Секція 5

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ І УПРАВЛІННЯ ПРОЕКТАМИ ТА ПРОГРАМАМИ В БЕЗПЕЦІ ЖИТТЄДІЯЛЬНОСТІ

УДК 004.632

ОРГАНІЗАЦІЙНИЙ ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ, ЩО ОБРОБЛЯЮТЬСЯ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Білан В.П.
Мандрона М.М., канд. техн. наук
Львівський державний університет безпеки життєдіяльності

«Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини" стаття 32 Конституції України [1].

Потребу та необхідність захисту особистих даних про особу чітко визначено на законодавчому рівні України. Питання щодо захисту персональних даних регулює Уповноважений Верховної Ради України з прав людини.

Персональні дані – це дані про особу, що дають змогу її ідентифікувати; це вид інформації, що належить до конфіденційної, яка є інформацією з обмеженим доступом. Вимоги до захисту персональних даних регламентується законодавством України.

Основною вимогою під час обробки конфіденційної інформації є забезпечення її захисту від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання, поширення [2-4]. Отже, для виконання цієї вимоги повинні створюватись комплексні системи захисту інформації, які містять комплекси засобів захисту від несанкціонованого доступу, тобто спеціальне ліцензійне, сертифіковане програмне забезпечення.

Експлуатація інформаційно-телекомунікаційної системи (ІТС) можлива лише за умови наявності затвердженого встановленим порядком Плану захисту інформації в ІТС. Дії користувачів ІТС повинні визначатися відповідними інструкціями. Повинні бути розроблені порядки дій користувачів у разі відмови системи захисту в цілому чи окремого її компоненту, також мають бути розроблені нормативні та розпорядчі документи, що визначають правила режиму доступу у приміщення, в якому розміщена ІТС, та порядок доступу користувачів до неї. Користувачі ІТС, котрі працюють з персональними даними повинні мати дозвіл керівника для виконання цієї роботи.

Проаналізувавши літературні джерела ми можемо виділити такі основі організаційні заходи із захисту інформації, тобто ті дії, які спрямовані на реалізацію захисту інформації шляхом регламентації діяльності персоналу і порядку функціонування засобів і систем забезпечення інформаційної діяльності.

Організаційні заходи щодо керування доступом повинні передбачати:

- визначення порядку доступу користувачів у захищене приміщення, до технічних засобів, носіїв інформації, програмного та інформаційного забезпечення;
- визначення порядку внесення/вилучення даних щодо атрибутів доступу користувача.

Організаційні заходи щодо забезпечення цілісності інформації повинні передбачати:

- резервне копіювання на матеріальних носії інформації еталонних копій операційних систем і функціональних програм;
- контроль цілісності системного програмного забезпечення;
- контроль цілісності комплексу засобів захисту.

Організаційні заходи антивірусного захисту інформації повинні передбачати:

- використання сертифікованого ліцензійного антивірусного програмного забезпечення;
- організацію постійного та своєчасного оновлення антивірусних баз.
- для забезпечення відновлюваності інформації у випадку збоїв системи або помилок користувачів в ІТС повинно здійснюватися періодичне резервне копіювання.

Під час обробки персональних даних в ІТС персонал має право створювати, модифікувати, вилучати, друкувати та копіювати на матеріальні носії файли з текстовими документи, за які вони відповідають, а також працювати із файлами, що створюються спільно з іншими користувачами, відповідно до наданих прав. Проте персонал не повинен виконувати роботи з налаштування конфігурації засобів захисту, загальносистемного та програмного забезпечення, оновленням антивірусних баз, систем управління базами даних, змінювати їх склад та структуру, коригувати права доступу. Усі ці роботи повинні виконуватись службою захисту інформації адміністратором безпеки і системним адміністратором.

Література

1. Конституція України [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/254к /96-вр.

2. Закон України «Про захист персональних даних: від 01.06.2010 р. № 2297-VI // Відомості Верховної Ради України (ВВР). – 2010. – № 34. – С. 481.

3. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах": від 27.03.2014 N 1170-VII.

4. Білан В.П. Вимоги законодавства щодо захисту персональних даних / В.П. Білан, М.М. Мандрона // Захист інформації в сучасному суспільстві: матер. 1 Міжнародної наук.-техні. конференції, 21-22 листопада 2014 р. – Львів: Вид-во ЛДУ БЖД, 2014. – С. 15-16.

УДК 614.843 (075.32)

МАТЕМАТИЧНА МОДЕЛЬ УПРАВЛІННЯ РИЗИКАМИ ДЛЯ ЗАБЕЗПЕЧЕННЯ ПРОТИПОЖЕЖНОГО ЗАХИСТУ МІСТА

Васильєв М.І.
Мовчан І.О., канд. техн. наук, доцент
Львівський державний університет безпеки життєдіяльності

У сфері пожежної безпеки користуються терміном «пожежний ризик», тобто це є міра можливості реалізації пожежної небезпеки об'єктів захисту міста та її наслідків для людей і матеріальних цінностей. Гарантування пожежної безпеки об'єктів захисту складається з визначення, аналізу та оцінювання пожежного ризику, що дозволяє розробляти і впроваджувати відповідні заходи для зменшення їх значень до прийнятного значення. У різних аспектах і контекстах ці завдання розглядалися в роботах таких вчених як: В. Бурков, С.Д. Бушуєв, Ю.П. Рак, В.А. Рач, М.М. Брушлінський, В.В. Холщевніков, Д.О. Самошин, В.В. Бігун та інших.

Згідно з рекомендаціями Всесвітньої організації охорони здоров'я і Постанови Кабінету міністрів України [1, 2], пожежні ризики класифікують так: 1) незначний ризик $\varepsilon \leq 10^{-6}$; 2) середній ризик $\varepsilon = 10^{-6}...5\cdot10^{-5}$; 3) високий (терпимий) ризик $\varepsilon = 5\cdot10^{-5}...5\cdot10^{-4}$; 4) неприйнятний ризик $\varepsilon > 5\cdot10^{-4}$. Наведені дані стосуються лише пожежних ризиків відносно можливості оперативної ліквідації пожежі на об'єктах, які розглядаються відповідно до аудиту пожежної безпеки.

Відомо, що пожежний ризик для міста залежить від багатьох чинників, а саме від: 1) пожежного ризику для об'єктів житлового сектора міста, в тому числі з урахуванням впливу людського фактора та ризику евакуації людей при виникненні пожежі; 2) пожежного ризику для соціально-культурних, громадських та адміністративних об'єктів міста; 3) пожежного ризику для споруд виробничого призначення; 4) організаційного ризику ліквідації пожежі пожежно-рятувальними частинами міста.

Основною задачею в процесі використання теорії прийняття рішення є вибір оцінки для прийняття відповідного рішення, тобто вибір певного критерію для прийняття цього рішення [3]. Таким критерієм можуть бути збитки *З* від пожежі та витрати *В* на протипожежний захист. Для розроблення оптимізаційної моделі визначення методів і засобів протипожежного захисту з урахуванням допустимого значення пожежного ризику необхідно знати на кінець звітного періоду дійсне значення пожежного ризику $\varepsilon_м$ для міста, а саме загальну кількість пожеж $N_п$ і споруд всіх об'єктів міста $N_о$ за ЄДРПОУ. Тоді [4]

$$\varepsilon_м = \frac{N_п}{N_о} \leq [\varepsilon], \qquad (1)$$

де $[\varepsilon]$ – допустиме значення пожежного ризику для міста.

У випадку, коли ε_M перевищує значення допустимого ризику [ε] для міста, необхідно розробляти та впроваджувати заходи для його зменшення до допустимих значень за рахунок витрат на придбання протипожежних технічних засобів для обладнання ними відповідних об'єктів міста. Найбільш доцільно розробляти та впроваджувати заходи протипожежного захисту на підставі результатів, які можуть бути отримані з використанням оптимізаційної моделі. Оптимізаційну модель визначення методів і засобів протипожежного захисту з урахуванням допустимого значення пожежного ризику для міста можна представити так:

Функція мети

$$\varepsilon_{M.i} \Rightarrow \min ; \quad (2)$$

за критерієм

$$\left| З_i - В_i \right| \Rightarrow \min ; \quad (3)$$

за обмеженнями, які накладаються на значення пожежних ризиків для відповідних груп об'єктів.

Для розв'язування оптимізаційної моделі використовувався метод Монте-Карло.

