Systems, and Technology. 1997. 4. «Використання макросів в Microsoft Office» http://itc.ua/articles/ispolzovanie_makrosov_v_microsoft_office_28520. 4. Цифрова стеганографія / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – 2002. 5. Стеганографічні методи захисту інформації / С.В. Ярмолик, Ю.Н. Листопад.

УДК 004. 056

Г.В. Микитин[1, 2]
[1]Національний університет "Львівська політехніка",
[1]кафедра захисту інформації,
[2]Фізико-механічний інститут ім. Г.В. Карпенка

СИСТЕМНА, НОРМАТИВНА, КОМПЛЕКСНА МОДЕЛІ ЗАХИСТУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

© Микитин Г.В., 2011

Розроблено системну, нормативну, комплексну моделі захисту інформаційних технологій на основі концепції об'єкт – загроза – захист – управління.

Ключові слова: захист, інформаційні технології, концепція, моделі: системна, нормативна, комплексна.

A system, normative, complex information technology security models based on the subject – threat – security – management concept.

Key words: security, information technology, concept, models – systemic, normative, complex.

Актуальність створення системної, нормативної, комплексної моделей захисту інформаційних технологій. Основою інформаційної безпеки інфраструктур суспільства та національної безпеки держави є концепція технічного захисту інформації в Україні [1]. Вирішення конкретної проблеми у відповідній предметній сфері потребує процедури управління. Наприклад, моніторинг параметрів екосистем навколишнього середовища за допомогою інформаційних систем координується управлінням на двох узгоджених рівнях – самого моніторингу, екологічної політики держави. Технічний захист інформації адекватно до потенційних загроз її безпеки, системи захисту має процедуру управління захистом, узгоджену з управлінням інформаційною безпекою на рівні державних інфраструктур.

Концепція об'єкт – загроза – захист – управління щодо безпеки ІТ має деякі аспекти. Розглянемо їх. Сьогодні провідними засобами розв'язання науково-технічних задач фундаментального та прикладного характеру є інформаційні, комунікаційні, інформаційно-комунікаційні технології. Інформаційна технологія – це задана і керована процедура (конструктивний алгоритм) представлення інформаційних процесів (ІП) з використанням відповідних інформаційних ресурсів (ІР) та інформаційних систем (ІС). Відповідно безпеку ІТ можна розглядати з позиції структури взаємозв'язку та взаємодії інформаційної технології і системи, інформаційних ресурсів і процесів, каналів зв'язку та каналів побічного електромагнітного випромінювання та наведення (КЗ/КПЕМВН), елементів управління (У).

Концепція безпеки ІТ і структура взаємозв'язку та взаємодії елементів знаходяться на рівні взаємовідношення. Концепція проектується на структуру взаємозв'язку: ІТ та ІС; ІР та ІП; КЗ/

Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua

КПЕМВН та У та формує безпеку ІТ: об’єкти захисту – ІР, ІС, ІП, КЗ/КПЕМВН, У; моделі загроз на рівні – ІР, ІС, ІП, КЗ/КПЕМВН; моделі захисту на рівні – ІР, ІС, ІП, КЗ/КПЕМВН; управління системою захисту на рівні – ІР, ІС, ІП, КЗ/КПЕМВН. Наприклад, для об’єкта – інформаційні процеси – захист даних відбувається на рівні алгоритмічних процедур (рис. 1). Загалом проблемі безпеки ІТ присвячується: розроблення законів і правил [2, 3], нормативних документів [4, 5]; діяльність технічних комітетів стандартизації [6]; реалізація проектів програм наукових досліджень НАН України; написання фундаментальних монографій і прикладних наукових праць, в яких викладено усталені підходи, стандартизовані методології, проаналізовано моделі загроз та запропоновано моделі захисту даних в інформаційно-комунікаційних технологіях [7–12].

Метою роботи є створення системної, нормативної, комплексної моделей захисту ІТ. Системна модель дає відповідь на запитання – що і як потрібно розробити для системи безпеки ІТ. Нормативна модель показує, на основі яких стандартів функціонуватиме ця система безпеки. Комплексна модель є підґрунтям для відповіді на запитання – чим реалізувати систему безпеки ІТ.

