використанні тесту кореляції – навпаки.

Висновки. В роботі був наведений статистичний аналіз генераторів псевдовипадкової послідовності, яка розподілена за рівномірним законом на основі використання програмних середовищ Matlab та Mathcad. Дана перевірка була представлена на основі порівняльного аналізу генераторів у двох програмних середовищах на основі оцінки похибок за математичним сподіванням, дисперсією та середньоквадратичним відхиленням, а також на основі критеріїв Колмогорова-Смірнова, Пірсона, Мізеса та тесту кореляції. Для оцінки генераторів за даними критеріями були використані об'єми вибірок n=100; n=1000; n=10000. Для кожного об'єму наведені числові результати похибок та проведений їх аналіз.

1. *Кнут Д.Э.* Искусство программирования. Том 2. Получисленные алгоритмы. – М.Мир, 2000. – 768 с.

2. *Харин Ю.С., Степанова М.Д.* Практикум на ЭВМ по математической статистике. Для мат. спец. ун-тов. – Мн.: изд-во «Университетское», 1987. – 304с.: ил.

3. *Черкесов Г.Н.* Надежность апаратно-программных комплексов. Учебное пособие. – СПб.: Питер, 2005. – 479 с.: ил.

4. *Гришин В.К.* Математическая обработка и интерпретация физического эксперимента / В.К. Гришин, Ф.А. Живописцев, В.А. Иванов. – М.: Изд-во Моск. ун-та, 1988. – 318 с.

Поступила 4.03.2013р.

УДК 681.3

С.М. Головань, А.М. Давиденко, Л.М. Щербак, м. Київ

ПРО ТЕРМІНОЛОГІЮ В ОБЛАСТІ БЕЗПЕКИ ІНФОРМАЦІЇ

In this paper, based on the results of comparative analysis of terminological framework in the area of information security today proposed a number of definitions.

Keywords: information security, information sources, threats, information security, security policy.

Вступ. Дана робота є дискусійною і присвячена питанням термінологічної бази в області безпеки інформації. Відмітимо, що по суті епіграфом до даної роботи може бути афоризм відомого французького філософа і математика Рене Декарта (1590-1650): «Визначте зміст слів і ви звільните людство від половини його непорозумінь».

Термінологічна база змінюється і вдосконалюється по мірі розвитку земної цивілізації. Це в повній мірі відноситься і до області безпеки інформації. Цій темі присвячена значна кількість публікацій, в тому числі [1, …,7].

В той же час на сьогодні в Україні не визначено загальноприйняте поняття безпеки інформації, не розроблені відповідний теоретико-методологічний та методичний інструментарій пізнання сутності, структури і динаміки, її формалізований категорійно-понятійний апарат. При висвітленні проблем у сфері безпеки інформації використовують такі терміни, як: «інформаційна безпека», «захист інформації», «охорона інформації» і, в ряді випадків, їх використовують як терміни-синоніми.

Українські стандарти з інформаційної безпеки у певній мірі гармонізовані до закордонних стандартів типу ISO, в яких поняття «information security» перекладається як «безпека інформації». В українських і іноземних вищих навчальних закладах ведеться підготовка фахівців з інформаційної безпеки, а не захисту інформації.

Відмітимо, що, відповідно до Закону України «Про інформацію» [2] інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом. Будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом. Інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація. В першу чергу захисту підлягає інформація з обмеженим доступом, а відкрита інформація підлягає безпеці, тобто запобігання пошкодження чи знищення інформації внаслідок свідомих дій зловмисника, помилок персоналу, стихійного лиха.

Основні результати. Перейдемо до основного змісту даної роботи. Базуючись на результатах порівняльного аналізу [1,..,7] термінологічної бази в області безпеки інформації запропонуємо ряд сучасних означень.

З метою послідовності наведення термінологічних означень використаємо умовну структурну схему взаємозв'язків об'єктів і суб'єктів при вирішенні проблем безпеки інформації, яка зображена на рис.1.

1.Джерелами інформації є фізичні і юридичні особи, документи, публікації, матеріальні носії інформації, засоби виробничої та трудової діяльності, інформаційні ресурси технічних апаратно-програмних комплексів та інше.