Висновки

1. Розроблена оптимізаційна модель методів і засобів протипожежного захисту міста на основі допустимого для міста значення пожежного ризику, яка дозволяє оперативно на основі аудиту визначати напрямки, додаткові витрати і відповідні засоби забезпечення прийнятного, в крайньому випадку високого (терпимого) ризику.

2. Розроблена оптимізаційна модель дозволяє управляти пожежним ризиком міста з урахуванням заходів на протипожежний захист, які підвищують пожежну безпеку міста.

Література

1. Бєгун В.В. Безпека життєдіяльності: Навчальний посібник / В.В. Бєгун, І.М. Науменко. – К.: 2004. – 328 с.

2. Постанова Кабинету міністрів України від 29 лютого 2012 р. № 306. – К. – 3 с.

3. Мушик **Э.** Методы принятия технических решений / Э. Мушик, П. Мюллер // Перевод с нем. – М.: Мир, 1990. – 208 с.

4. Климась Р. Визначення ймовірності виникнення пожеж у будівлях і спорудах різного призначення / Р. Климась, Д. Матвійчук // Надзвичайна ситуація № 11, 2011. – с. 44-45.

УДК 004.056.53

ЗАХИСТ ВІД ПРОСЛУХОВУВАННЯ ПРИМІЩЕННЯ

Галайчук О.О.
Мандрона М.М., канд. техн. наук
Львівський державний університет безпеки життєдіяльності

Під час проведення нарад чи переговорів інформація передається за допомогою людської мови. Людська мова це звукові хвилі, які поширюються однаково на всі сторони від джерела звуку і заповнюють весь об'єм приміщення. Під час розмови виникає акустичний канал витоку інформації, який складається з джерела небезпечного сигналу, фізичного середовища поширення (наприклад – повітря, земля, вода, будівельні конструкції та інше) та технічного засобу приймання, що визначає фізичний шлях, яким зловмисник здійснюватиме несанкціоноване отримання інформації. Інформацію можна прослуховувати безпосередньо по стінах, вікнах, дверях, трубах опалення, системах пожежогасіння, металевих балках і конструкціях та інших предметах, що знаходяться у приміщенні [1].

У залежності від ситуації для прослуховування використовують дуже різні методи та засоби. В основному пристрої для прослуховування поділяють на дві групи: ті, що прослуховують на відстані та ті, які знаходять безпосередньо біля джерела звуку (рис. 1).

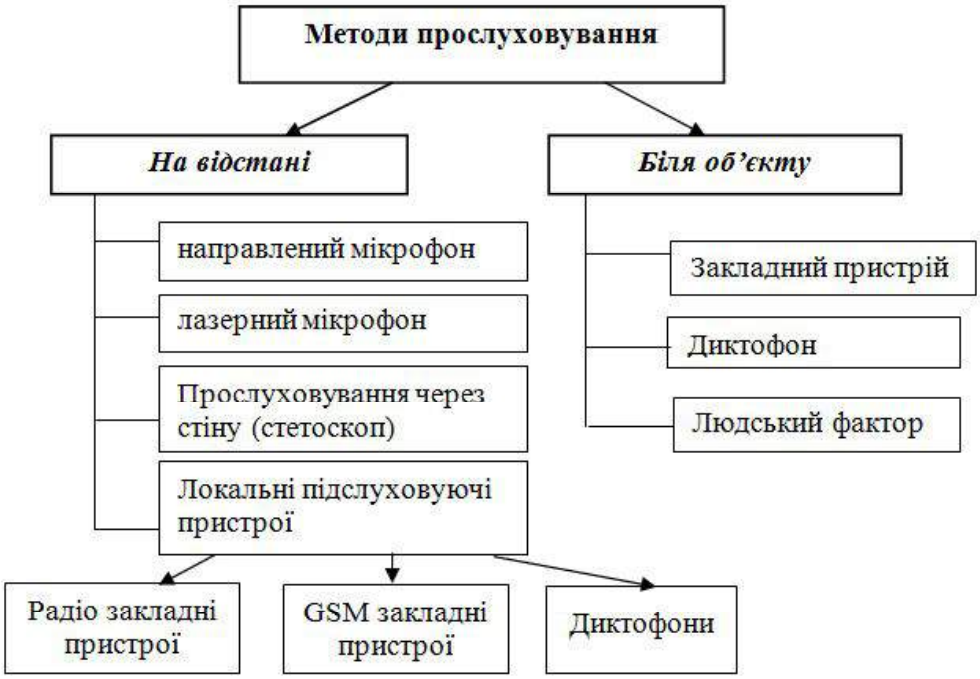

Рис. 1. *Класифікація методів прослуховування приміщення*

Захист від прослуховування – сучасний спосіб забезпечення збереження конфіденційних даних із застосуванням технічних засобів, що блокують деякі канали витоку інформації або виявляють електронні пристрої [2].

Методи захисту мовної інформації поділяють на пасивні, активні, організаційні. *Пасивні методи* – збільшення звукоізоляції огороджуючи конструкцій за рахунок: подвійних дверей з тамбуром і ущільнювачем, багатошарових стін, використання звукопоглинаючих матеріалів. *Активні методи* – це активне і віброакустичне зашумлення.

Методи захисту акустичної інформації [2-3] спрямовані на:

- створення маскувальних вібраційних і акустичних перешкод для зменшення співвідношення сигнал/шум на межі контрольованої зони до величин, що забезпечують неможливість виділення інформаційного акустичного сигналу засобом розвідки;
- створення маскувальних електромагнітних перешкод у сполучних лініях чи лініях електроживлення, що мають у своєму складі електроакустичні перетворювачі (володіють мікрофонним ефектом), з метою зменшення відносин сигнал/шум до величин, що забезпечують неможливість виділення інформаційного сигналу засобом розвідки;
- електромагнітне чи ультразвукове приглушення диктофонів у режимі запису;
- створення прицільних радіоперешкод акустичними і телефонними радіозакладками з метою зменшення відносин сигнал/шум до величин, що забезпечують неможливість виділення інформаційного сигналу засобом розвідки;
- порушення функціонування (придушення) засобів несанкціонованого підключення до телефонних ліній;
- виведення з ладу (знищення) засобів несанкціонованого підключення до телефонних лініях.

В основі активних методів захисту акустичної інформації є використання спеціальної техніки, тобто різного типу генераторів шумових сигналів, вібровипромінювачів, подавлювачів GSM сигналів, диктофонів і закладних пристроїв, нелінійні локатори, детектори поля та ін.

Література

1. Андрианов В.И. Шпионские штучки и устройства для защиты объектов и информации: справочное пособие / Андрианов В.И., Бородин В.А., Соколов А.В.– Спб.: Лань, 1996. – 272 с.

2. Технічний захист інформації (приміщень). [Електронний ресурс]. – Доступно з: http://ssbb.com.ua/uk/tehnichniy-zahist-informatsiyi-primishhen-2.

3. Захист від прослуховування. [Електронний ресурс]. – Доступно з: http://sirius.kiev.ua/index.php?option=com_content&view=article&id=206&Itemid=&lang

4. Перелік засобів технічного захисту інформації, дозволених для забезпечення технічного захисту державних інформаційних ресурсів та інформації. [Електронний ресурс]. – Доступно з: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=234237&cat

УДК 005.8+614.8

УПРАВЛІННЯ ПРОЕКТОМ СТВОРЕННЯ МОБІЛЬНОГО КОМПЛЕКСУ ДЛЯ ГАСІННЯ ПОЖЕЖ НА ТОРФОВИЩАХ

Герасимчук А.І.
Івануса А.І., канд. техн. наук
Львівський державний університет безпеки життєдіяльності

Низький рівень ефективності гасіння пожеж на торфовищах зумовлений нераціональним використанням застарілої пожежно-рятувальної техніки, великої кількості паливо-мастильних матеріалів та особового складу рятувальних підрозділів. Тому, з метою впровадження в практичну діяльність гасіння пожеж на торфовищах, пропонується розробити спеціальний мобільний комплекс (МК) для гасіння пожеж даного виду.

Реалізація проекту створення МК орієнтована на виконання наступних завдань:

- покращення екологічного стан потенційно небезпечного районів виникнення пожеж на торфовищах;
- зменшення використання ресурсів при ліквідації пожеж на торфовищах;

Особливістю даного комплексу є застосування нового підходу, засобів та існуючих енергозберігаючих розробок при ліквідації пожеж на торфовищах, що дозволяє значно скоротити використання різного роду ресурсів. Практична реалізація проекту створення МК передбачає монтування на базі причіпного шасі спеціально бурильного та пожежно- технічного обладнання, що приводиться в дію за допомогою використання гібридної енергозберігаючої системи. Простота використання та розміщення такого автономного обладнання на базі причіпного шасі дозволить раціональніше використовувати основну пожежно-рятувальну техніку та особовий склад підрозділів.

