УДК 004.056

В.Б. Дудикевич[1], Л.С. Сікора[2],
Г.В. Микитин[1], О.Я. Рудник[1]
[1]Національний університет "Львівська політехніка",
кафедра "Захист інформації",
79013, м. Львів, вул. С. Бандери, 12
[2]Національний університет "Львівська політехніка",
кафедра "Автоматизовані системи управління",
79013, м. Львів, вул. С. Бандери, 12

МЕТОДОЛОГІЯ ЗАХИСТУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Methodological principles of information technology protection data processing, management, decision support, expert systems, based on the model object – hazard – safety and on the principle of security system integrity at the level of interaction between information resources, systems, processes, networks (channels), lifecycle management and safety management were proposed.

Keywords - information technology, resources, systems, processes, network, management, hazard, safety.

Запропоновано методологію захисту інформаційних технологій оброблення даних, управління, підтримки прийняття рішень, експертних систем на основі моделі об'єкт – загроза – захист та принципу цілісності системи безпеки на рівні взаємодії інформаційних ресурсів, систем, процесів, мереж (каналів), управління життєвим циклом та захистом.

Ключові слова - інформаційні технології, ресурси, системи, процеси, мережі, управління, загроза, захист.

Вступ

Згідно класифікації інформаційних технологій (ІТ) найбільш використовувані на практиці – за ступенем охоплення завдань управління у різних предметних сферах [1,2,3]. Інформаційні технології оброблення даних, управління, автоматизації офісу, підтримки прийняття рішень, експертних систем використовуються для вирішення прикладних задач – неруйнівного контролю і технічного діагностування матеріалів та конструкцій, моніторингу екосистем довкілля, космічних досліджень стану навколоземного простору, зокрема прогнозування впливу сонячної активності на біосферу і людину і т. і. [4]. Відповідно актуальним є створення ієрархічної структури рівнів інформаційної технології як синтезу методів і засобів, об'єднаних алгоритмом основних процесів збору/ відбору, оброблення, представлення інформаційних ресурсів. Така постановка задачі дає можливість враховувати прикладні аспекти збору/ відбору і оброблення різнорідних даних від об'єктів дослідження відповідно до ступеня секретності інформації та представлення в її базах даних, сховищах даних, базах знань, базах моделей, масивах. Окрім того, інформаційним процесам у фазах – збору/ відбору, передавання, оброблення, зберігання, представлення властиві загрози витоку, модифікації, втрати даних про стан досліджуваних об'єктів зокрема, особливого призначення. Метою роботи є – розроблення методології комплексної системи безпеки інформаційних технологій із застосуванням принципу системного ефекту – емерджентності, який обумовлює цілісність захисту на основі ієрархічної структури рівнів ІТ.

1. Інформаційні технології: ієрархічна структура рівнів

В роботах [5,6] представлені системна, нормативна і комплексна моделі захисту інформаційних технологій. Для врахування відповідних задач у предметних сферах інформаційні технології – оброблення даних $(IT)_1$, управління $(IT)_2$, автоматизації офісу $(IT)_3$, підтримки прийняття рішень $(IT)_4$, експертних систем $(IT)_5$ доцільно представити системою взаємозв'язку та взаємодії рівнів (рис.1): інформаційних ресурсів (ІР) – баз даних (БД), сховищ даних (СД), баз знань (БЗ), баз моделей (БМ), масивів інформації (МІ); інформаційних систем (ІС) – інформаційно-аналітичних систем (ІАС), вимірювальних інформаційних систем (ВІС), автоматизованих систем управління (АСУ), систем автоматизації офісу (САО), систем підтримки прийняття рішень (СППР), експертних систем (ЕС); інформаційних процесів (ІП); інформаційних мереж (каналів) (ІМ (К)); комплексного управління (У) – життєвим циклом, системою безпеки ІТ.

