УДК 338.47

Редькін О.С., Тардаскіна Т.М.

ФУНКІОНАЛЬНО-ВАРТІСНИЙ АНАЛІЗ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ АТС

На основі функціонально-вартісного аналізу як варіанту системного підходу формулюються моделі та задачі проектування, створення та оцінки ефективності системи інформаційної безпеки АТС в телекомунікаційних мережах. Розглядаються основні положення методики функціонально-вартісного аналізу системи інформаційної безпеки.

On the basis functionally-value analysis as a version of system approach models and tasks of projecting, creation and evaluation of efficiency of system information security of ATS in the telecommunication network are formulated. The main points of methodics of functionally-value analysis of information security system are considered.

Особливості розвитку світу інформації, можливості необмеженого та неконтрольованого впливу, несанкціонований доступ, комп'ютерні віруси та інше гостро поставили перед суспільством проблеми інформаційної безпеки, яка повинна здійснюватися комплексно та систематично з використанням різних засобів (технічних, організаційних, правових) щоб запобігти інформаційному тиску та в цілому будь-якій іншій інформативній небезпеці. Інформаційна безпека є головною частиною економічної безпеки держави та національної безпеки в цілому. Зрозуміло, що становлення суспільства нового типу дуже гостро ставить питання інформаційної безпеки простору держави, людини, суспільства, а також створення ефективної системи забезпечення прав громадян і соціальних інститутів на вільне одержання, поширення і використання інформації. Це питання неможливо обійти, тим більше, що воно стосується всіх галузей і є дуже актуальним зараз і для нашої країни, що й викликало потребу в його розгляді.

Завдання обгрунтування доцільності витрат на систему інформаційної безпеки можуть бути вирішені при системній організації інформаційно-аналітичної роботи та врахуванні всіх аспектів: законодавчих, організаційних, техніко-технологічних, ергономічних, економічних та правових на всіх етапах життєвого циклу: технічного завдання, проектування, створення, експлуатації та утилізації. Розглянемо проблему та задачі функціонально-вартісного аналізу як варіанту системного підходу на прикладі побудови системи захисту інформації в таких об'єктах інформаційної діяльності, як програмно-керовані автоматизовані телефонні станції (АТС), актуальні в контексті забезпечення інформаційної безпеки телекомунікаційних мереж, управління державою та дотримання економічних інтересів.

Розв'язання цих задач проводилось в напрямах вивчення методів оцінки витрат на захист інформації [1], методів обгрунтування інвестицій в інформаційну безпеку [2], оцінки ефективності та зрілості технологій безпеки [3]. В роботах [4,5] зроблено спробу застосування функціонально-вартісного аналізу (ФВА) системи інформаційної безпеки телекомунікаційних мереж загального користування. Особливість нинішнього етапу розвитку інформаційних і практично всіх технологій характеризується надзвичайно високим ступенем їх інтеграції в усіх сферах людської діяльності та зумовленою цими обставинами потенційною вразливістю та техногенною небезпекою. В той же час, складність програмно-керованих АТС з точки зору захисту інформації і комплекс завдань забезпечення інформаційної безпеки, встановлених законами України та низкою нормативно-правових документів [6,7] визначають необхідність застосування методів системного і функціонально-вартісного аналізу.

Функціонально-вартісний аналіз (Activity Based Costing – ABC) в економіці трактується як процес розподілу витрат з використанням первинних носіїв вартості з

остаточним розподілом витрат по основним продуктам та послугам [1]. Аналіз орієнтується на виробничу або логістичну структуру підприємства і дозволяє досить точно і зрозуміло встановити зв'язок між елементами собівартості продукції та виробничими процесами. Стосовно оцінки систем захисту інформації метод функціонально-вартісного аналізу застосовується для побудови моделі бізнес-процесів підприємства на основі показників вартості, трудомісткості й продуктивності та дозволяє розподіляти накладні витрати у відповідності з детальним прорахунком використання ресурсів, докладними уявленнями щодо процесів та функцій, які їх складають, а також їх впливом на собівартість. Але функціонально-вартісний аналіз доцільно розповсюдити на всі етапи життєвого циклу системи інформаційної безпеки. Так, на етапі технічної експлуатації нормативно-правовими документами [8] передбачається удосконалення порядку забезпечення захисту інформації, впровадження нових технологій захисту та модернізація автоматизованої системи, включаючи проведення аналітичної оцінки поточного стану безпеки інформації. У економіці таке розповсюдження частково реалізується у методах функціонально-вартісного управління (Activity Based Management - ABM), який разом з ABC використовується для реорганізації бізнес-процесів з метою підвищення продуктивності, зниження собівартості та поліпшення якості.