Покращення екологічного стану потенційно небезпечних районів виникнення пожеж на торфовищах можливе в результаті створення умов швидкого реагування та тривалого використання даного автономного МК безпосередньо на місці виникнення надзвичайної події.

Засобами комп'ютерного моделювання створено 3D - модель мобільного комплексу гасіння пожеж на торфовищах, що представлена на рис. 1, де:

1. Сонячні панелі;
2. Додаткові батареї та обладнання для роборти сонячної батареї;
3. Вогнегасники;
4. Генератор;
5. Пожежно-технічне обладнання;
6. Бурова установка;
7. Насоси для подачі води;

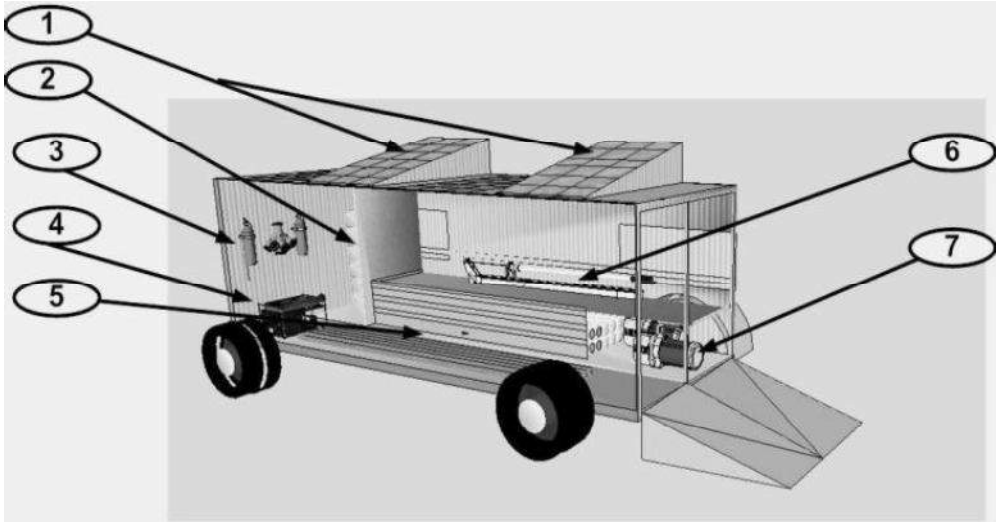

Рис. 1. *Модель створення мобільного комплексу гасіння пожеж на торфовищах у 3D вимірі*

У результаті проведеного дослідження можна зробити висновок, що мобільний комплекс для гасіння пожеж на торфовищах дозволить реалізувати проект забезпечення безпеки людей в умовах обмеженого фінансування.

Література

1. Бушуєв С. Д. Креативные технологии управления проектами и программами / С. Д. Бушуєв, Н. С. Бушуєва, И. А. Бабаєв [и др.] – К. : «Самит-Книга», 2010. – 768 с.

2. Кононенко И. В. Модель и метод оптимизации портфелей проектов предприятия для планового периода / И. В. Кононенко, К. С Бухреева // Восточно-европейский журнал передовых технологий. – 2010. – № 43. – С. 9-11.

3. Рак Ю. П. Система цивільного захисту та безпеки держави, проектно-орієнтоване управління: компетентнісний підхід / Ю.П. Рак, В.П. Квашук // Вісник ЛДУБЖД. – Львів, 2013. – №7 – С. 92-99.

4. Гуліда Е.М., Войтович Д.П. Оптимізація границь обслуговування районів міста пожежно-рятувальними підрозділами // Оптимізація наукових досліджень – 2009: Всеукраїнська наук.-практ. конф., 17 черв. 2009 р. – Зб. мат. – Миколаїв, 2009. – С. 216-218.

УДК 658.52; 681.3

ІНФОРМАЦІЙНА БЕЗПЕКА БЕЗДРОТОВИХ МЕРЕЖ

Губик О.З.
Гриник Р.О.
Львівський державний університет безпеки життєдіяльності

На сьогоднішній час широкого застосування набули без провідникові Wi-Fi мережі стандарту 802.11. Гаджети з підтримкою стандарту 802.11 організовують зв'язок один з одним, використовуючи в якості каналу передачі даних певний діапазон радіочастот. Дані передаються по радіоканалу відправником, за замовчування вважається, що приймач також працює в обраному радіодіапазоні радіочастот. Основним недоліком використання даного механізму є те, що будь-яка третя особа, яка використовує цей діапазон, теж здатна прийняти ці дані та обробити їх. Для організації захисту даних що передаються необхідно використовувати який-небудь механізм захисту, щоб забезпечити мінімальний захист мережа повинна включати в себе наступні компоненти:

- Засіб прийняття рішення, що до того хто має право доступу до мережі. Дана вимога реалізується за допомогою аутентифікації користувача.
- Механізм захисту повідомлення підчас його руху по мережі. Дана вимога реалізуються за допомогою алгоритмів шифрування інформації.

В сучасних мережах захист інформації здійснюється одночасним використанням аутентифікації користувача та шифруванням повідомлення що передається. Стандарт IEEE 802.11 підтримує використання двох методів аутентифікації [1]:

- Відкрита аутентифікація. Даний метод аутентифікації здійснює захист на основі обмеження доступу до мережі по фільтрації MAC адрес.
- Аутентифікація із загальним ключем. Даний метод здійснює захист на основі шифрування повідомлення, тобто абонент робить запит у точки доступу на що у відповідь отримує 128 байт інформації, котрі шифрує за допомогою ключа і відправляє назад до точки доступу, точка розшифровує повідомлення і порівнює з вихідним, якщо воно ідентичне надає права доступу абоненту.

Уразливість мережі при використанні відкритої аутентифікації полягає в тому, що MAC-адреси передаються за допомогою незашифрованих фреймів стандарту 802.11, що дає можливість зловмиснику прослухати мережу, дізнатись MAC-адресу яка знаходиться в «довірчому списку» точки доступу та імітувавши її підключитись до мережі.

Уразливість мережі при використанні методу аутентифікації із загальним ключем є значно нижчою ніж при використанні відкритої аутентифікації, але якщо зловмисник володіє необхідними навичками і має необхідне програмне забезпечення то через невеликий проміжок часу він отримає доступ до мережі. Уразливість обумовлена як раз тим, що механізм WEP застосовує алгоритм складання ключа на основі поточного шифру RC4. Частина векторів ініціалізації можуть розкрити біти ключа в результаті проведення статистичного аналізу. Дослідники компанії AT&T і університету Rice скористалися цією вразливістю і з'ясували, що можна дістати WEP-ключі довжиною 40 або 104 біт після обробки 4 мільйонів фреймів, це означає що для пасивного взлому мережі з довжиною ключа 104 біти зловмиснику знадобиться менше години часу. Зловмисник також може використовувати активні атаки на мережу, зміст цих атак полягає у тому що порушник впливає на мережу для отримання певної інформації для індуктивного обчислення секретного ключа. В основі активної атаки WEP лежить те, що при потоковому шифруванні відбувається XOR початкового повідомлення і ключа для обчислення зашифрованого повідомлення. Індуктивне обчислення ключа ефективне в силу відсутності хорошого методу контролю цілісності повідомлень. Значення ідентифікатора ключа (ICV), завершального кадру WEP, обчислюється за допомогою функції CRC32 (циклічний надлишковий 32-бітний код), схильною до атак з маніпуляцією бітами. В результаті існують атаки, засновані на повторному використанні вектора ініціалізації (IV Replay) і маніпуляції бітами (Bit-Flipping) [2].

Отже зі всього вище сказаного можна зробити висновок, що бездротові мережі мають багато недоліків і являються вразливими як до пасивних так і до активних атак, а тому при передачі даних через Wi-Fi мережу необхідно звертати увагу на їх зміст і якщо вони мають конфіденційну інформації краще захистити її з допомогою додаткового шифрування.

Література

1. Захист у мережах Wi-Fi [Електронний ресурс] Режим доступу: https://uk.wikipedia.org/wiki/Захист_у_мережах_Wi-Fi

2. Юдін О.К., Весельська О., Аналіз захищеності бездротових мереж з використанням WEP-технології, Наукоємні технології №3, 2012, с.62-67

УДК 005.8 + 65.012.12

ПРОЕКТНО-ОРІЄНТОВАНЕ УПРАВЛІННЯ ДОРОЖНЬО-ТРАСПОРТНИМИ ПРОЕКТАМИ НА ШОСЕ В НІЧНИЙ ПЕРІОД ЧАСУ

Данилів О.Б.