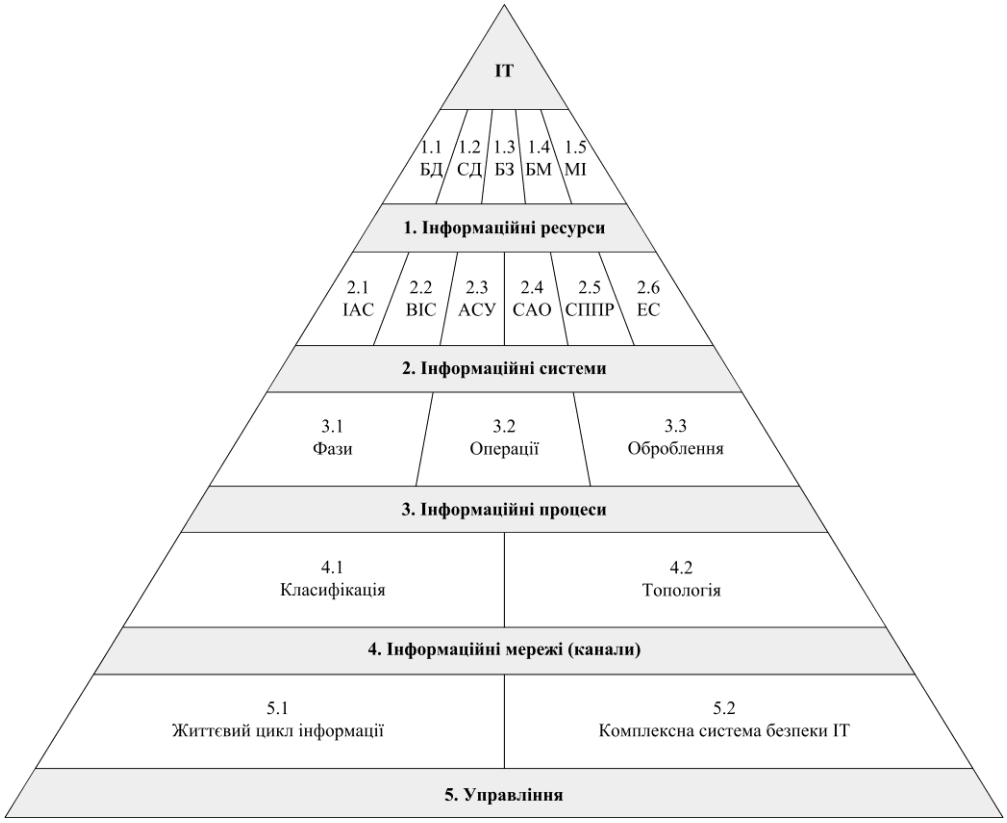

Рис. 1. Ієрархічна структура рівнів інформаційних технологій

2. Методологія захисту інформаційних технологій

Структура методології захисту інформаційних технологій. Значного підвищення безпеки відповідної ІТ можна досягти шляхом багаторівневої побудови системи захисту. В цьому випадку імовірна загроза зможе впливати на захищену ІТ тільки у разі подолання всіх рівнів захисту. Пропонується методологія захисту інформаційних технологій: оброблення даних (1); управління (2); автоматизації офісу; підтримки прийняття рішень (3); експертних систем (4) на основі системної, нормативної, комплексної моделей захисту даних. Структура методології безпеки ІТ створена на моделі об'єкт – загроза – захист [7]. Комплексність безпеки інформаційних технологій обумовлює необхідні рівні захисту ІР, ІС, ІП, ІМ(К), У.

До складу комплексного захисту інформації входять заходи і засоби, які реалізують способи, методи, механізми захисту інформації від: витоків технічними каналами; несанкціонованих дій і несанкціонованого доступу до інформації; спеціального впливу на інформацію. Методологія комплексної системи безпеки IT_1 – IT_5 представлена п'ятьма рівнями на рис. 2. [8].