2. *Безпека інформації* визначається як стан захищеності у часі і просторі інформаційного середовищі та інформаційних ресурсів суспільства в інтересах фізичних, юридичних осіб та держави.

3. Концепція і структура безпеки інформації

Основу концепції і структури безпеки інформації складають:

– сформована система поглядів на проблему безпеки інформації;

– фізичні і юридичні особи;

– спеціалісти вирішення проблеми безпеки інформації;

– теорія та практика безпеки інформації в суспільстві та інформаційно-телекомунікаційних системах;

– системи технічних та технологічних засобів безпеки інформації.

4. Концептуальна модель безпеки інформації

Дана концепція містить наступні компоненти:

– джерела інформації;

– напрями, способи, методи, заходи та засоби захисту інформації;

– об’єкти і суб’єкти загроз, цілі загроз, джерела загроз, загрози та атаки на джерела інформації.

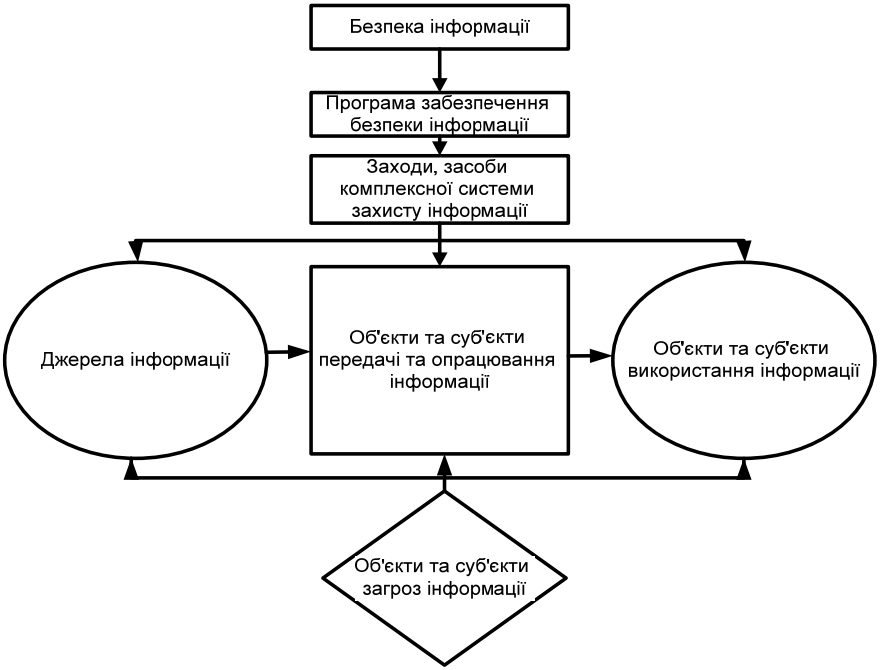

Рис. 1. Умовна структурна схема взаємозв’язків об’єктів і суб’єктів при вирішенні проблем безпеки інформації

Загроза потенційно є причиною небажаного інциденту, що здатний заподіяти шкоду системі чи організації та її активів. Ця шкода є результатом прямої чи непрямої атаки, спрямованої на інформацію, якою оперує система чи служба інформаційних технологій, і являє собою, наприклад, її несанкціоноване знищення, розкриття, зміну, перекручування, втрату доступності чи втрату. Загроза може здійснитися, заподіяти шкоду у випадку наявності в активах уразливих місць. Загрози, причиною яких є людина, розділяють на випадкові й навмисні. І випадкові, і навмисні загрози повинні бути ідентифіковані й визначені їхні рівні й імовірність. Приклади загроз наведені у табл. 1.

5. *Комплексна система захисту інформації*

Кожен вид захисту інформації забезпечує окремі аспекти безпеки інформації:

– правовий – сукупність законів та нормативних актів, правил, процедури і заходи захисту інформації на правовій основі;

Таблиця 1

Приклади загроз

Людські		Довкілля
Навмисні	**Випадкові**	
Підслуховування Зміна інформації Злом системи Навмисний програмний код Злодійство	Помилки і недогляд Вилучення файлу Невірна маршрутизація Фізичні ушкодження	Землетрус Блискавка Потоп Пожежі

– організаційний – попередження доступу на об'єкт інформаційної діяльності сторонніх осіб за допомогою організаційних заходів (правила розмежування доступу).