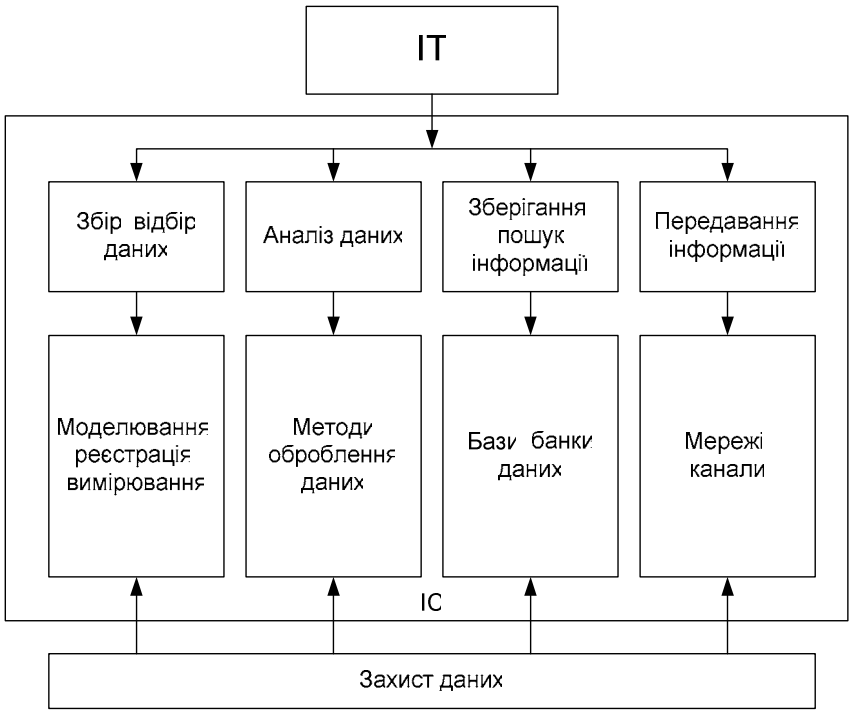

Рис. 1. Безпека ІТ на рівні алгоритмічних процедур

Системна модель захисту інформаційних технологій. На основі принципів системного аналізу: цілісності, ієрархічності, багатоаспектності пропонується системна модель захисту даних в інформаційних технологіях. Принцип цілісності передбачає інтеграцію (об’єднання) частин цілого і проявляється в появі нових властивостей (ознак, параметрів, характеристик, фізичних величин) цілого, які відсутні у його частинах. Принцип ієрархічності надає можливість точно виділити істотні властивості і взаємозв’язки складного об’єкта, що забезпечує докладний опис його властивостей за рахунок використання апріорних знань про внутрішню будову об’єкта. Принцип багатоаспектності вимагає розгляду об’єкта з різних точок зору з урахуванням взаємозв’язків виявлених аспектів. В основу такої моделі покладено концепцію захисту даних: об’єкт – загроза – захист – управління.

Системна модель захисту ІТ представлена у вигляді тривимірного простору *x-y-z*, охопленого сферою (рис. 2). У площині *x-z* знаходяться об’єкти захисту: інформаційні ресурси, інформаційні системи, інформаційні процеси, канали зв’язку та канали побічного електромагнітного випромінювання і наведення, елементи управління. У площині *y-z* представлені рівні моделей

Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua

загроз адекватно до об'єктів захисту, що у площині *x-z*. У площині *x-y* представлена система захисту інформаційних технологій (СЗІТ) адекватно до об'єктів захисту та моделей загроз. Стратегічна структура СЗІТ така: засади – законодавчі, нормативно-методологічні, наукові; моделі захисту; напрямки; методології, способи, методи; засоби СЗІТ – технічні (апаратні, фізичні), програмні. Подання об'єкта захисту – інформаційних технологій п'ятьма взаємозв'язаними підсистемами: ІР; ІС; ІП; КЗ/ КПЕМВН; У дає змогу формувати моделі загроз для цих підсистем та відповідні моделі їх захисту на законодавчій, нормативній та науковій основах, не порушуючи концепції об'єкт – загроза – захист – управління для відповідного класу ІТ.