Як у цілому для узагальнених об'єктів інформаційної діяльності, так, зокрема, і для програмно-керованих АТС, задачі функціонально-вартісного аналізу системи інформаційної безпеки залишаються остаточно не вирішеними і недостатньо формалізованими.

Метою цієї статті є дослідження моделей та задач і розробка основних положень методики функціонально-вартісного аналізу системи інформаційної безпеки в АТС.

Вимоги до функціонально-вартісного аналізу інформаційної безпеки АТС. Технічний захист інформації перетворюється у забезпечення інформаційної безпеки інформаційних ресурсів, при чому інформаційний ресурс включає в себе інформацію та засоби, в яких вона обробляється і циркулює. По друге, дещо змінились пріоритети. В цілому, забезпечення інформаційної безпеки сьогодні включає в себе такі поняття, як цілісність (integrity) інформації, конфіденційність (confidentiality), захищеність від несанкціонованого доступу (authentication, non-repudiation), та забезпечення надійності (availability) функціонування системи [9].

Процес забезпечення інформаційної безпеки все більше перетинається з процесами управління якістю надання телекомунікаційних послуг, де захищеність інформаційних ресурсів є складовою частиною оцінки якості; управління економічною ефективністю, де є взаємозв'язок між інформаційними та економічними ризиками; та задачами технічної експлуатації в частині забезпечення вимог до збереження мінімального набору критично важливих функцій, до живучості інформаційних систем, до запасу сталості при дії дестабілізуючих факторів зовнішнього середовища. Порушення цілісності системи на фоні зниження активності її елементів тягне за собою дезорганізацію управління, одночасне зниження активності елементів та їх живучості – втрату гнучкості, а зниження живучості та порушення цілісності системи – втрату найважливіших функцій. Поняття живучості системи передбачає її спроможність своєчасно виконувати свої функції в умовах дії дестабілізуючих факторів (фізичне руйнування, часткова втрата ресурсів, відмови та збої елементів, несанкціоноване втручання в контур управління). При цьому технічна надійність, яка проявляється як здатність системи працювати без відмов, визначає мінімальний поріг стійкості системи, за яким без наявності відновлення втрачених елементів та функцій може настати повна її зупинка. Живучість інформаційних систем має визначальну роль для інформаційної безпеки в цілому.

На різних стадіях життєвого циклу систем інформаційної безпеки та різних етапах проектування, створення та експлуатації формуються показники захищеності, гарантій,

якості та взаємопов'язані з ними техніко-економічні показники. Функціонально-вартісний аналіз має активно впливати на процеси створення і експлуатації систем інформаційної безпеки та включає виявлення та аналіз впливу різноманітних факторів і визначення на основі аналізу впливів засобів протидії та відповідних заходів. Склад та рівень показників живучості, захищеності, якості та техніко-економічної ефективності визначаються на основі аналізу вимог нормативно-правових та нормативно-технічних документів і з урахуванням можливостей та розвитку технологій. З іншого боку, враховуються ресурси конкретного підприємства чи організації.

Функціонально-вартісний аналіз є різновидом системного аналізу, в якому враховуються і поєднуються практично важливі головні властивості та вимоги до систем інформаційної безпеки:

– нормативно-правова база системи технічного захисту інформації, стандартні набори функціональних послуг захисту, які забезпечують заданий рівень захищеності;

– вимоги до заданого критерію рівня довіри до реалізації системи захисту;

– оцінка витрат на реалізацію заходів захисту, які не повинні перевищувати можливі збитки від реалізації загроз.

Задачі функціонально-вартісного аналізу відносяться до класу комбінованих детерміновано-нечітких задач. Вихідні дані моделі поділяються на повністю визначені або стохастичні параметри з відомими числовими імовірнісними характеристиками; і нечіткі параметри або параметри, які мають якісний характер і оцінюються експертними методами за допомогою якісних шкал та методів нечіткої логіки. Труднощі вирішення стохастичних та нечітких задач полягають у самій постановці задач, складності виявлення та аналізу значень та впливу різних факторів.