Рак Ю.П., д-р техн. наук, професор, заслужений працівник освіти України

Львівський державний університет безпеки життєдіяльності

За даними статистики значний відсоток дорожньо-транспортних пригод припадає на неосвітлених ділянках шосе, особливо в нічний період часу. Причиною такого зростання аварійності та числа жертв є як збільшення автотранспорту, різким зростанням темпу життя, що спричиняє неуважність та слабку видимість дорожньої розмітки.

Таким чином більшість сучасних доріг чи магістралей України характеризується умовами невизначеності, а адже для попередження стану безпеки необхідно впроваджувати елементи стратегічного менеджменту управління на всіх фазах реалізації проекту. Модель-схему такого управління можна представити у вигляді наступної блок-схеми. (див. рис. 1)

Рис.1. *Блок-схема використання стратегічного менеджменту в управлінні дорожньо-транспортними потоками на шосе в нічний період часу для підвищення стану безпеки*

Запропонований підхід дозволить забезпечити підвищений стан безпеки на автомагістралях у нічний період часу, а впровадження проектно-орієнтованого управління, зокрема елементів стратегічного менеджменту, вирішити строгу систематичність на всіх станах реалізації проекту та мінімізувати число жертв від дорожньо-транспортних пригод.

Література

1. Рульєв В.А., Гуткевич С.О. Менеджмент.
2. Електронна адреса статистики ДТП. Режим доступу http://nbnews.com.ua/ru/tema/96580/
3. Бушуєв С. Д. Управление проектами: основы профессиональных знаний и система оценки компетентности проектных менеджеров / С. Д. Бушуев, Н. С. Бушуева. – К.: ІРІДІУМ.

УДК 004.413.4

ОСОБЛИВОСТІ ОЦІНКИ РИЗИКІВ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Деменко В.О.
Полотай О.І.
Львівський державний університет безпеки життєдіяльності

В умовах сьогодення, великого значення набуває поняття «інформаційна безпека», яка набула статусу цілої галузі наукового дослідження. Основним об'єктом даного дослідження виступає інформація зі всіма своїми властивостями.

Порушення основних властивостей інформації може стати серйозною загрозою для організації, фірми, установи, регіону, держави, суспільства та людства загалом. Інформацію в умовах сучасного інформаційного суспільства стає все важче контролювати, оскільки вона легко підпадає під вплив великої кількості загроз і вразливостей. Серед таких загроз виступає комп'ютерне шахрайство, шпигунство, саботаж, природні катаклізми, тощо.

З кожним днем зростає ризик та ймовірність виникнення загроз інформаційної безпеки. Постає необхідність в оцінці даних ризиків, з метою зменшення ймовірності їх появи а також зниження збитків від їх настання до мінімальних значень. Оцінка ризиків є важливою складовою будь-якого процесу інформаційної безпеки. Процедуру оцінювання ризиків використовують для визначення масштабів загроз безпеці інформації, ймовірності реалізації загрози, та наслідків, які вони спричиняють.

Оцінка ризику – це складний процес, який включає в себе наступні обов'язкові кроки [1]:

1. визначення ймовірності загроз

2. розрахунок впливу, який спричиняє кожна загроза на окремі об'єкти захисту;

3. визначення кількісних та (або) якісних характеристик ризику настання кожної загрози.

Велика кількість методів оцінки ризиків інформаційної безпеки характеризуються не тільки своєю сферою використання, а й процедурами, які притаманні кожному, окремо взятому методу. На те, який саме метод оцінки ризику вибрати, впливає ряд непов'язаних один з одним факторів, серед яких варто виділити такі [2]:

- величина тимчасових часових (динамічних) рядів;
- величина допоміжної інформації та її різноманіття;
- вимоги, що адекватності моделі оцінки ризиків та точності і достовірності результатів.

Існуючі методи оцінки ризиків інформаційної безпеки поділяються на:

- статистичні – використовуються для систематизації, обробки і використання статистичних даних (часових рядів) з метою їх аналізу, для одержання змістовних висновків та розробки ґрунтовних висновків та рекомендацій;
- ймовірнісно-статистичні – базуються на поєднанні результатів аналізу статистичних даних та допоміжної інформації, з метою визначення відповідності між загрозами інформаційної безпеки та збитками, які вони спричиняють;
- теоретико-ймовірнісні – за допомогою експертної оцінки та їх статистичної оброки, використовуються з метою визначення ймовірності настання кожної загрози, про які мало відомо і які раніше не виникали. Цей метод можна віднести до експертних методів, які базуються на їх досвіді та знаннях, а також способах перевірки їх узгодженості;

Отже, при оцінці ризиків необхідно приймати до уваги всі можливі джерела загроз, які можуть мати фатальний вплив або непереборні наслідки, та оцінити їх вплив на навколишнє середовище.

Література

1. Левадний С.М. Оцінка інформаційних активів / С.М. Левадний. [Електронний ресурс]. – Режим доступу з http://www. rusnauka.com/21_SEN_2014/ Informatica/4_174674.doc.htm

2. Цуркан В.В. Проблеми оцінки ризиків інформаційної безпеки / В.В. Цуркан. [Електронний ресурс]. – Режим доступу з http://nc.asta.edu.ua/Kyrsi%202009/tezi/images_tezi/S_6_Curkan.htm

УДК 004.057.4

ПОРІВНЯЛЬНИЙ АНАЛІЗ КРИПТОГРАФІЧНИХ МЕТОДІВ АУТЕНТИФІКАЦІЇ ПОВІДОМЛЕНЬ

Денисюк В.А.
Лагун А.Е., канд. техн. наук, доцент
Львівський державний університет безпеки життєдіяльності

На цей час через інтенсивний розвиток інформаційних технологій та використання глобальної мережі Internet, обмін електронною кореспонденцією потребує особливого захисту. Крім того, актуальною є проблема захисту інформації, яка передається через комп'ютерні мережі. Забезпечити надійний захист конфіденційної інформації від несанкціонованого доступу, підтвердити авторство власників інформації, проконтролювати цілісність переданої інформації дозволяють криптографічні методи захисту інформації.

Розглянемо особливості застосування криптографічних методів для контролю незмінності масивів даних і аутентифікації повідомлень.

Для надійного контролю незмінності масивів даних використовуються два підходи [2]: обчислення MAC – Message Authentification Code – коду аутентифікації повідомлень і обчислення MDC – Manipulation Detection Code – коду виявлення маніпуляцій (з інформацією).

Обчислення MAC вимагає для обчислення контрольної комбінації знання секретного ключа, а при виявленні маніпуляцій ключа не потрібно. Зловмисник не зможе обчислити MAC для довільно створеного ним повідомлення, проте зможе обчислити MDC, через те що для цього не потрібно секретних даних. Зважаючи на це, MAC може передаватися від передавача до приймача повідомлень відкритим каналом, а для передавання MDC повинен використовуватися захищений канал.

Для вироблення коду аутентифікації вхідне повідомлення розбивається на блоки B_1, B_2, …, B_n і для кожного блоку виконується перетворення за криптографічним алгоритмом E_K, як побітова сума за модулем 2 поточного блоку і результату виконання попереднього кроку. Отже, контрольна комбінація має вигляд:

$$C = C_K(B) = E_K(B_1 \oplus E_K(B_2 \oplus E_K(\ldots \oplus E_K(B_n)))). \quad (1)$$

Іншим методом аутентифікації повідомлень є використання цифрового підпису. В загальному випадку цифровий підпис – це набір алгоритмів і протоколів, що дозволяють побудувати інформаційну взаємодію між двома й більше учасниками таким чином, щоб факт авторства переданого масиву даних міг бути підтверджений або спростований незалежною третьою стороною. Будь-яка схема цифрового підпису передбачає доповнення певного інформаційного масиву додатковим кодом (цифровим підписом), створити який може лише автор повідомлення за допомогою секретного ключа підпису, а всі інші користувачі можуть лише перевірити відповідність цього підпису підписаним даним [1].