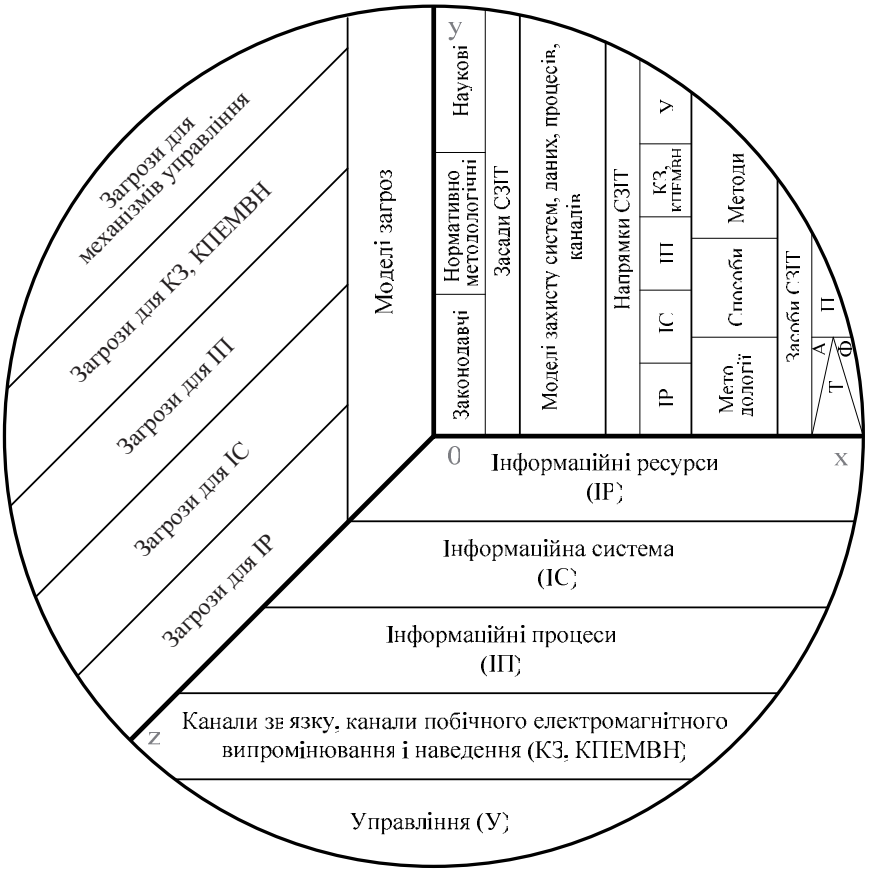

Рис. 2. Системна модель захисту інформаційних технологій

Вихідним аспектом забезпечення міцності комплексного захисту ІТ є інформаційні ресурси, ступінь їх цінності та гриф таємності. При створенні моделі загроз для ІТ необхідно враховувати такі елементи:

- загрози як намір нанесення шкоди інформації шляхом порушення її цілісності, конфіденційності або заволодіння нею у корисних цілях;
- джерела загроз, які класифікуються за природою виникнення: випадковість, навмисне заволодіння, нанесення шкоди інформації тощо;
- цілі загроз, орієнтовані на такі ознаки інформації, як конфіденційність, цілісність, доступність;
- способи несанкціонованих дій (НСД) – підходи, які характеризують процес розглядання конкретної фізичної загрози для певного виду інформації.

Моделі захисту ІТ орієнтовані на:

- законодавчі, нормативно-методологічні, наукові засади, які системно формують: основні принципи технічного захисту інформації, норми та вимоги, порядок проведення робіт та

Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua

здійснення контролю його ефективності; концепції і моделі безпеки ІТ; управління та планування безпеки; методи управління захистом ІТ;

- напрямок безпеки ІТ – ІР; ІС; ІП; КЗ/ КПЕМВН; У, для кожного з яких обґрунтовуються критерії вибору (створення) методології, способу, методу, засобів СЗІТ з метою оптимізації проведення робіт із захисту даних;
- технічні і програмні засоби захисту ІТ: технічні пристрої – електричні, електромеханічні, електронні забезпечують секретність інформації, захист від модифікації, контроль даних; програмні засоби захисту – антивірусні програми, системи виявлення атак, контролери мережевого трафіку, комплексні системи захисту, програмні методи шифрування, методи маскування, автентифікації інформації, методи цифрового підпису тощо забезпечують розмежування доступу та виключають несанкціоноване використання інформації.