Методи функціонально-вартісного аналізу мають відповідати таким вимогам:

– забезпечувати кількісну оцінку витрат на інформаційну безпеку, використовуючи як кількісні так і якісні оцінки імовірності подій та їх наслідків;

– бути прозорими з точки зору користувача та дозволяти йому вводити свої емпіричні дані та зменшувати невизначеність якісних оцінок вглиб за стадіями реалізації проектів;

– бути універсальним, тобто однаково застосованим до оцінки витрат на придбання апаратних засобів, програмного забезпечення, на створення системи, навчання персоналу тощо;

– служити задачам вибору найкращого варіанту з декількох альтернативних засобів попередження певних загроз;

– давати матеріал для оцінки впливу ризиків та вибору стратегії, яка зменшувала б ризик та оптимізувала б витрати на створення і експлуатацію системи захисту.

Функціонально-вартісний аналіз має дати відповідь про роль і ефективність аудиту та моніторингу інформаційної безпеки, сканування вразливостей об'єкту інформаційної діяльності, ефективність системи виявлення атак тощо.

Важливою вимогою є модульний принцип функціонально-вартісного аналізу. Процес забезпечення інформаційної безпеки включає такі етапи, як виявлення критеріїв захищеності від різного роду впливів, критеріїв гарантій коректності реалізації послуг безпеки інформації, показників якості, до яких входить інформаційна безпека телекомунікаційних послуг та техніко-економічних показників. Модульний принцип дозволяє подолати численність показників захищеності, гарантій коректності реалізації, якості, факторів зовнішніх та внутрішніх впливів, телекомунікаційних технологій, складність взаємодії між ними та їх взаємовпливу, наявність обмежень технічного, технологічного, організаційного та економічного характеру, необхідність оцінки ступеню ризику реалізації загроз на етапі прийняття рішень.

Моделі і задачі функціонально-вартісного аналізу. Моделі функціонально-вартісного аналізу будуються за модульним принципом як відносно об'єктів аналізу, так і стосовно

процедур і задач аналізу. Складний комплекс АТС, як об'єкт аналізу з точки зору інформаційної безпеки, поділяється на окремі архітектурні компоненти інформаційної безпеки, по аналогії з тим, як це розглянуто в [4,5]. Методи функціонально-вартісного аналізу модульно структуровані за стадіями життєвого циклу системи забезпечення інформаційної безпеки та задачам, які характеризуються єдиними методами й інструментами досліджень. Методи функціонально-вартісного аналізу забезпечують послідовне уточнення оцінок при переході від початкових стадій та етапів життєвого циклу до наступних: розробки та планування, реалізації та впровадження, техобслуговування та підтримки.

Програма забезпечення інформаційної безпеки складається з політики безпеки, заходів і засобів попередження впливів порушників та інших дестабілізуючих факторів, процедур виявлення порушень, реагування на інциденти, планів відновлення та, в додаток до технології інформаційної безпеки, заходів інформаційної безпеки на протязі стадій технічного завдання та проектування і виготовлення. Кінцевою метою є вибір ефективних засобів протидії загрозам при реалізації системи інформаційної безпеки, витрати на яку не перевищують втрати, очікувані від реалізації суттєвих загроз.

На етапі реалізації функціонально-вартісний аналіз є основою для оцінки інформаційної безпеки. Впродовж стадії експлуатації мереж реалізована програма забезпечення інформаційної безпеки повинна підтримувати поточну інформаційну безпеку при змінах навколишнього середовища, допомагати у керуванні політикою та процедурами безпеки, в реагуванні на інциденти та в планах відновлення системи інформаційної безпеки.

До складу функціонально-вартісного аналізу входять: оцінка захищеності ресурсів та гарантій, оцінка живучості та надійності, оцінка технічної і економічної ефективності (ТЕЕ) та задачі підвищення рівня ефективності (рис.1). Основними методами оцінки є розрахунково-аналітичний (інструментальний), експертний, імітаційний. Застосовуються методи нечіткої логіки, експертні методи, атестація та експертиза Оцінка захищеності, техніко-економічної ефективності та підвищення рівня ефективності проводяться на основі єдиної інформації та математичних моделей, які включають: результати стадій функціонально-вартісного аналізу, фактори ризику та впливу на показники, показники функціонально-вартісного аналізу, нормативно-правова база.