Аутентифікація з використанням цифрового підпису вимагає виконання таких кроків:

1) створення пари відкритого і закритого ключів, причому закритий буде використовуватися для підпису інформаційного повідомлення, а відкритий – для перевірки підпису;
2) підписування інформаційного повідомлення за допомогою закритого ключа і якогось алгоритму шифрування;
3) перевірка підпису за допомогою відкритого ключа і алгоритму розшифрування;
4) застосування необоротної хеш-функції для інформаційних масивів, що підписуються.

Останній крок використовується для зменшення величини цифрового підпису, оскільки при великих обсягах даних без використання хеш-функції розмір підпису був би майже таким самим, як і розмір підписаного повідомлення.

В роботі було проведено дослідження схеми цифрового підпису Діффі й Хеллмана [3]. В цьому випадку генерують випадкову послідовність розміру $2n$, яка буде закритим ключем підпису K_z . Закритий ключ складається з двох підключів K_1 і K_2, які використовуються для знаходження ключа перевірки підпису K_V за допомогою алгоритму шифрування E_K:

$$K_V = (E_{K_1}(B_1), E_{K_2}(B_2)) = (K_{V1}, K_{V2}). \quad (2)$$

При підписуванні біта (0 або 1) вибирають відповідну половину закритого ключа

Для перевірки підпису будь-який користувач, знаючи цифровий підпис біта (K_1 або K_2), відповідну частину ключа перевірки підпису K_{V1} або K_{V2}, може обчислити $E_{K_i}(B_i)$і перевірити його на рівність з K_{Vi}. У випадку рівності автора цифрового підпису аутентифіковано.

В подальших дослідженнях планується реалізувати цифрові підписи бітових груп з використанням різних алгоритмів шифрування і визначити їх ефективність.

Література

[1] Баричев С. Г., Гончаров В. В., Серов Р. Е. Основы современной криптографии. – М.: Горячая линия. – Телеком, 2001. – 120 с.

[2] Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М: Издательство Триумф, 2003. – 816 с.

[3] W.Diffie, M.E.Hellman. New Directions in cryptography// IEEE Trans. Inform. Theory, IT-22, vol 6 (Nov. 1976), pp. 644-654.

УДК 351.651: 620.26: 004.422

ОСНОВНІ ЗАСАДИ СТВОРЕННЯ ДОВІДНИКОВО-АНАЛІТИЧНОГО ПРОГРАМНОГО КОМПЛЕКСУ ДЛЯ ПІДРОЗДІЛІВ ОРС ЦЗ

Жаврук П.С.
Нуянзін В.М., канд. техн. наук
Черкаський інститут пожежної безпеки імені Героїв Чорнобиля НУЦЗУ

Метою розробки довідниково-аналітичного програмного комплексу «Довідник небезпечнихречовин» було створення інформаційної системи яка б дозволила підвищити ефективність роботи підрозділів ОРС ЦЗ під час ліквідації наслідків НС. Оснащення даною програмою комп'ютерів, наприклад диспетчерів оперативно-координаційного центру, дозволить швидко ідентифікувати небезпечну речовину під час виникнення надзвичайної ситуації та передавати керівнику ліквідації НС всю необхідну інформацію стосовної її властивостей, а також рекомендацій щодо засобів захисту особового складу та необхідних дій підрозділів при локалізації та ліквідації аварійних ситуацій.

На теперішній час в ДСНС України розроблено та діють 2 довідники про небезпечні речовини [2, 3]. На закордонному ринку програмного забезпечення існують продукти, що дозволяють проводити ідентифікацію небезпечних речовин за декількома параметрами. Вони відрізняються між собою функціональними можливостями, програмними платформами, інтерфейсом користувача, необхідністю доступу до мережі інтернет та ін.

Проте жодну з існуючих відомих світових електронно-довідникових систем неможливо в повній мірі використовувати в Україні з метою підвищення ефективності роботи підрозділів ОРС ЦЗ. Розроблена комп'ютерна програма повинна була задовольняти всім вимогам сьогодення, бути легкою в користуванні та інформативною, окрім того вона повинна опиратися на чинну нормативно-правову базу України.

Аналіз програмно-апаратного забезпечення для реалізації довідниково-аналітичного програмного комплексу показав, що оптимальним середовищем розробки програмного забезпечення є Borland C ++ Builder [3].

Готовий програмний продукт має досить простий інтерфейс, який умовно можна розділити на 3 блоки (рис. 3):

1. Класифікаційний блок – представлений 5 кнопками, що дозволяють перемикати пошук за українською, російською та англійськими назвами, кодом ООН та аварійною карткою.
2. Інформаційна база даних – відображає поле пошуку та поточний перелік небезпечних речовин.
3. Головний інформаційний блок складається із 4 вкладок – Оперативна інформація; Аварійна картка; Зворотній зв'язок та вкладки Роздрукувати.

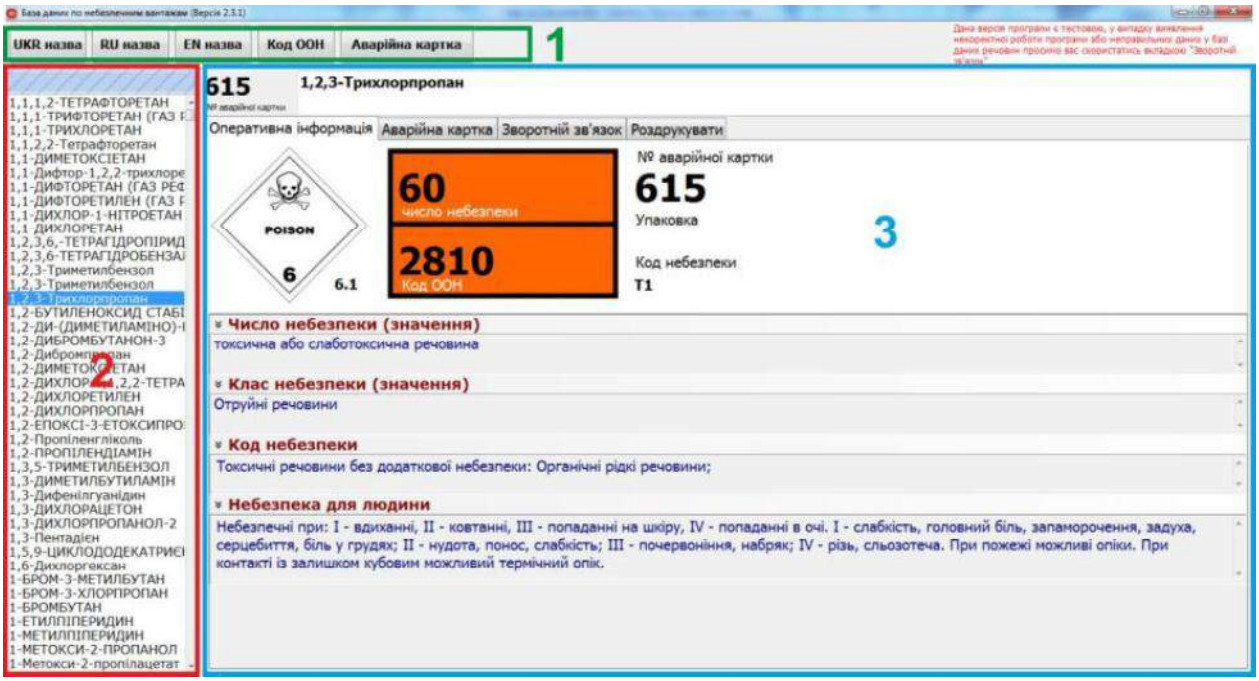

***Рис. 3** – Інтерфейс робочого вікна програмного продукту*

4. Класифікаційний блок – представлений 5 кнопками, що дозволяють перемикати пошук за українською, російською та англійськими назвами, кодом ООН та аварійною карткою.

5. Інформаційна база даних - відображає поле пошуку та поточний перелік небезпечних речовин.

6. Головний інформаційний блок складається із 4 вкладок – Оперативна інформація; Аварійна картка; Зворотній зв'язок та вкладки Роздрукувати.

У результаті проведених досліджень розроблено довідниково-аналітичний програмний комплекс «Довідник небезпечних речовин», що підвищує ефективність дій підрозділів ОРС ЦЗ у разі виникнення НС, які пов’язані з обігом небезпечних речовин.

Література

1. Небезпечні хімічні речовини в природі, промисловості і побуті. Довідник експрес-інформації у символах / Під ред.. О.В. Гайдука. – К.: Агентство «Чорнобильінтерінформ», 1998.

2. Інформаційний довідник з маркування небезпечних вантажів, які перевозяться на залізничному та автомобільному транспорті. – К. УкрНДІПБ МНС України, 2007.

