УДК 004.056

Г.В. Микитин, к.т.н., доц., с.н.с., НУ “Львівська політехніка”, Фізико-механічний інститут ім. Г.В. Карпенка НАН України

СИСТЕМНИЙ ПІДХІД ДО ЗАХИСТУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Анотація. Розроблено системний підхід до захисту інформаційних технологій на основі: структури взаємозв’язку, взаємовідношення, взаємодії інформаційної технології та інформаційної системи, інформаційних ресурсів та інформаційних процесів, каналів зв’язку, управління.

Annotation. System approach to the information technology security based on: interaction structures, correlations, interaction between information technology and information system, information resources and information processes; communication channels; management.

Ключові слова: структура взаємозв’язку, інформаційні технології і системи, інформаційні ресурси і процеси, канали зв’язку, управління, системний підхід.

Концепція технічного захисту інформації [1], закон про захист інформації в інформаційно-комунікаційних системах [2], технічні комітети стандартизації України у предметних – інформаційні технології (ТК 20), технічний захист інформації (ТК-107) [3], правила проведення захисту інформаційних систем (ІС) [4], комплекс діючих державних, міждержавних, міжнародних стандартів у сфері захисту інформаційних технологій (ІТ) та інші документи державного і наукового рівнів регламентують критерії, настанови і правила щодо створення системи безпеки функціонування інформації в інформаційних системах відповідних рівнів. Згідно [5] технічний захист інформації передбачає етапи: визначення та аналіз загроз; розроблення системи захисту інформації; реалізацію плану захисту інформації; контроль функціонування та управління системою захисту інформації. Система стандартів [6,7,8] встановлює підхід щодо критеріїв оцінювання безпеки інформаційних технологій. Загалом проблемі безпеки ІТ присвячено багато фундаментальних і прикладних наукових праць, монографій, в яких викладено підходи, методології, моделі щодо захисту даних (ЗД) в інформаційно-комунікаційних технологіях [9,10,11,12,13,14,15]. При створенні комплексної системи захисту ІТ в рамках нормативного документу [16] потрібно керуватись підходом до захисту і протидії потенційним загрозам на рівні їх ефективного виявлення, блокування та нейтралізації. У цьому напрямку розглянемо проблему захисту даних на основі структури взаємозв’язку, взаємовідношення, взаємодії інформаційної технології та інформаційної системи, інформаційних ресурсів (ІР) та інформаційних процесів (ІП), каналів зв’язку, каналів побічного

електромагнітного випромінювання і наведення (КЗ, КПЕМВН) та елементів управління (У). Метою роботи є – створення системного підходу до захисту даних в ІТ на основі структури елементів ІР-ІС-ІП-КЗ/КПЕМВН-У та принципів системного аналізу (СА) [17].

1. Структура взаємозв'язку, взаємовідношення, взаємодії інформаційної технології і системи, інформаційних ресурсів і процесів та захисту даних

Інформаційні технології сьогодні є провідними засобами розв'язання прикладних науково-технічних задач у відповідних предметних сферах. Інформаційна технологія – це задана і керована процедура (конструктивний алгоритм) представлення інформаційних процесів з використанням відповідних інформаційних ресурсів та інформаційних систем. Взаємозв'язок, взаємодія ІТ, ІС, ІР, ІП представляє єдину базову структуру, яка має функціональне взаємовідношення до ЗД (рис.1).

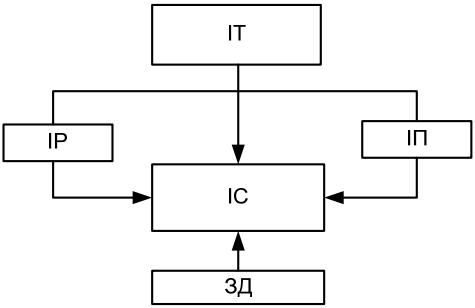

Рис. 1. Структура взаємозв'язку, взаємовідношення, взаємодії ІТ та ІС; ІР та ІП; ЗД