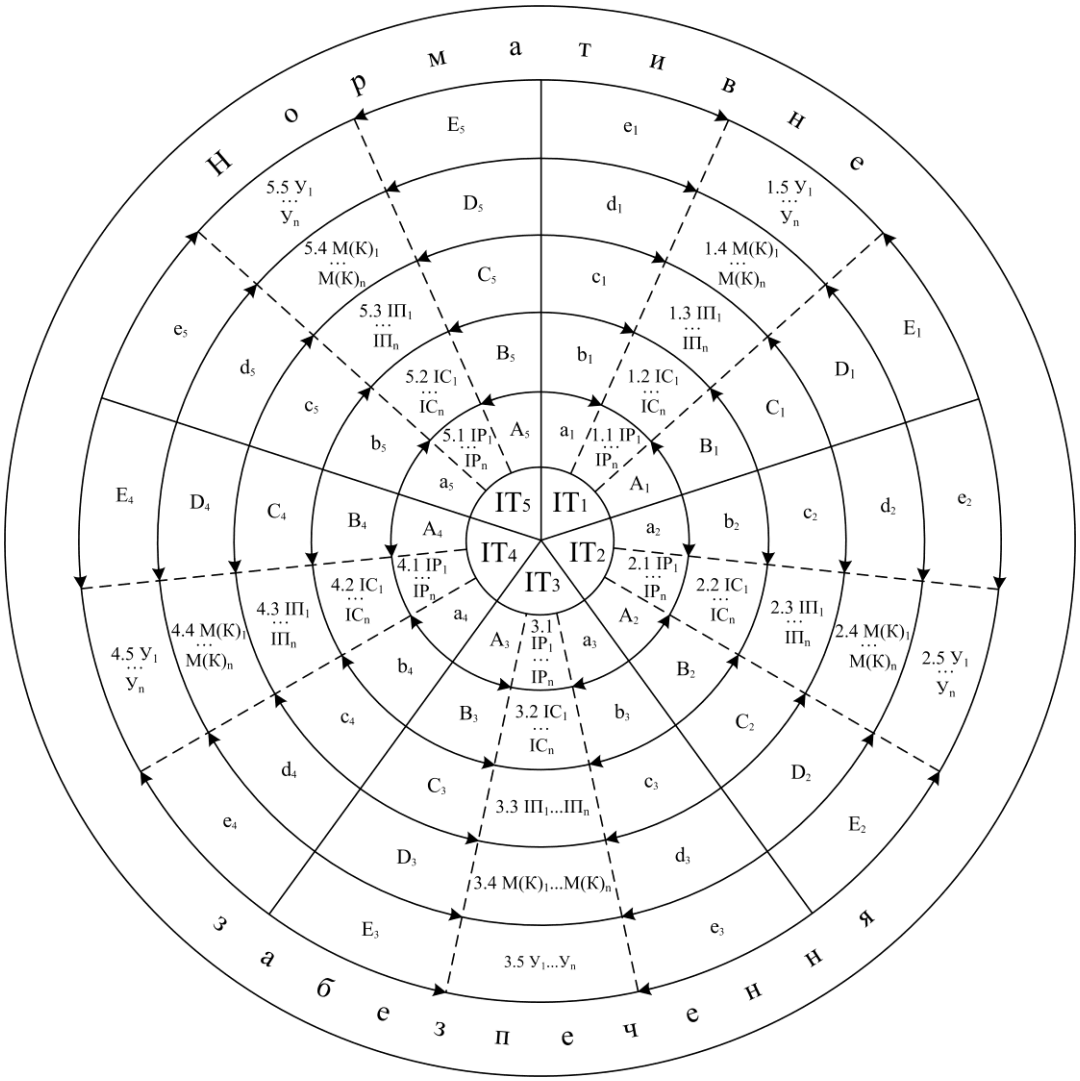

Рис. 2. Структура методології комплексної системи безпеки: IT_1 – оброблення даних, IT_2 – управління, IT_3 – автоматизації офісу, IT_4 – підтримки прийняття рішень, IT_5 – експертних систем

На першому рівні – захисту підлягають ІР: масиви інформації у різних предметних сферах, бази моделей, бази і банки даних у відповідних інформаційних системах. На другому рівні – передбачається захист функціональних апаратних (фізичних, технічних) та програмних елементів конкретної ІС для завдань управління.Третій рівень – передбачає захист ІП, які протікають в ІС: сприйняття/ збір/ відбір, оброблення, зберігання, представлення, передавання інформації, які формують інформаційний зміст фаз, операцій та оброблення даних. Четвертий рівень – передбачає захист ІМ (К) відповідно до їх класифікації та топології для ІАС, АСУ, САО, СППР, ЕС та видів каналів для вимірювальних інформаційних систем. На п’ятому рівні – передбачається управління об’єктом – життєвим циклом інформації, яка функціонує в ІС та управління комплексною системою безпекою ІТ.