3. Нуянзін В.М., Биченко А.О., Пустовіт М.О., Удовенко М.Ю. Розроблення нових заходів захисту від шкідливих речовин // «Надзвичайні ситуації: безпека та захист». Матеріали IV Міжнародної науково-практичної конференції – Черкаси: ЧІПБ ім. Героїв Чорнобиля НУЦЗ України, 2014. –с. 266-267.

УДК 005.8

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ЯК ЗАСІБ ОПЕРАТИВНОГО УПРАВЛІННЯ ПРОЕКТОМ ПІДВИЩЕННЯ БЕЗПЕКИ ПОТЕНЦІЙНО-НЕБЕЗПЕЧНИХ ОБ'ЄКТІВ

Жовтянський М.С.
Рак Ю.П., д-р техн. наук, професор, заслужений працівник освіти України
Львівський державний університет безпеки життєдіяльності

Інтенсивне впровадження інформаційних технологій у всі сфери виробничої діяльності, а також високий рівень невизначеності при виникненні надзвичайних ситуацій (далі – НС) вимагає особливої уваги щодо виконання рятувальних робіт. Такий стан вимагає повсякденного використання оперативно-рятувальними службами у своїй діяльності інновацій, що базуються на інтегруванні ІТ-технологій та комп'ютерно-інтегрованих комплексів, здатних виконувати оперативно-рятувальну діяльність, як на попереджувальній фазі, так і на всіх інших фазах проекту підвищення безпеки на потенційно-небезпечних об'єктах (ПНО).

Успіх реалізації такого проектно-орієнтованого управління службами, у відповідності до всіх ієрархій ДСНС України, вимагає створення умов оперативного доступу до баз даних та баз знань.

Нами запропонована модель інформаційно-пошукової експертної системи (УПЕС) див. рис.1., що забезпечує постійну інформаційну підтримку для рятувальника засобами GPS-навігації.

Рис. 1. *Модель-схема інформаційно-пошукової системи оперативного управління інформаційним ресурсом засобами GPS-навігації*

Запропоновано проектне середовище оперативного управління силами та засобами, що входять у структурні підрозділи ДСНС України використовуючи елементи іновінгу та GPS-навігації (див. рис. 2).

Рис.2. Блок-схема проектного середовища оперативного управління рятувальними службами засобами GPS-навігації

Очікуваними результатами після реалізації даного проекту є:

- Проведення детальної розвідки під час слідування на ПНО з використанням даної програми;
- Зменшення рівня матеріальних збитків при виникненні НС на ПНО, шляхом отримання достовірної інформації про об'єкт;
- Впровадження новітніх технологій у ДСНС.

Література

1. Кодекс цивільного захисту України від 02.10.2012 № 5403-VI.
2. Рак Ю. П. Інформаційні технології як засіб реалізації інноваційних процесів при підготовці сучасного фахівця з аварійно-рятувальних робіт / Ю. П. Рак // Освіта регіону. – № 3. – 2010.
3. Рак Ю. П. Система цивільного захисту та безпеки держави, проектно-орієнтоване управління: компетентнісний підхід / Ю. П. Рак, В. П. Квашук // Вісник ЛДУБЖД. – Львів, 2013. – №7.

УДК 514.18

ОСОБЛИВОСТІ ВПЛИВУ ІНФОРМАЦІЙНОГО ЧИННИКА НА ЗДОРОВ'Я ЛЮДИНИ ТА БЕЗПЕКУ СУСПІЛЬСТВА

Задорожна Х.О.
Кузиляк В.Й.
Львівський державний університет безпеки життєдіяльності

Основною причиною будь-якого конфлікту є психологічна діяльність людини. Формування людської психіки, починається з моменту народження особистості. Основним джерелом формування особистості в сучасному світі є новітні технології засобів масової інформації.

На сьогодні інформація набула глобального значення, важливим є поняття «Інформаційно-гібридна війна». Це комплекс аспектів, що впливають на суспільство з метою психічного контролю над ним.

Не зважаючи на певні переваги комп'ютерного віку, він також негативно впливає на психічний, емоційний та фізичний розвиток особливо підростаючого покоління. Проведення дітьми більшої частини свого дозвілля вдома, біля телевізора чи комп'ютера призводить до погіршення стану здоров'я, зниження інтересу до активного використання вільного часу, що часто призводить до формування пасивності, байдужості тощо, що в майбутньому може вплинути на розвиток суспільства.[2]

На сьогоднішній час, на жаль, не існує достатніх гарантій захисту особи від загроз, пов'язаних з порушенням інформаційної та інформаційно-психологічної безпеки особистості. Немає єдиної системи знань, яка дозволяла б розкривати можливості біоенергетики без шкоди здоров'ю людини. Існує численна кількість публікацій, що свідчить про спроби використання механізмів інформаційно-енергетичного впливу на людину з метою програмування її дій, поведінки. Застосовуються технології, засоби та методи психофізичного впливу на великі соціальні групи людей через свідомість і підсвідомість людини з метою формування необхідних подій та маніпулювання громадською думкою.

Джерелами загроз інформаційного простору є суперечності певних інтересів, систем цінностей, цілей між особистістю та суспільством, державою або наявністю в однієї зі сторін стосовно іншої домагань, претензій або інших спонукувань до конфлікту. Найбільш небезпечним джерелом загроз цим інтересам вважається суттєве розширення можливостей маніпулювання свідомістю людини через створення навколо неї індивідуального віртуального інформаційного простору, а також можливість використання технологій впливу на її психічну діяльність.[1]

Таким чином, маніпулювати людиною можна завдяки запланованій системі дій, яка може бути направлена на підкорення одних груп людей іншими групами за допомогою певних методів та засобів інформаційної війни.

Література

1. Інформаційна безпека (соціально-правовіаспекти): Підручник / Остроухов В. В., Петрик В. М., Присяжнюк М. М. та ін.; за ред. Є. Д. Скулиша. – К. : КНТ, 2010. –776 с.

2. [http://studopedia.su/ 9 45768 suchasni – informatsiyni – tehnologii – ta-bezpekazhittiediyalnosti-lyudini-osoblivosti-vplivu-informatsiynogo-chinnika-na-zdorovya-lyudini-ta-bezpeku-suspilstva.html]

УДК 504.054

ПРОГНОЗУВАННЯ НАСЛІДКІВ АВАРІЙ НА ЗАПОРІЗЬКІЙ АЕС З ВИКОРИСТАННЯМ ПРОГРАМНОГО ПРОДУКТУ

Закарян К. А.
Клеєвська В. Л.
Національний аерокосмічний університет им. Н. Є. Жуковського «ХАІ»

Електроенергетика - одна з провідних галузей сучасної промисловості. Темпи зростання виробництва електроенергії значно вище ніж у всіх інших галузях виробництва.

За оцінками Міжнародного енергетичного агентства споживання енергії у світі за останні 30 років зростало зі швидкістю більше 3% на рік. Зростання народонаселення (до 2% на рік) і економічний розвиток у XXI столітті призведуть до підвищення світового виробництва в 3-5 разів до 2050 року і в 10-15 разів до 2100 року. Це вимагатиме збільшення енергозабезпечення в 3-5 разів.

Згідно з висновками ряду дослідників, атомні електростанції сприяють скороченню викидів в атмосферу парникових газів, використання атомної енергії замість викопних видів палива дозволило запобігти загибелі від забруднюючих природне середовище викидів близько 1,8 млн. чол. в усьому світі. У випадку аварії атомні електростанції представляє дуже серйозну небезпеку для населення і навколишнього середовища.

За всю історію існування атомних електростанцій на деяких з них, траплялися катастрофічні за своїми наслідками аварії. У 1979 році сталася серйозна аварія на АЕС Три Майл Айленд в США, у 1986 році – масштабна катастрофа на Чорнобильській АЕС, яка серйозно відбилася на всій ядерній енергетиці в цілому, а у березні 2011 року відбулася остання велика аварія на АЕС Фукусіма-1 в Японії, викликана сильним землетрусом і подальшим цунамі.

За показником виробництва електроенергії на АЕС Україна входить до вісімки, а за вкладом одержуваної електроенергії в загальний обсяг електроенергії - до п'ятірки країн світу. Ядерна енергетика в Україні є важливою

складовою загального паливно-енергетичного комплексу і займає провідні позиції в електропостачанні країни.

Запорізька АЕС (ЗАЕС) - найбільша атомна електростанція в Європі; рішення про її будівництво було ухвалене в 1978 році. ЗАЕС розташована в степовій зоні на березі Каховського водосховища в Запорізькій області України поруч з містом Енергодар.