Системна і нормативна моделі є підґрунтям для комплексної моделі захисту ІТ. Згідно з [4], проблема захисту інформації стратегічно представлена двома векторами: захист інформації від несанкціонованого доступу (НСД); захист інформації від витоку технічними каналами (побічного електромагнітного випромінювання і наведення, оптичними, акустичними, радіотехнічними тощо) та каналами спеціального впливу (сформованими фізичними полями і сигналами).

Комплексний захист ІТ від НСД до інформації та від її витоку можливими каналами на основі структури взаємозв'язку і взаємодії ІТ та ІС, ІР та ІП, КЗ та У здійснюється на рівнях: методологічного, апаратного-фізичного (технічного), програмного, комунікаційного, управлінського забезпечення.

3. Нормативна модель захисту інформаційних технологій. Нормативну модель захисту ІТ зображено у вигляді зрізаної піраміди, кожна сторона якої відповідає функціональним рівням системи захисту інформаційних технологій: А – методологічному, В – технічному (апаратному, фізичному, канальному), С – програмному, D – метрологічному (рис. 3).

Стандарти 1 – n є нормативною базою у сфері захисту ІТ згідно з функціональними рівнями. До них належать: державні стандарти України ДСТУ; державні стандарти України, гармонізовані з міжнародними ДСТУ ISO/IEC; міждержавні стандарти ГОСТ; міждержавні, гармонізовані з міжнародними ГОСТ Р ИСО/МЭК; міжнародні стандарти ISO (Міжнародна організація зі стандартизації), IEC (Міжнародна електротехнічна комісія), ITU (Міжнародний союз телекомунікацій) тощо; національні стандарти організацій зі стандартизації окремих країн BSI, DIN, ANSI т. і.; регіональні стандарти організацій, які представляють у глобальному процесі стандартизації інтереси великих регіонів або континентів CEN (Європейський комітет стандартизації), CENELEC (Європейський комітет стандартизації в електротехніці) т. і.; стандарти промислових консорціумів та професійних організацій ICC, API т. і.

Методологічний рівень представляє підхід до захисту інформаційних технологій – концепції, моделі, методології захисту даних та управління захистом ІТ. Технічний (апаратний, фізичний, канальний) – апаратні пристрої, які впроваджені в апаратуру оброблення даних; пристрої, узгоджені з нею через інтерфейс; автоматичні пристрої і системи – елементи електронно-механічного обладнання охоронної сигналізації, замки тощо; канали витоку інформації. Програмний рівень – це відповідно спеціалізовані програми, призначені для захисту ІТ. Метрологічний рівень розкривають елементи: метрологічної атестації, випробувань, стандартизації і сертифікації технічних і програмних засобів захисту інформації.

Аспекти метрологічного рівня необхідно розглядати відповідно до нормативного документа [4], де окреслені етапи побудови системи захисту інформації в ІТ: визначення й аналіз загроз; розроблення системи захисту інформації; реалізація плану захисту інформації; контроль функціонування та керування системою захисту інформації.

Реалізація цих етапів потребує: проведення метрологічної експертизи технічного завдання на розроблення системи захисту інформації; обґрунтування критеріїв вибору засобів вимірювальної

Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua

техніки (ЗВТ), які комплектують систему захисту ІТ; розроблення рекомендаційних вимог до метрологічних характеристик ЗВТ, проведення метрологічної атестації (МА) ЗВТ; розроблення методик виконання вимірювань параметрів фізичних полів та сигналів з метою оцінювання імовірності витоку інформації технічними каналами та каналами спеціального впливу на систему; проведення МА системи захисту інформації згідно із стандартизованими методиками виконання вимірювань.