Структура методології комплексної системи безпеки інформаційних технологій має властивості цілісності та емерджентності. Цілісність – властивість системи проявляти себе як єдине ціле за умови, що зміни параметрів захисту підсистем обумовлюють зміну параметрів безпеки системи в цілому. Імовірні загрози для інформаційних ресурсів як підсистеми відповідно змінюють стан безпеки інших підсистем – ІС, ІП, М(К), У, що формує захист відповідної інформаційної технології у цілому. Емерджентність – властивість системи, що відображає її стан як функцію стану її елементів та взаємозв’язків, взаємовідношень між ними, причому останні надають системі нових властивостей, які не проявляються у вихідному стані

$$C(S) = f(C(n), V(n)), \quad (1)$$

де $C(S)$ – вихідний стан системи, $C(n)$ – стан елементів системи, $V(n)$ – взаємозв'язки, взаємовідношення між елементами системи.

Концепція об'єкт – загроза – захист на рівнях інформаційних технологій. Комплекс загроз (a-b-c-d-e) та комплекс елементів захисту (A-B-C-D-E) взаємозв'язані рівнями інформаційних технологій (1-2-3-4-5) – підсистемами безпеки ІР, ІС, ІП, ІМ(К), У. В табл.1-4 представлений приклад методології захисту для технологій оброблення даних ($ІТ_1$) на другому і п'ятому рівнях – інформаційних систем ($ІС_1$ ...$ІС_n$) і управління життєвим циклом та захистом даних ($У_1$ ... $У_n$) згідно концепції об'єкт – загроза – захист. Відповідно комплексна система безпеки інформаційних технологій представлена

Таблиця 1.

Об'єкт захисту: інформаційні системи

Інформаційні системи					
Інформаційно-аналітичні системи (ІАС)	Вимірювальні інформаційні системи (ВІС)	Автоматизовані системи управління (АСУ)	Системи автоматизації офісу (САО)	Системи підтримки і прийняття рішень (СППР)	Експертні системи (ЕС)
Класифікація за спектром виконуваних завдань	*Класифікація ВІС за функціональним призначенням*	*Класифікація АСУ за предметними сферами*	*Класифікація за способом реалізації*	*Класифікація за концептуальною моделлю*	*Класифікація за видом вирішуваної задачі*
Інформаційно-пошукові системи	Вимірювальні системи (ВС) - ближньої дії	Управління підприємством (АСУП)	Комп'ютерні офісні технології	Концептуальна модель Спрага	Інтерпретації даних
Системи для професійних аналітиків	Системи автоматичного контролю (САК)	Управління технологічними процесами (АСУ ТП)	Некомп'ютерні офісні технології	Модель еволюціонуючої СППР	Діагностування
Системи підготовки управлінської звітності та контролю	Системи технічного діагностування (СТД)	Проектно-конструкторські (САПР)	*Класифікація за величиною обслуговуваного офісу*	Орієнтовані на знання СППР	Моніторингу
Системи прийняття управлінських рішень	Системи розпізнавання образів (СРО)	*Класифікація АСУ з позицій управління*	Системи для малого офісу	Орієнтовані на правила СППР	Проектування
Класифікація за сферою використання	Телевимірювальні системи (ТВС) – ВС дальньої дії	Децентралізовані	Системи для середнього офісу	Спеціалізовані (прикладні) СППР	Прогнозування
Системи фінансового аналізу	*Класифікація за організацією алгоритму функціонування*	Централізовані	Системи для великого офісу	СППР генератори	Планування
Системи планування бізнес-діяльності	Із жорстким алгоритмом функціонування	Централізовані розосереджені	*Класифікація за функціональними особливостями*	*Класифікація за завданнями*	Навчання
Системи планування та аналізу маркетингу	Програмовані системи	Ієрархічні	Системи управління документами	Унікальні проблеми	Керування
Системи прогнозуван-	Адаптивні системи	*Класифікація структур АСУ за*	Системи управління	Повторювані проблеми	*Класифікація за режимом*

продовж. табл. 2.