На Запорізькій атомній електростанції усі шість ректорів віднесені до реакторів типу ВВЕР-1000. Реактор типу ВВЕР – реактор енергетичний, водо-водяний, гетерогенний, на теплових нейтронах, з водою в якості теплоносія, сповільнювача й відбивача нейтронів, реактор типу ВВЕР-1000 - ядерний реактор серії реакторів ВВЕР з номінальною електричною потужністю 1000 МВт, теплової – 3000 МВт.

Варто відзначити, що радіаційний стан навколишнього середовища є найважливішою характеристикою, що визначає умови безпечної життєдіяльності людини. Тому, починаючи з 50-х років XX століття, ведення радіаційного контролю та моніторингу є одним із пріоритетних завдань в галузі охорони навколишнього середовища та забезпечення радіаційної безпеки.

Радіаційний стан характеризується рівнями радіації і розмірами зон радіоактивного зараження або забруднення, які є основними показниками небезпеки для життя людей і роботи промислових підприємств.

Для автоматизованого прогнозування розмірів зон можливого радіоактивного забруднення унаслідок аварії на ЗАЕС розроблено програмне забезпечення, що дозволяє швидко і якісно оцінити масштаби забруднення і вжити заходів щодо їх усунення, врятувати життя населення.

При оперативному прогнозуванні наслідків аварії на ЗАЕС з використанням запропонованого програмного продукту можна миттєво отримати параметри зон можливого радіаційного забруднення.

Такий прогноз здійснюється з урахуванням метеорологічних умов на момент аварії і величини викиду радіоактивних речовин для ЗАЕС.

Література

1. Бєгун В. Чи безпечні атомні електростанції України? Надзвичайна ситуація. – 2010. – № 4. – С. 48 – 51.

2. Методика прогнозування соціально-економічних наслідків надзвичайних ситуацій техногенного характера, спричинених аваріями з викидом радіоактивних речовин / упоряд. Л.Б. Яковлев – Х.: «ХАІ», 2000. – 30с.

УДК 004.056.5

ФОРМАЛІЗОВАНЕ ПРЕДСТАВЛЕННЯ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СПРИЧИНЕНИХ ПЕРСОНАЛОМ

Іванчук Т.С.
Кухарська Н.П., канд. фіз.-мат. наук, доцент
Львівський державний університет безпеки життєдіяльності

Забезпечення безпеки конфіденційної інформації (КІ) завжди було і залишається однією з важливих проблем захисту інформації. У результаті її витоку зазнає значного матеріального і морального збитку не тільки власник КІ, але і держава у цілому.

Це пов'язано з очевидними і цілком об'єктивними закономірностями, які мають місце у сучасних непростих умовах інформаційних взаємовідносин. Проведені Аналітичним центром InfoWatch дослідження [1] демонструють доволі стійку тенденцію до збільшення кількості випадків витоку КІ. Аналіз статистичних даних показує: у 2014 році 73 % витоків КІ були наслідком впливу внутрішніх загроз на автоматизовану інформаційну систему, її відносно самостійні структурні елементи. У розподілі за характером дій порушника у 81 % випадках зафіксований "класичний" витік – втрата контролю над інформацією. 12 % усіх витоків конфіденційних даних зв'язано з неправомірним використанням інформації, до якої працівники мали легітимний доступ. У таких випадках, як правило, мова йде про фінансове шахрайство банківських працівників. 7 % зареєстрованих інцидентів класифіковано як порушення, що пов'язані з отриманням несанкціонованого доступу до інформації (перевищення прав доступу, маніпуляція з інформацією, котра не потрібна працівнику для виконання службових обов'язків) У 2014 році внутрішні зловмисники майже не використовували такі канали передачі інформації, як мобільні пристрої (0,2 %), знімні носії (2,0 %), електрону пошту (1,2 %), паперові документи (4,9 %). "Просунутий" зловмисник став обізнаним: сучасні засоби контрою дають змогу успішно перехопити передачу КІ перерахованими каналами і через те не ризикував даремно. Водночас, зауважимо, частка витоків не завжди відображає розмір небезпеки, пов'язаний з конкретним каналом. Цілком очевидно, достатньо одного випадку витоку критично важливої інформації, наприклад, каналом "Електронна пошта", щоб організація стикнулася з багатомільйонними втратами.

Ризики спричинені персоналом є окремою групою ризиків інформаційної безпеки (ІБ) організації, позаяк, спектр причин і умов їх реалізації доволі широкий. Опишемо ризики, джерелом яких є персонал, у вигляді факторної моделі – системи причин й умов, що сприяють їх реалізації (рис. 1).

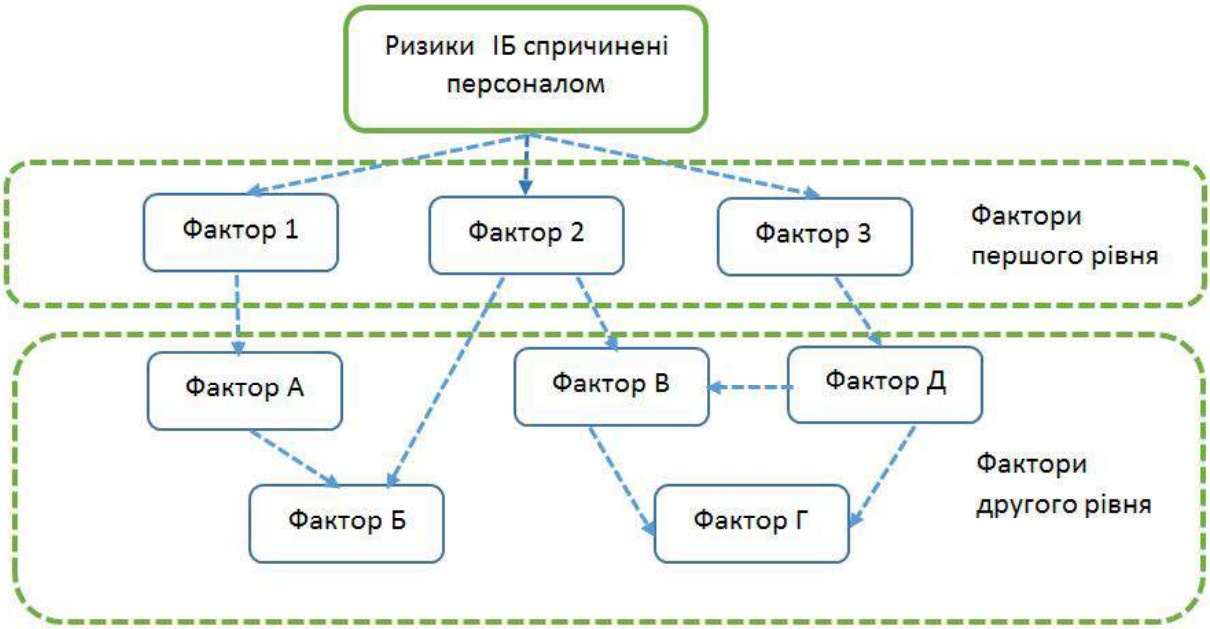

Рис.1. *Узагальнена структура факторної моделі ризиків ІБ, джерелом яких є персонал*

Виокремимо два рівні факторів:

- Фактори ризику другого рівня – явища, котрі можуть оброблятися (оцінюватися, управлятися) організацією кожен зокрема, між факторами цієї групи існують багаточисленні зв’язки, можливі цикли як позитивного, так і негативного зворотного зв’язку.
- Фактори ризику першого рівня безпосередньо впливають на реалізацію ризиків від персоналу, вони консолідують вплив всієї множини факторів ризику другого рівня і дають змогу спростити роботу з моделлю. Зв'язки всередині групи факторів першого рівня відсутні.

Фактори ризику першого рівня деталізуються через систему факторів ризику другого рівня – більш дрібних (і через те більш зрозумілих) явищ, що сприяють реалізації загроз ІБ від персоналу. Відзначимо, що деякі фактори другого рівня можуть повторюватися для декількох факторів першого рівня, оскільки впливають на них одночасно.

На основі використання запропонованої моделі підвищення захищеності організації щодо загроз ІБ від персоналу може бути досягнуто шляхом оцінювання та контролю з боку організації факторів ризику другого рівня.