– технічний – забезпечує обмеження доступу до носія повідомлення апаратно-технічними засобами (антивіруси, фаєрволи, маршрутизатори, токіни, смарт-карти тощо):

• попередження витоку по технічним каналам;

• попередження блокування ;

– інженерний — попереджує руйнування носія внаслідок навмисних дій або природного впливу інженерно-технічними засобами (сюди відносять обмежуючі конструкції, охоронно-пожежна сигналізація);

– криптографічний – попереджує доступ до за допомогою математичних перетворень повідомлення:

• попередження несанкціонованої модифікації ;

• попередження несанкціонованого розголошення.

6. *Політика безпеки* формується на основі аналізу поточного стану і перспективи розвитку інформаційної системи, можливих загроз і визначає:

– мету, задачі і пріоритети системи безпеки;

– галузь дії окремих підсистем;

– гарантований мінімальний рівень захисту;

– обов'язки персоналу по забезпеченню захисту;

– санкції за порушення захисту.

Якщо виконання політики безпеки проводиться не в повній мірі або непослідовно, тоді імовірність порушення захисту інформації різко зростає.

Висновки. У даній роботі на основі результатів порівняльного аналізу термінологічної бази в області безпеки інформації [1-7] запропоновано ряд сучасних означень.

1. Настанови з керування безпекою інформаційних технологій. Частина 1. Концепції та моделі безпеки інформаційних технологій : ДСТУ ISO/IEC TR 13335-1:2003. – [Чинний від 2004 – 10 – 01]. – К. : Держспоживстандарт України, 2005. – IV. 17 с. – (Національний стандарт України).

2. Про інформацію [Електронний ресурс] Закон України від 02.10.2002 р. № 2657-

XII. (у редакції № 2938-VI від 13.01.2011) – Режим доступу: http. // www. zakon1. rada.gov.ua. – Заголовок з екрану.
3. Рекомендації по стандартизації "Інформаційні технології. Основні терміни і визначення в галузі технічного захисту інформації" (Р 50.1.053-2005) - all-ib.ru .
4. *Коженевський С.Р.* Термінологічний довідник з питань технічного захисту інформації / Кожевенський С.Р., Кузнецов Г.В., Хорошко В.О., Чирков Д.В. / За ред. проф. В.О. Хорошка. – К.: ДУІКТ, 2007. – 365 с.
5. *Николайчук Я.М.* Теорія джерел інформації. / Видання друге, виправлене. – Тернопіль: ТзОВ «Терно-граф», 2010. – 536 с.
6. *Задірака В.К., Олексюк О.С.* Компютерна криптологія: Підручник. – К., 2002. – 504 с.
7. *Кормич Б.А.* Інформаційна безпека: організаційно-правові основи. – К.: Кондор, 2004. – 384 с.

Поступила 11.03.2013р.

УДК 681

А.А. Владимирский, И.А. Владимирский, г.Киев

ЗОНД ДЛЯ ВНУТРИКАНАЛЬНОГО ОБСЛЕДОВАНИЯ ТЕПЛОВЫХ СЕТЕЙ

The new combined video-, termo- and audioprobe for intracanal check underground urban heat networks are developed.

Введение. Старение и износ основной части трубопроводов тепловых сетей в Украине и других странах СНГ приводит к устойчивому ежегодному росту повреждаемости теплотрасс с возникновением утечек. В крупных городах борьба с утечками является ежедневной практикой, которую можно считать неотъемлемой частью технологии транспортировки тепла потребителям. Это вынуждает искать новые подходы, новые эффективные методы точного и оперативного определения мест повреждений подземных трубопроводов.

В качестве вспомогательного средства поиска утечек в ИПМЭ им. Г.Е.Пухова НАНУ разработан, изготовлен и испытан диагностический зонд для внутриканального обследования теплотрасс [1]. Зонд (рис.1.а) состоит из комбинированного измерительного устройства, телескопической штанги и индикаторного блока. В герметичном измерительном устройстве установлены видеокамера повышенного разрешения, светодиодные прожектора подсветки, микрофон и измеритель теплового излучения. Видеоизображение, уровень акустического шума и температура отображаются в реальном времени на экране индикаторного блока.