ня		*підсистемами забезпечення*	потоком робіт		*роботи*
Класифікація за структурними функціями	*Класифікація ВІС за структурною схемою*	Програмне	Системи управління зображеннями/ образами	Цілісний вибір	Статичні
Тиражовані системи	Ланкові	Інформаційне	Системи формо обігу	Багато-критеріальний вибір	Квазідинамічні
Засоби генерації звітів	Радіальні	Технічне	Системи управління бізнес-процесами	Об'єктивна модель	Динамічні
Інтегровані системи	Магістральні	Математичне	Системи спільної роботи	Суб'єктивна модель	*Класифікація за ступенем інтеграції ПЗ*
Інструменти добування даних	Радіально-ланкові	Лінгвістичне	Системи управління інформацією – портали	Функціонально специфічні СППР	Автономні
Системи оперативного аналітичного оброблення даних (OLAP)	Радіально-магістральні	Організаційне	Системи управління контентом	СППР загального призначення	Гібридні
Операційного (транзакційного) оброблення даних (OLTP)		Методичне	Системи управління виведенням		
Системи аналітичного оброблення даних (DSS)		Правове	Системи управління корпоративним и електронними записами		
Корпоративне сховище даних		Ергономічне	Системи управління знаннями		

Таблиця 2.

Загроза-захист: інформаційні системи

Інформаційні системи : ІАС, ВІС, АСУ, САО, СППР, ЕС	
Загроза b:	Захист В: програмно-технічний
• помилки користувачів; • внутрішні відмови інформаційної системи; • відмова підтримуючої інфраструктури; • неможливість працювати з системою через відсутність відповідної підготовки (нестача загальної комп'ютерної грамотності, невміння інтерпретувати діагностичні повідомлення, невміння працювати з документацією і т. і.); • неможливість працювати з системою через відсутність технічної підтримки (неповнота документації, нестача довідкової інформації тощо); • відступ (випадковий або умисний) від встановлених правил експлуатації;	• захист від стихійних лих; • здійснення за допомогою спеціалізованих давачів автоматизованої процедури виявлення та протидії атакам; • стикування із зовнішніми корпоративними та комерційними інфраструктурами відкритих ключів, побудованих на стандартах відкритих систем; • контроль та обмеження доступу; • захист від несанкціонованого доступу;

продовж. табл. 2.

• вихід системи з штатного режиму експлуатації в силу випадкових чи навмисних дій користувачів чи обслуговуючого персоналу (перевищення розрахункового числа запитів, надмірний обсяг оброблюваної інформації тощо); • помилки при (пере) конфігуруванні системи; • відмови програмного і апаратного забезпечення; • руйнування або пошкодження апаратури; • порушення роботи (випадкове або навмисне) систем зв'язку, електроживлення, водо-та / або теплопостачання, кондиціювання; • руйнування або пошкодження приміщень; • неможливість або небажання обслуговуючого персоналу та/ або користувачів виконувати свої обов'язки (цивільні безлади, аварії на транспорті, терористичний акт або його загроза, страйк і т. і.); • вбудовування "логічної бомби", яка з часом руйнує програми і / або дані;	використання власних аварійних електрогенераторів або резервних ліній електроживлення; • установка джерел безперебійного живлення; • захист від побічного електромагнітного випромінювання і наведень (ПЕМВН); • організація дискових масивів; • зберігання архівних копій інформації.

Таблиця 3.

Об'єкт захисту: управління ІТ – життєвим циклом інформації; захистом

Управління ІТ	
Управління життєвим циклом інформації	Управління комплексною системою безпеки ІТ
Завантаження, оновлення даних	Контроль і усунення програмно-технічних впливів на інформаційні системи (ІС), що призводять до втрати інформації
Обслуговування і оновлення системи та її елементів	Контроль і усунення каналів несанкціонованого доступу до об'єктів ІС
Архівування даних	Контроль, усунення і (або) послаблення витоку інформації каналами ПЕМВН
Адміністрування	Контроль і усунення зняття інформації, що передається по каналах зв'язку
Засоби системного аудиту	Оцінка ефективності заходів із забезпечення режиму секретності та безпеки інформації на об'єктах ІС
Мережевий інформаційний сервіс	Оцінка ефективності заходів із комплексної протидії технічним засобам розвідки
Ядро безпеки	Оцінка ефективності заходів із забезпечення безпеки зв'язку
Управління елементами відбору та реєстрації даних (наприклад, давачами)	Оцінка ефективності функціонування засобів захисту інформації
Моніторинг результатів функціонування системи (режим "реального часу")	
Управління елементами збирання та реєстрації даних	

Таблиця 4.