Фундаментом функціонально-вартісного аналізу є нормативно-правова база. З точки зору забезпечення безпеки інформації, комплекс заходів та засобів захисту можна розглядати як набір функціональних послуг, які в сукупності створюють необхідний функціональний профіль захисту. Кожна послуга є набором функцій, що дозволяють протистояти певній множині загроз. Політику безпеки може бути здійснено з використанням різних механізмів, окремо чи в комбінації, в залежності від об'єктів політики. Загалом механізми належатимуть до одного з трьох класів, які можуть перетинатись: запобігання, реєстрування, протидії, відновлення. Вибір раціональних варіантів, оптимальне планування захисту, оцінка ефективності проектування, виконання робіт та експлуатації системи інформаційної безпеки можна здійснити на базі науково та технічно обґрунтованих норм, які відповідають сучасному рівню техніки та технології. З нормативно-правовою базою пов'язані такі характеристики як собівартість, прибуток, рентабельність.

Загрози інформаційній безпеці АТС можна поділити на типові та специфічні для кожного об'єкта інформаційної діяльності. Типові загрози розглянуті в низці нормативних документів системи технічного захисту інформації та чисельних наукових роботах. Але й типові загрози інформаційним ресурсам АТС характеризуються динамічністю і залежать від загального правового та техніко-технологічного стану інформаційної безпеки в державі та на підприємстві, застосованих в АТС телекомунікаційних та інформаційних технологій, характеристик об'єкту інформаційної діяльності, видів циркулюючої інформації, рівня грамотності й культури суспільства і персоналу в сфері інформаційної безпеки тощо.