Захист даних в інформаційних технологіях необхідно формувати на основі пропонованого системного підходу. Тоді інформація, яка циркулює в такій структурі буде вважатися обмеженою в доступі адекватно моделі об'єкт – загроза – захист – управління. Інформаційні ресурси – це вся інформація, що визначає, інтелектуальний рівень інфраструктур суспільства. Ресурси ІС – засоби вводу-виводу, зберігання, оброблення, передавання інформації в ІС. Інформаційні процеси – процеси отримання (збору/ відбору), зберігання, перетворення, представлення і передавання інформації, взяті в сукупності або зокрема. Існує чотири класи інформаційних технологій: опрацювання даних, які використовуються для розв'язування добре структурованих задач; керування, які використовуються при неповній структурованості задач; підтримки прийняття рішення; експертні. У відповідності до ІТ з усіх класів інформаційних систем часто використовуються: інформаційно-аналітичні, вимірювальні інформаційні системи, системи підтримки прийняття рішень. Вони є автоматизованими, оскільки центральним ядром є електронно-обчислювальна машина. Далі зміст і характер інформаційних процесів визначається відповідною інформаційною системою, в якій вони протікають.

Функціонально інформаційно-аналітична система здійснює систематичну цілеспрямовану реалізацію послідовності процедур: збору/ відбору даних; аналізу (оброблення); зберігання та пошуку; передавання інформації (рис. 2). Інформація, отримана на основі моделювання об’єктів (в рамках класифікації моделей) – є результатом процедури збору даних про об’єкт дослідження (ОД) предметної сфери.

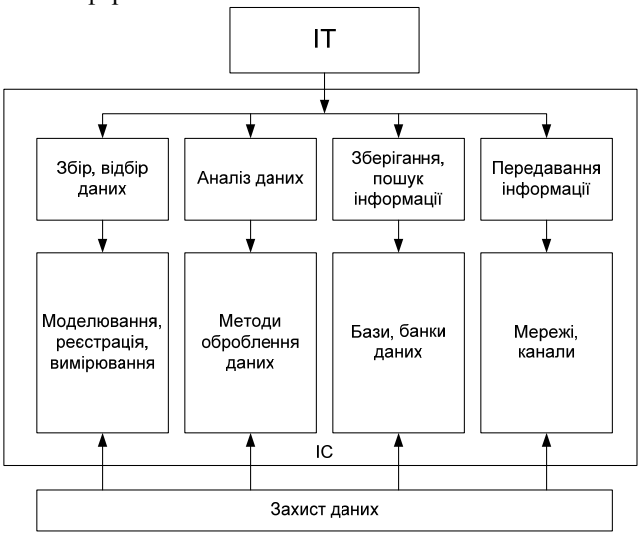

Рис. 2. Безпека ІТ на рівні алгоритмічних процедур

Суть моделювання полягає у відтворенні певної реально існуючої або уявної системи (об'єкта) за спеціально побудованою, згідно відповідних правил, схемою аналога. Інформація, отримана методами і засобами реєстрації, вимірювання параметрів ОД та відображає їх адекватні моделі у відповідних предметних сферах – є результатом процедури відбору засобами інформаційних вимірювальних технологій і систем. Процедура передавання інформації зачіпає питання оптимальних критеріїв захисту мереж та каналів зв’язку. Безпека функціонування ІТ в цілому передбачає захист даних на рівні інформаційних процесів та створення відповідної системи управління захистом.

2. Системна підхід до захисту інформаційних технологій

На основі принципів СА: цілісності, ієрархічності, багатоаспектності пропонується системний підхід до захисту ІТ. В основі такого підходу є структура взаємозв’язку, взаємовідношення, взаємодії ІТ та ІС, ІР та ІП, каналів зв’язку та елементів управління (рис. 3). 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.

Системний підхід до захисту ІТ представлений у вигляді тривимірного простору *x-y-z*, охопленого сферою (рис.3).