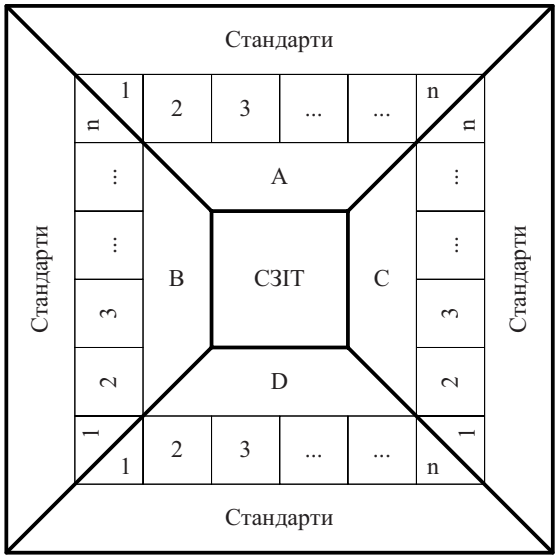

Рис. 3. Нормативна модель захисту інформаційних технологій

Безпека ІТ представляє питання стандартизації та сертифікації засобів технічного захисту інформації. У цьому напрямі в Україні діють технічні комітети (ТК): інформаційні технології (ТК-20) з 1995 р., технічний захист інформації (ТК-107) з 2008 р. Серед основних елементів структури ТК-20: телекомунікації та обмін інформацією між системами; інженерія програмних засобів, автоматична ідентифікація та методи роботи з даними; управління даними та обмін; мови програмування та системний інтерфейс; коди та кодування інформації; оброблення, кодування та передавання звуків і зображень; методи та засоби безпеки в інформаційних технологіях; інформаційні та комунікаційні технології навчання; біометрія, мікропроцесорні системи; автоматизовані системи. Структура ТК-107 – технічний захист інформації така: архітектура та побудова систем безпеки інформаційно-комунікаційних технологій (ІКТ); служби (та послуги) систем безпеки в ІКТ; безпека глобальних ІКТ.

4. Комплексна модель захисту інформаційних технологій. Комплексна система захисту інформаційних технологій (КСЗІТ) представлена у вигляді ієрархічних сфер, в яких закладені п’ять рівнів захисту даних в ІТ (рис. 4).

Першим рівнем КСЗІТ є самі об’єкти захисту – інформаційні ресурси; інформаційні системи; інформаційні процеси; канали зв’язку та канали побічного електромагнітного випромінювання і наведення, управління безпекою.

Другий рівень – підхід до захисту, що відображає застосування відповідних принципів захисту даних – ступінь секретності інформації – *1*; апаратні та фізичні засоби захисту інформації – *2*; етапи життєвого циклу інформації в інформаційній системі – *3*; комплекс взаємозв’язку, взаємовідношення, взаємодії змінних в часі елементів, умов, факторів, які впливають на безпеку ІТ – *4*; елементи управління безпекою ІТ – *5.*

Третій рівень – КСЗІТ, представлена такими підсистемами захисту даних: методологічною – *I;* технічною – *II*; програмною – *III;* комунікаційною – *IV*; управлінською – *V*. Кожна підсистема КСЗІТ має відповідне нормативне забезпечення. Наприклад, рівень управлінського забезпечення захисту ІТ ґрунтується зокрема на таких нормативних документах:

Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua

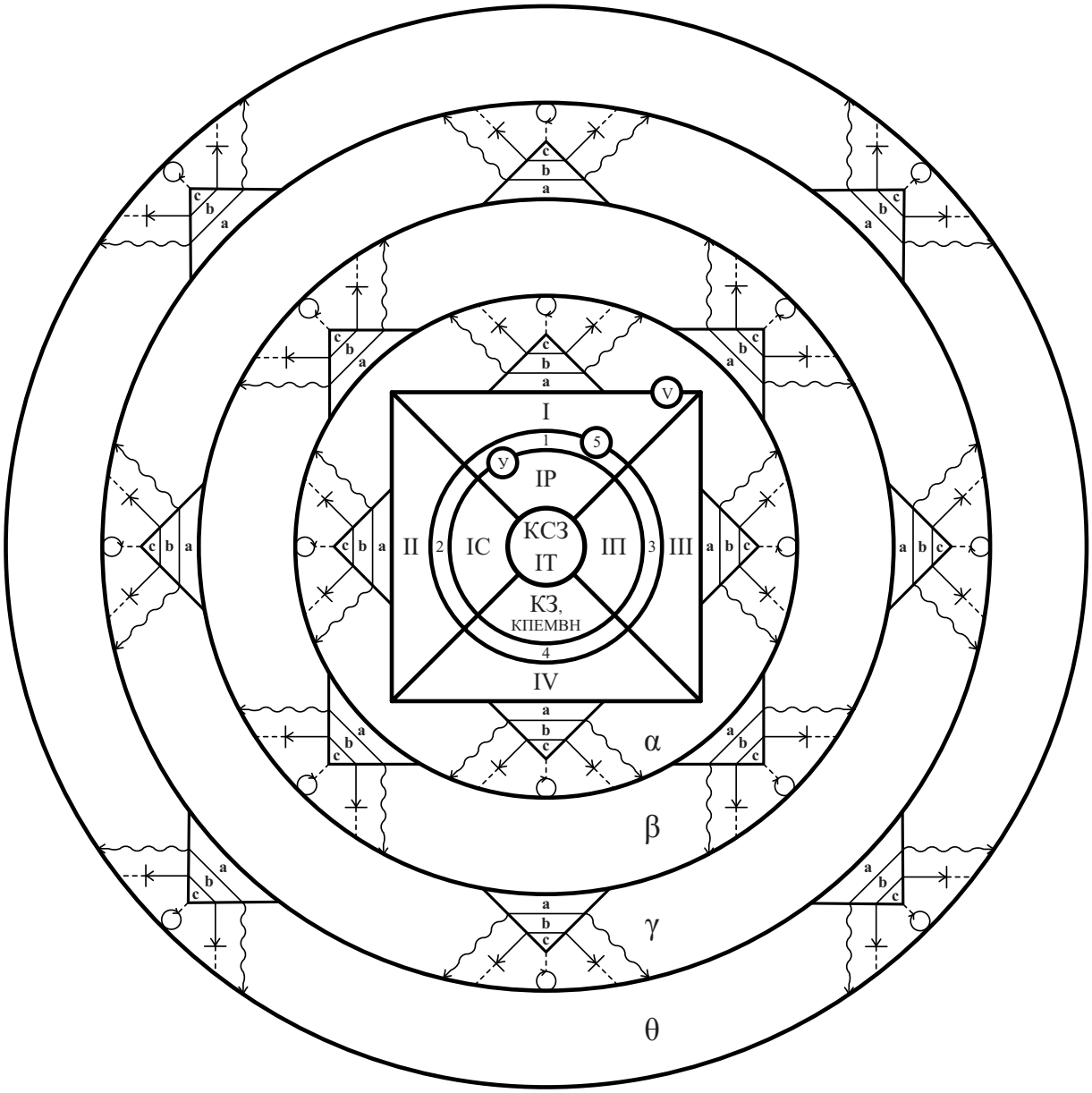

Рис. 4. Комплексна модель захисту інформаційних технологій

ДСТУ ISO/IEC TR 13335-1 – Інформаційні технології. Настанови з керування безпекою інформаційних технологій (ІТ). Частина 1. Концепції й моделі безпеки ІТ

ДСТУ ISO/IEC TR 13335-2 – Інформаційні технології. Настанови з керування безпекою інформаційних технологій (ІТ). Частина 2. Керування та планування безпеки ІТ

ISO/IEC TR 13335-3 – Інформаційні технології. Настанови з керування безпекою інформаційних технологій (ІТ). Частина 3. Методи керування захистом ІТ.

Четвертий рівень – захисні пояси, які відображають характер захисту інформації: зовнішній пояс, який охоплює всю територію, де розташовані будівлі, що містять інформаційні технології – α; пояс будівель (приміщень), або пристроїв ІТ – β; пояс компонентів системи і технічних засобів, програмного забезпечення, елементів баз даних – γ; пояс технологічних процесів оброблення інформації (введення, виведеннч, внутрішнє оброблення тощо) – θ.