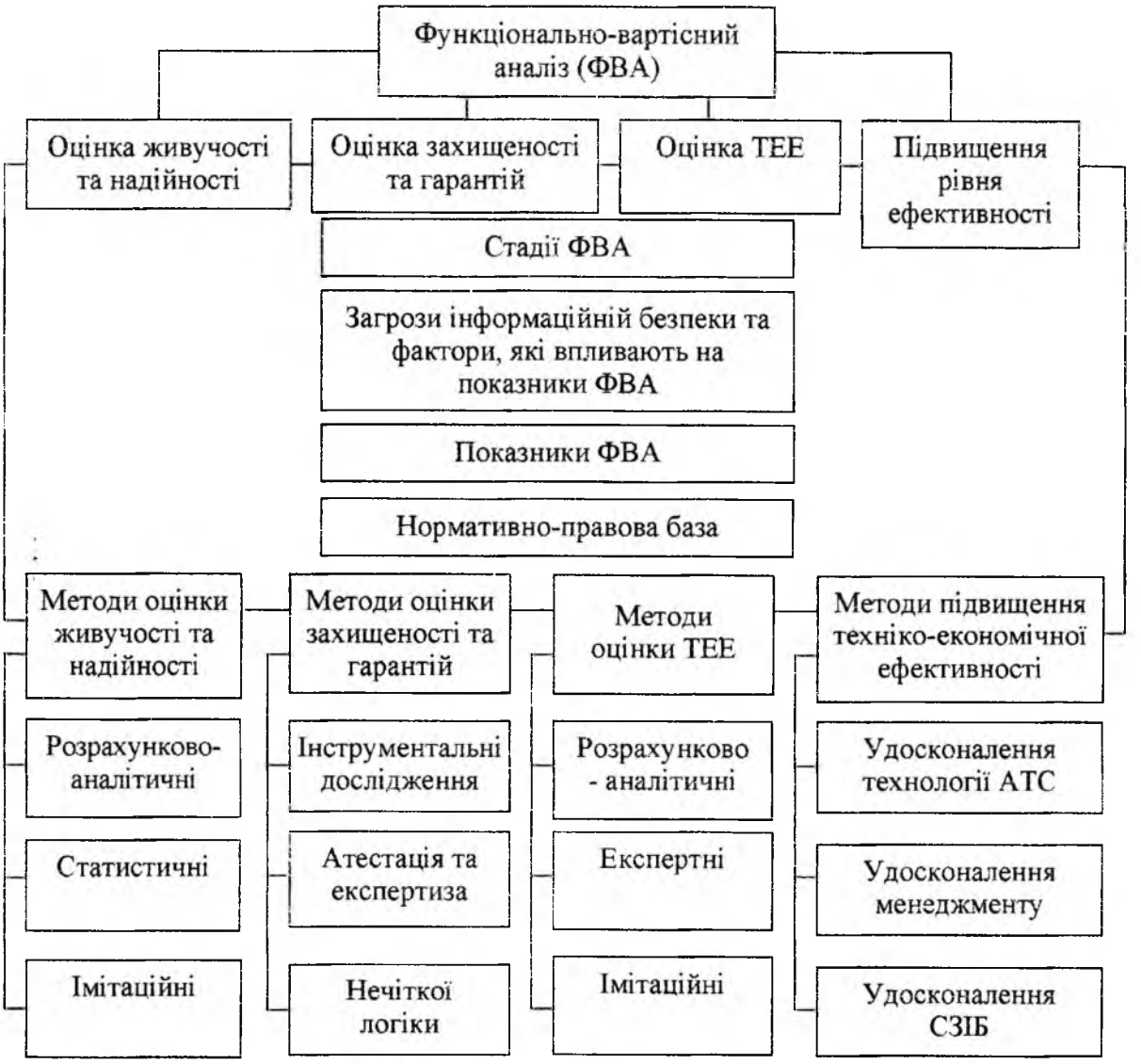

Рис.1 Задачі функціонально-вартісного аналізу

В цілому, напрямки розвитку систем інформаційної безпеки визначаються тенденціями розвитку телекомунікацій в бік цифровізації, пакетизації (застосування IP-технологій), інтеграції й конвергенції мереж йінформаційних і телекомунікаційних технологій, мультисервісності, реалізації сенсорних мереж і "інформаційної матриці 21 століття" [9]. Указані тенденції підвищують значення і роль функціонально-вартісного аналізу.

До факторів, що впливають на показники функціонально-вартісного аналізу відносяться:

– функціональне призначення та структуризація – об'єкт інформаційної діяльності, комплексна система інформаційної безпеки, комплекс засобів протидії загрозі, засіб захисту;

– характеристики циркулюючої інформації – обсяги, тип та категорії;

– організація керування та інструментального контролю інформаційної безпеки: ручне, автоматизоване.

Показники та обмеження функціонально-вартісного аналізу поділяють на якісні, структурні та кількісні. До якісних та структурних показників відносяться: працездатність,

захищеність, гарантії реалізації, функціональна повнота, комплексність, ергономічність, технологічність, наявність сертифікату, атестату відповідності або експертного висновку. Кількісні показники можна поділити на матеріальні, часові, вартісні.

Для вирішення деяких з задач функціонально-вартісного аналізу не можуть бути застосовані повністю формалізовані методи і алгоритми, пошук однозначних відповідностей. Процес аналізу є неоднозначним і його результати не будуть наперед визначеними. Найбільшими труднощами аналізу є задачі оцінки захищеності й якості.

Пропонується кількісна методика обґрунтування витрат на інформаційну безпеку (точніше техніко-економічної ефективності), яка заснована на методах функціонально-вартісного аналізу та повернення інвестицій на безпеку (Return on Investment for Security) і поєднує оцінку витрат з оцінками очікуваних загроз, ризику і втрат.

Фінансова вигода забезпечується щорічними збереженнями, які отримані при впровадженні системи інформаційної безпеки.

$$А_{щзб}=А_{втр}\,Е - А_{вит}$$

де: $А_{щзб}$ – величина щорічних збережень; $А_{втр}$ – показник очікуваних втрат;

Е – коефіцієнт ефективності системи захисту; $А_{вит}$ – щорічні витрати на інформаційну безпеку.

Величина коефіцієнту ефективності системи захисту Е може бути знайдена на підставі таких міркувань. Психологічні дослідження показують, що 10...15% людей не схильні до злочинів при будь-яких обставинах [10]; приблизно така ж кількість людей здатна коїти злочини незважаючи на можливість покарання; остання частка людей може коїти злочини, якщо після скоєння не наступає невідворотно покарання. Тому вже сам факт чи знання, що система захисту введена в дію, зменшує імовірність реалізації загроз зловмисниками. Відомо, що з огляду все ширшого впровадження систем захисту вповільнювало зростання кількості атак на корпоративні мережі, а в деякі періоди навіть зменшувало кількість атак. Тому можна прийняти, що відразу після введення в дію системи захисту коефіцієнт її "психологічної" ефективності Е = 0,85.