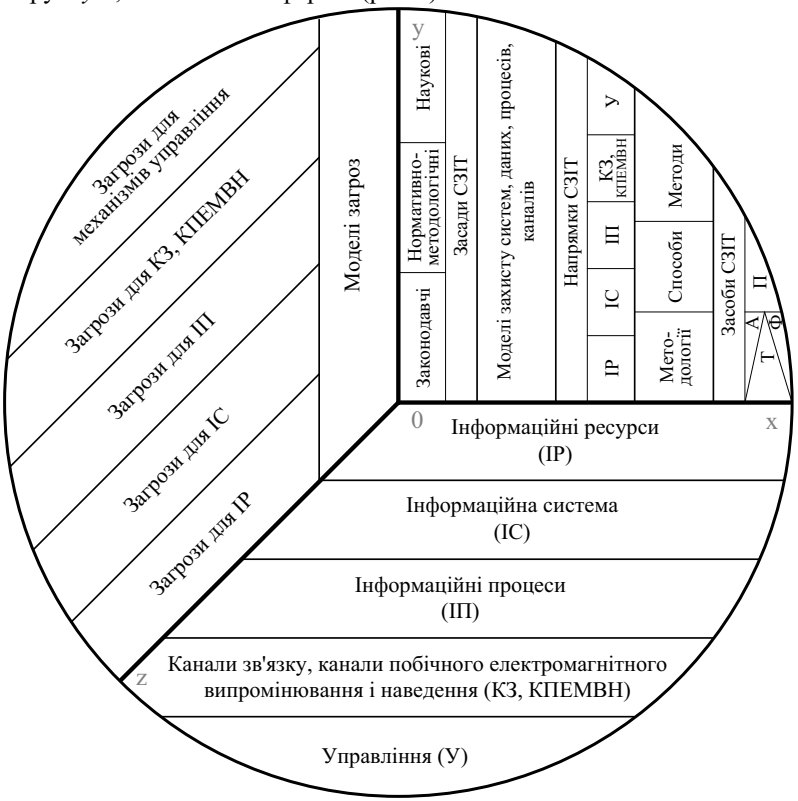

Рис.3. Системний підхід до захисту інформаційних технологій

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 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 дозволяє 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. 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 і т. і.;

– 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 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 т. і. забезпечують розмежування доступу та виключають несанкціоноване використання інформації.

Згідно [5] 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 т. і.) 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'язу і взаємодії ІТ та ІС, ІР та ІП, КЗ, У здійснюється на рівні: нормативно-методологічного,

апаратного-фізичного (технічного), програмного, комунікаційного забезпечення.

Основою захисту ІТ рівень нормативно-методологічного забезпечення – закони, концепції, настанови, правила, порядок проведення робіт, технічні комітети, стандарти. Розглянемо нормативну базу у сфері захисту ІТ – деякі державні стандарти України, які гармонізовані з міжнародними та міждержавними за схемою об'єкт – захист:

ДСТУ ISO/IEC 9594-8 – Інформаційні технології. Взаємозв'язок відкритих систем. Каталог: Основні положення щодо сертифікації відкритих ключів та сертифікації атрибутів

ДСТУ ISO/IEC 9797-1 – Інформаційні технології. Методи захисту. Коди автентифікації повідомлень (MACs). Частина 1. Механізми, що використовують блокові шифри

ДСТУ ISO/IEC 9797-2 – Інформаційні технології. Методи захисту. Коди автентифікації повідомлень (MACs). Частина 2. Механізми, що використовують спеціалізовані геш-функції

ДСТУ ISO/IEC 9798-1 – Інформаційні технології. Методи захисту. Автентифікація об'єктів. Частина 1. Загальні положення

ДСТУ ISO/IEC 9798-2 – Інформаційні технології. Методи захисту. Автентифікація об'єктів. Частина 2. Механізми, що ґрунтуються на використанні алгоритмів симетричного шифрування

ДСТУ ISO/IEC 9798-3 – Інформаційні технології. Методи захисту. Автентифікація об'єктів. Частина 3. Механізми, що ґрунтуються на використанні алгоритмів цифрового підпису

ДСТУ ISO/IEC 9798-4 – Інформаційні технології. Методи захисту. Автентифікація об'єктів. Частина 4. Механізми, що ґрунтуються на використанні функцій обчислення криптографічного контрольного значення

ДСТУ ISO/IEC 9798-5 – Інформаційні технології. Методи захисту. Автентифікація об'єктів. Частина 5. Механізми, що використовують методи засновані на нульових знаннях

ДСТУ ISO/IEC 9798-6 – Інформаційні технології. Методи захисту. Автентифікація об'єктів. Частина 6. Механізми, що використовують неавтоматизовану передачу даних.