Загроза – захист: управління КС БІТ

Управління КС БІТ	
Загроза е:	Захист Е: програмно-технічний
• перехоплення паролів; • спроба проникнення в систему;	• організація роботи у відповідності із загальним регламентом; • контроль звернень до захищених компонентів комп'ютерної системи;

продовж. табл. 4.

• створення або зміна записів бази даних захисту; • несанкціоноване отримання та використання привілеїв; • несанкціонований доступ до наборів даних; • установка неперевірених виконуваних модулів і командних процедур, де можуть ховатися “троянські коні”, “черв'яки” і т. і; • “прибирання сміття” на диску або в оперативній пам'яті; • помилки обслуговуючого персоналу та користувачів.	• реагування при несанкціонованих діях (затримка чи відмова обслуговування, сигналізація); • авторизація; • автентифікація; • ідентифікація; • обмеження доступу; • розмежування доступу; • криптографічне перетворення інформації; • використання в якості базової операційної системи - ос з відкритим для користувачів програмним кодом (наприклад, solaris), з якої вилучені не використовувані сервіси та протоколи; • забезпечення обліку та реєстрації подій, значимих для процедур виявлення порушень системи безпеки інформації та моніторингу стану захищеності серверів • парольна ідентифікація користувача за персональним “ключем”; • старт-карти управління доступом.

Висновки

1. Створено ієрархічну структуру рівнів інформаційної технології як єдиний алгоритм функціонування інформаційних ресурсів в інформаційних системах на основі протікання інформаційних процесів в інформаційних мережах (каналах) в рамках управління життєвим циклом інформації і комплексною системою безпеки.

2. Розроблено методологію захисту інформаційних технологій на основі ієрархічної структури рівнів ІТ розкриває системний ефект безпеки відповідно до концепції об’єкт – загроза – захист: система безпеки ІТ (ІР – ІС – ІП – ІМ (К) – У) без підсистем безпеки (наприклад, ІС) не коректна; сутність підсистеми безпеки розкривається не її внутрішнім змістом, а змістом цілої системи безпеки ІР – ІС – ІП – ІМ(К) – У; система безпеки ІТ має ознаки, властиві тільки їй, які є відсутніми у підсистем.

1. Рудикова Л.В. Основы современных информационных технологий. – Пособие: в 2-х ч. – Ч.2. – Гродно: ГрГУ, 2008. – 272 с. 2. Макарова Н.В., Волков В.Б. Информатика: Учебник для вузов – СПб.: Питер, 2011. – 576 с. 3. Моисеенко Е.В., Лаврушина Е.Г. Информационные технологии в экономике. – Владивосток: ВГУЭС, 2005. – 231 с. 4. Сергієнко І.В. Інформатика в Україні: становлення, розвиток, проблеми. – К.: Наук. думка, 1999. – 354 с. 5. Микитин Г.В. Системний підхід до захисту інформаційних технологій // Збірник наукових праць інституту проблем моделювання в енергетиці ім. Г.С. Пухова НАН України. – 2010. – Вип. № 57. – С.192-200. 6. Микитин Г.В. Системна, нормативна та комплексна моделі захисту інформаційних технологій // Вісник Національного університету “Львівська політехніка”: Автоматика, вимірювання та керування. – № 695. – 2011. – С.126-132. 7. Дудикевич В.Б., Микитин Г.В., Гарасим Ю.Р. Ієрархічна модель захисту даних в інформаційних технологіях // Збірник тез доповідей ІІ Міжнародної науково-практичної конференції «Проблеми і перспективи розвитку ІТ - індустрії». – Харків, 2010. – Вип. 7(88). – С. 212-213. 8. Дудикевич В., Сікора Л., Микитин Г., Рудник О. Методологічні засади захисту інформаційних технологій // Матеріали І-ої Міжнародної науково-технічної конференції “Захист інформації і безпека інформаційних систем”. – 31 травня – 01 червня 2012 р. Львів. – С. 8-9.