Визначення показника очікуваних втрат $А_{втр}$ засноване на знанні Власником цінності своєї інформації та емпіричних відомостях про вторгнення, про втрати від вірусів, про відбиття атак на ресурси тощо. Порушення безпеки може призводити до фінансових втрат, пов'язаних з: простоями та виходом з ладу мережного обладнання; нанесенням шкоди іміджу та репутації підприємства; оплатою робіт з відновлення функціонування системи, програмного забезпечення тощо; витратами по судочинству тощо.

Для одержання оцінки очікуваних втрат використовують таблицю оцінки загроз та ризиків, яка дає можливість кількісно оцінити імовірності подій. В таблиці взаємопов'язуються імовірності загроз, ступінь небезпечності загроз і частота подій. Показник $А_{втр}$ обчислюється за формулою:

$$А_{втр} = f*L\,,$$

де: f – частота виникнення потенційної загрози, рівень якої визначається на основі імовірності загроз; L – величина втрат у гривнях, яка визначається на основі небезпечності порушення.

Витрати на створення системи інформаційної безпеки поділяють на одноразові та періодичні. Одноразові витрати складаються з витрат на закупівлю апаратних засобів, програмного забезпечення, проектування системи. Періодичні витрати складаються з витрат на технічне обслуговування та супроводження, заробітну плату персоналу, навчання та підвищення кваліфікації спеціалістів, витрат на дослідження загроз порушення політики безпеки.

Таким чином, у даній публікації запропоновано конкретні етапи та задачі функціонально-вартісного аналізу для системи інформаційної безпеки АТС. Функціонально-вартісний аналіз на всіх стадіях життєвого циклу АТС дозволяє виділити область раціональних рішень, сформувати проектні процедури знаходження оптимальних рішень, оцінки системи інформаційної безпеки та обґрунтування витрат на систему захисту. Напрямком подальших досліджень може бути розробка методології функціонально-вартісного аналізу та способів вирішення основних задач об'єктно-орієнтованого проектування та задач наступних етапів і стадій життєвого циклу систем інформаційної безпеки АТС. Зокрема, практичним напрямом роботи є розробка методики обґрунтування ефективності витрат на інформаційну безпеку.

Література:

1. Петренко С.А., Терехова Е.М. Оценка затрат на защиту информации. // "Защита информации, INSIDE". - 2005. - № 1. - С.36 – 48.
2. Петренко С.А., Терехова Е.М. Обоснование инвестиций в безопасность. // "Защита информации, INSIDE". – 2005. - № 1. - С.49 – 53.
3. Петренко С.А., Курбатов В.А. Оценка эфективности и зрелости технологий безопасности. // "Защита информации, INSIDE". – 2005. - № 1. - С.49-53.
4. Кононович В.Г., Тардаскіна Т.М. Функціонально-вартісний аналіз системи забезпечення інформаційної безпеки телекомунікаційної мережі загального користування. // "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні",. – 2005. - вип. 11. - С.19-28.
5. Тардаскіна Т.М. Оцінка витрат на інформаційну безпеку цифрових систем комутації. // „Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні". – 2005. - вип.. 10. - С.28-35.
6. Порядок захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах. Затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 24.12.2001 р. № 76. // Зареєстровано в Міністерстві юстиції України 11.01.2002р. за №27/6315.
7. НД ТЗІ 1.1-001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення. Введ. 01.07.99. –К.: ДСТСЗИ СБ України, 1999. – 26 с.
8. НД ТЗІ 1.1-001-99. Типове положення про службу захисту інформації в автоматизованій системі. Затверджене наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 04.12.2000 р. Введ. 01.07.99. – К.: ДСТСЗИ СБ України, 1999. – 20 с.
9. Леваков А. Анатомия информационной безопасности США. Jet Info online №6 (109) 2002, http://daily.sec.ru/dailypblshow.cfm?rid=9&pid=5503 &pos=13&stp=10. С. 74.
10. Гостев И.М., Поволоцкий А.М. Защита традиционного документооборота нетрадиционными средствами. Зашита информации. INSIDE. – 2005. - № 3. – С. 22 – 24.

Рекомендовано до публікації
д.е.н., проф. Орловим В.М. 14.12.05

Надійшла до редакції
28.11.05