ДСТУ ISO/IEC 11770-1 – Інформаційні технології. Методи захисту. Управління ключовими даними. Частина 1: Загальні положення

ДСТУ ISO/IEC 11770-2 – Інформаційні технології. Методи захисту. Управління ключовими даними. Частина 2. Протоколи, що ґрунтуються на симетричних криптографічних перетвореннях.

ДСТУ ISO/IEC 11770-3 – Інформаційні технології. Методи захисту. Управління ключовими даними. Частина 3. Протоколи, що ґрунтуються на асиметричних криптографічних перетвореннях

ДСТУ ISO/IEC 13888-1 – Інформаційні технології. Методи захисту. Неспростовність. Частина 1. Загальні положення

ДСТУ ISO/IEC 13888-2 – Інформаційні технології. Методи захисту. Неспростовність. Частина 2. Методи, що ґрунтуються на використанні симетричних алгоритмів

ДСТУ ISO/IEC 13888-3 – Інформаційні технології. Методи захисту. Неспростовність. Частина 3. Методи, що ґрунтуються на використанні асиметричних алгоритмів

ДСТУ ISO/IEC 14888-1 – Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 1. Загальні положення

ДСТУ ISO/IEC 14888-2 – Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 2. Механізми на основі ідентифікаторів

ДСТУ ISO/IEC 14888-3 – Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 3. Механізми на основі сертифікатів

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

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

ДСТУ ISO/IEC 15946-1 Інформаційні технології. Методи захисту. Криптографічні перетворення, що ґрунтуються на еліптичних кривих. Частина 1. Основні положення

ДСТУ ISO/IEC 15946-2 Інформаційні технології. Методи захисту. Криптографічні перетворення, що ґрунтуються на еліптичних кривих. Частина 2. Електроні цифрові підписи

ДСТУ ISO/IEC 15946-3 Інформаційні технології. Методи захисту. Криптографічні перетворення, що ґрунтуються на еліптичних кривих: Частина 3. Встановлення ключів

ДСТУ ГОСТ 30833 (ИСО/МЭК 15418-99) – Автоматична ідентифікація. Ідентифікатори застосування EAN/UCC та ідентифікатори даних FACT. Загальні положення та порядок ведення

ДСТУ ISO 9160 – Інформаційні технології. Шифрування даних. Вимоги до взаємодії на фізичному рівні

ДСТУ ISO/IEC 10118-1 – Інформаційні технології. Методи захисту. Геш-функції. Частина 1. Загальні положення

ДСТУ ISO/IEC 10118-2 – Інформаційні технології. Методи захисту. Геш-функції. Частина 2. Геш-функції з використанням n-бітового блокового шифру

ДСТУ ISO 7498-2 – Системи оброблення інформації. Взаємозв'язок відкритих систем. Базова еталонна модель. Частина 2. Архітектура захисту

інформації

ДСТУ ГОСТ 31078 – Захист інформації. Випробування програмних засобів на наявність комп'ютерних вірусів. Типова настанова

ДСТУ ГОСТ 31078 – Захист інформації. Випробування програмних засобів на наявність комп'ютерних вірусів. Типова настанова.

Для захисту інформації на рівні апаратного-фізичного забезпечення використовуються: апаратні ключі; системи охоронної і пожежної сигналізації; засоби блокування пристроїв і інтерфейсів вводу-виводу інформації, системи цифрового відеоспостереження; системи контролю й керування доступом, спеціалізовані замки т. і.

Захист даних в ІТ на рівні програмного забезпечення (прикладного, системного) становлять: системи розмежування доступу до інформації; системи ідентифікації та автентифікації; системи аудиту та моніторингу; системи антивірусного захисту т. і.