П’ятий рівень – комплекс методів і засобів протидії потенційним загрозам на рівні: виявлення – *a*; блокування – *b;* нейтралізації – *c.*

Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua

Висновки. 1. Створена системна модель захисту ІТ на основі концепції: об'єкт – загроза – захист – управління дає змогу враховувати взаємозв'язок та взаємодію інформаційної технології і системи; інформаційних ресурсів і процесів; каналів зв'язку / каналів побічного електромагнітного випромінювання і наведення та елементів управління безпекою і на цій основі розробляти моделі загроз та адекватні до них моделі захисту.

2. Створена нормативна модель безпеки ІТ на основі рівнів методологічного, технічного, програмного, метрологічного забезпечення захисту даних, що дає змогу використовувати стандартизовані підходи, методології, способи, методи, засоби захисту ІТ або розробляти нові, уніфікувати їх на основі системної моделі та стандартизувати.

3. Створена комплексна модель системи захисту ІТ на основі п'яти рівнів безпеки: об'єкти захисту; підхід до захисту; підсистеми захисту; зовнішні і внутрішні пояси захисту; методи і засоби виявлення, блокування і повної нейтралізації загроз. Модель дає змогу реалізувати на практиці систему безпеки ІТ на основі: ступеня цінності ІР, взаємозв'язку і взаємодії ІР, ІС, ІП, КЗ/КПЕМВН, У, концепції об'єкт – загроза – захист – управління, тим самим забезпечити цілісність, конфіденційність і доступність інформації.

4. Запропоновані системна, нормативна, комплексна системи захисту ІТ впроваджені у сферу безпеки інформаційно-комунікаційних технологій. У роботі [11] запропоновано концептуальні моделі захисту інформації для комунікаційних технологій стаціонарного, стільникового, супутникового зв'язку на фізичному, канальному, мережевому, системному рівнях. У роботі [12] запропоновано автоматизовану систему оброблення інформації з обмеженим доступом "Захист аудіоінформації" на основі: концептуальної моделі: реєстратори – канали витоку – засоби захисту аудіоінформації.

1. Концепція технічного захисту інформації в Україні. Затверджено постановою Кабінету Міністрів України від 8 жовтня 1997 р. № 1126 // Урядовий кур`єр, 12.11.1997. 2. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" // Відомості Верховної Ради України, 2005, № 26, ст. 347. 3. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних, інформаційно-телекомунікаційних системах / Затверджено постановою КМУ від 29.03.2006 № 373/ http://www.kmu.gov.ua. 4. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення. – К.: ДСТСЗІ СБ України, 1997. 5. НД ТЗІ 2.1-001-2001 Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення. 6. Технічні комітети стандартизації України. Каталог / Уклад. Т.Б. Гордієнко. – К.: ДП "УкрНДНЦ", 2010. – 213 с. 7. Головань С.М., Дудикевич В.Б., Зачепило В.С., Пархуць Л.Т., Щербак Л.М. Документаційне забезпечення робіт із захисту інформації з обмеженим доступом. – Л.: Вид-во Нац. ун-ту "Львівська політехніка", 2005. – 288 с. 8. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации. – К.: Юниор, 2003. – 504 с. 9. Пасічник В.В., Жежнич П.І., Кравець Р.Б., Пелещишин А.М., Тарасов Д.О. Глобальні інформаційні системи та технології: моделі ефективного аналізу, опрацювання та захисту даних. – Л.: Вид-во Нац. ун-ту "Львівська політехніка", 2006. – 348 с. 10. Домарев В.В. Безопасность информационных технологий. Системный подход. – К.: ООО ТИД ДИА Софт, 2004. – 992 с. 11. Микитин Г.В. Концептуальні моделі захисту інформації для технологій стаціонарного, стільникового, супутникового зв'язку / В.Б. Дудикевич, Ю.Р. Гарасим, Г.В. Микитин // Вісник Нац. ун-ту "Львівська політехніка". – 2010. – № 665: Автоматика, вимірювання та керування. – С. 18–26. 12. Микитин Г.В. Автоматизована система обробки інформації "Захист аудіоінформації": реєстратори, канали витоку, засоби захисту / В.Б. Дудикевич, Г.В. Микитин, Ю.Р. Гарасим // Вісник Нац. ун-ту "Львівська політехніка". – 2010. – № 685: Комп'ютерні системи проектування. Теорія і практика. – С. 156–167.

Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua