдиний правовий режим їх надання;
- розробити та впровадити методологію розрахунку цін на надання послуг у СЗІБ.

Література: ***1.*** *Соглашение о сотрудничестве государств–участников Содружества Независимых Государств в области обеспечения информационной безопасности [Електронний ресурс]. – Режим доступу: http://adilet.minjust.kz/rus/docs/P1200000692* ***2.*** *Закон України Про ліцензування певних видів господарської діяльності [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/1775-14* ***3.*** *Постанова КМУ від 25.05.2011 № 543 Про затвердження переліків послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та криптосистем і засобів криптографічного захисту інформації, господарська діяльність щодо яких підлягає ліцензуванню [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/543-2011-%D0%BF* ***4.*** *Постанова КМУ від 18.05.2011 № 517 Про затвердження переліку послуг у галузі технічного захисту інформації, господарська діяльність щодо надання яких підлягає ліцензуванню [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/517-2011-%D0%BF* ***5.*** *DiaWest: в 2011 году рынок корпоративных услуг вырос на 35% [Електронний ресурс]. – Режим доступу: http://www.apitu.org.ua/node/2341* ***6.*** *Закон України Про ціни і ціноутворення [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/5007-17* ***7.*** *Наказ ДСТСЗІ СБУ від 14.07.2004 № 56 Про затвердження Граничних тарифів на послуги конфіденційного зв'язку [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/z0909-04* ***8.*** *В Україні лише третина населення має доступ до інтернет [Електронний ресурс]. – Режим доступу: http://www.pravda.com.ua/news/2012/09/25/6973396/* ***9.*** *Исследование: 17,6 млн украинцев регулярно пользуются интернетом [Електронний ресурс]. – Режим доступу: http://biz.liga.net/all/it/novosti/2262042-17-6-mln-ukraintsev-polzuyutsya-internetom-issledovanie.htm* ***10.*** *Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою: ГСТУ СУІБ 1.0/ISO/IEC 27001:2010. – [проект]. - К.: Національний банк України 2010. – 49 с.: табл. – (Галузевий стандарт України).* ***11.*** *Валерий Васильев Услуги в области ИТ-безопасности [Електронний ресурс]. – Режим доступу: http://www.pcweek.ru/security/article/detail.php?ID=141643* ***12.*** *Ткаченко В. В. Дорожная карта специалиста по ИБ [Електронний ресурс]. – Режим доступу: http://www.trn.ua/articles/2144/* ***13.*** *Постанова КМУ від 11.04.2012 № 295 Про затвердження Правил надання та отримання телекомунікаційних послуг [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/295-2012-%D0%BF* ***14.*** *Копитін Ю. В. Модель страхування ризиків інформаційної безпеки [Електронний ресурс]. – Режим доступу: http://digitech.onat.edu.ua/files/13.pdf* ***15.*** *А. А. Анисимов Менеджмент в сфере информационной безопасности [Електронний ресурс]. – Режим доступу: http://www.intuit.ru/department/itmngt/manofis/* ***16.*** *Рекомендация МСЭ-Т X.1205 Обзор кибербезопасности [Електронний ресурс]. – Режим доступу: http://www.itu.int/* ***17.*** Анна Кожина *Основной движущей силой рынка ИБ будут мобильные и облачные технологии [Електронний ресурс]. – Режим доступу: http://www.itbestsellers.ru/experts/detail.php?ID=19880*

УДК 004.056.53(045)

СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НА БАЗІ МІЖНАРОДНИХ СТАНДАРТІВ СЕРІЇ ISO

Анна Чунарьова, Андрій Чунарьов
Національний авіаційний університет

Анотація: **Проведено аналіз сучасних заходів управління інформаційною безпекою інформаційних мереж на базі міжнародних стандартів серії ISO. Виділено ряд переваг застосування системи управління інформаційною безпекою. Запропоновано сценарій управління ризиками інформаційної безпеки та розроблену структурну схему оцінки інформаційних ризиків інформаційної мережі підприємства.**

Summary: **An analysis of contemporary events information security management of information networks based on international standards of series ISO. Highlighted a number of advantages of information security management system. We propose a scenario of risk management information security and developed a structural block diagram of information risk assessment information network.**

Ключові слова: **Інформаційна безпека, оцінка ризиків, управління інформаційною безпекою, модель**