Рівень комунікаційного забезпечення захисту ІТ тримають:

– засоби мережевого захисту: міжмережеві екрани (для блокування атак із зовнішнього середовища), системи виявлення вторгнень (для виявлення спроб НСД як ззовні, так і усередині мережі), засоби створення віртуальних приватних мереж (для організації захищених каналів передавання даних через незахищене середовище), засоби аналізу захищеності (для виявлення можливих каналів реалізації загроз інформації в корпоративних мережах);

– заходи/ засоби захисту інформації від її витоку технічними і спеціальними каналами: використання екранованого кабелю та екранованого устаткування; встановлення на лініях зв'язку високочастотних фільтрів; побудова екранованих приміщень, так званих “капсул”; встановлення активних систем зашумлення.

Висновок.

Запропонований системний підхід на основі структури взаємозв’язку інформаційної технології і системи, інформаційних ресурсів і процесів, каналів зв’язку та елементів управління безпекою інформації дозволяє:

– створювати моделі захисту для об’єктів – ІР, ІС, ІП, КЗ/ КПЕМВН, У адекватно до моделей загроз і, на цій основі, формувати уніфіковану модель захисту ІТ для забезпечення цілісності, конфіденційності, доступності інформації на усіх етапах її життєвого циклу;

– формувати комплексну систему безпеки ІТ на рівні – нормативно-методологічного, апаратно-фізичного, програмного, комунікаційного забезпечення захисту даних в ІТ з метою функціонального виявлення, блокування, нейтралізації потенційних загроз згідно концепції об’єкт – загроза – захист – управління.

1. Концепція технічного захисту інформації в Україні. Затверджено постановою Кабінету Міністрів України від 8 жовтня 1997 р. N 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. Технічні комітети стандартизації України. Каталог / Укладач Т.Б. Гордієнко.– Київ: ДП “УкрНДНЦ”, 2010. – 213 с.
4. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних, інформаційно-телекомунікаційних системах / Затверджено постановою КМУ від 29.03.2006 №373/ http: // www.kmu.gov.ua
5. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення. – К. : ДСТСЗІ СБ України, 1997
6. ГОСТ Р ИСО/МЭК 15408-1-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. – М.: ИПК Издательство стандартов, 2002.
7. ГОСТ Р ИСО/МЭК 15408-2-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. – М.: ИПК Издательство стандартов, 2002.
8. ГОСТ Р ИСО/МЭК 15408-3-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. – М.: ИПК Издательство стандартов, 2002.
9. *Головань С.М., Дудикевич В.Б., Зачепило В.С., Пархуць Л.Т., ЩербакЛ.М.* Документаційне забезпечення робіт із захисту інформації з обмеженим доступом. – Л.: Видавництво НУ львівська політехніка, 2005. -288 с.
10. *Хорошко В.А., Чекатков А.А.* Методы и средства защиты информации. – К.: Юниор, 2003. – 504 с.
11. *Домарев В.В.* Безопасность информационных технологий. Системный подход. – К.: ООО ТИД ДИА Софт, 2004. – 992 с.
12. *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.: Видавництво НУ “Львівська політехніка”, 2006. – 348 с.
13. *Юдін О.К., Корченко О.Г., Конахович Г.Ф.* Захист інформації в мережах передачі даних: Підручник. – К.: Вид-во ТОВ «НВП» ІНТЕРСЕРВІС», 2009. – 716 с.
14. *Микитин Г.В.* Концептуальні моделі захисту інформації для технологій стаціонарного, стільникового, супутникового зв’язку/ *Дудикевич В.Б., Гарасим Ю.Р., Микитин Г.В.* // Вісник Національного університету “Львівська політехніка” “Автоматика, вимірювання та керування”, 2010. – №665. – С. 18-26.
15. *Микитин Г.В.* Автоматизована система обробки інформації “Захист аудіоінформації”: реєстратори, канали витоку, засоби захисту/ *Дудикевич В. Б., Микитин Г.В., Гарасим Ю.Р.* // Вісник Національного університету “Львівська політехніка” “Комп’ютерні системи проектування. Теорія і практика”, 2010. – №685. – С. 156-167.
16. *НД ТЗІ 3.7-003-05.* Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі / Затверджено: наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 08.11.2005 №125 / http: // www.dstszi.gov.ua
17. *Згуровський М.З., Панкратова Н.Д.* Основи системного аналізу. – К.: Видавнича група BHV, 2007. – 498 с.

Поступила 13.09.2010р.