Література

1. Глобальное исследование утечек конфиденциальной информации в 2014 году [Электронный ресурс]. – Режим доступа : http://www.infowatch.ru/report2014

УДК 658.012.32

РИЗИКОУТВОРЮЮЧІ ФАКТОРИ СЕРЕДОВИЩА ПРОЕКТУ

Копитіна М.В.
Одеська національна академія зв'язку ім. О.С. Попова

Середовище функціонування проекту перебуває в умовах невизначеності та характеризується появою ризиків, що зумовлені впливом зовнішніх та внутрішніх причин. Багатогранність змісту ризиків обумовлюється різноманітністю ризикоутворюючих факторів і властиві всім видам діяльності. Однією із найголовніших задач управління ризиками є аналіз ризикоутворюючих факторів, що визначає успішність існування проекту.

Під ризикоутворюючими факторам в проектній діяльності, слід розуміти сутність процесів або явищ, що сприяють виникненню того чи іншого виду ризику і визначають його характер [1]. Вплив факторів поширюється як на певні, так і на цілі групи ризиків. В узагальненому вигляді ризикоутворюючі фактори доцільно розділити на зовнішні та внутрішні. Структура розподілу факторів на групи, при виконанні проекту представлена на рис. 1.

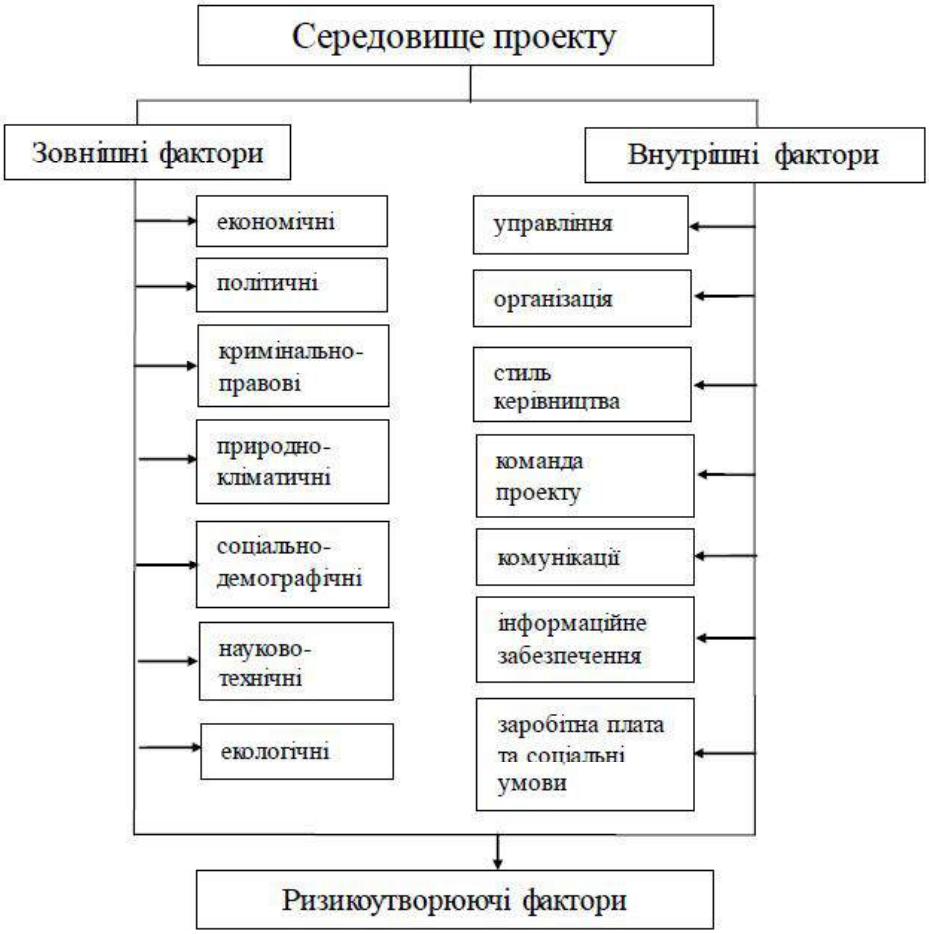

Рис. 1. *Структура ризикоутворюючих факторів середовища проекту*

Зовнішні фактори ризику існують поза функціонуванням проекту і до них відносяться такі як: економічні, політичні, кримінально-правові, природно-кліматичні, науково-технічні, екологічні.

Внутрішні фактори пов'язані з організаційно-економічними механізмами реалізації проекту. Серед внутрішніх факторів ризику можна виділити основні:

1) управління та організація проектом;
2) стиль та методи керівництва;
3) система взаємодії між учасниками проекту;
4) професіоналізм команди проекту;
5) засоби комунікації;
6) санкції за порушення;
7) наявність інформаційного забезпечення
8) заробітна плата та соціальні умови.

Таким чином, ідентифікація та аналіз ризикоутворюючих факторів необхідні для успішної реалізації проекту на всіх стадіях життєвого циклу, оскільки проведення цих процедур, дозволить підвищити ефективність системи управління ризиками в проектній діяльності.

Література

1. Кузнецова Н.В. Управление рисками: учеб. пособие / Н.В.Кузнецова. — Владивосток: Издательство Дальневосточного университета, 2004 — 168 с.

2. Вишняков Я.Д. Общая теория рисков: учеб. пособие для студ. высш. учеб.заведений / Я.Д.Вишняков, Н.Н.Радаев. — 2-е изд., испр. —М.: Издательский центр «Академия», 2008. — 368 с.

УДК 654.1

АНТИШПИГУНСЬКИЙ ЗАХИСТ GSM МЕРЕЖ МОБІЛЬНОГО ЗВ'ЯЗКУ

Косиєв О. А.
Гриник Р.О.
Львівський державний університет безпеки життєдіяльності

Мобільний зв'язок став невід'ємною частиною нашого життя, але розвиток мобільних технологій зумовлює розвиток шпигунського програмного забезпечення, в тому числі і для прослуховування розмов по мобільному телефону, тому захист мобільного телефону від прослуховування стає дедалі актуальнішим питанням.

Технологія глобальної системи мобільного зв'язку (Global System for Mobile Communications) спершу створювалась і впроваджувалась із врахуванням усіх державних вимог щодо рівня захищеності. Більшість держав світу для забезпечення підтримки цього рівня ввели заборону на використання і продаж потужних шифраторів, скремблерів, криптографічного обладнання, тощо. Самі ж оператори мобільного зв'язку захищають радіоканали шляхом шифрування сигналу з використанням достатньо складних алгоритмів.

Розрізняють кілька методів прослуховування абонентів – активний і пасивний. Для пасивного прослуховування абонента необхідне спеціальне устаткування та підготовлений персонал. На сьогодні на "чорному" ринку можна придбати цілі комплексні системи які дають можливість здійснювати прослуховування абонентів у радіусі 500 метрів. Опис таких систем і принцип їх роботи можна легко знайти в Інтернеті. За допомогою такого обладнання можна відстежувати GSM-розмови в реальному часі, ґрунтуючись на доступі до SIM-картки людини чи бази даних оператора мобільного зв'язку. Також розмови можна прослуховувати із затримкою, залежно від використовуваного оператором рівня шифрування у випадку, якщо доступ до бази даних відсутній. Така система також може бути і частиною мобільного комплексу відстеження й прослуховування рухомих об'єктів.

Другий метод прослуховування – це активне втручання в ефір. Для роботи з таким комплексом, який складається з кількох модифікованих телефонів та комп'ютера необхідний персонал, який володіє достатньою кваліфікацією в сфері зв'язку. Принцип дії такої атаки полягає в перехопленні мобільною системою сигналів для встановлення з'єднання і передачі даних за рахунок ближчого місцезнаходження до абонента (до 500 м), замінюючи найближчу базову станцію. Тобто комплекс стає "посередником" між абонентом і базовою станцією з усіма проблемами безпеки зв'язку, які виникають в такій ситуації. Такий мобільний комплекс після з'єднання здатен виконувати будь-яку функцію з керуванням зв'язком, в тому числі, з'єднати його з будь-яким необхідним номером чи, навіть, скасувати шифрування для довільного сеансу зв'язку.

Існує ще третій спосіб для прослуховування розмов і перехоплення трафіку мобільного абонента, для цього на смартфон «жертви» необхідно встановити шкідливе програмне забезпечення, при встановленні якого зловмисники можуть самі вибрати або й взагалі скасувати алгоритм шифрування, передати (або знищити) конфіденційну інформацію абонента і багато іншого.

Для сучасних смартфонів існують спеціальні програми, які можуть повідомляти користувача про конфігурацію налаштувань поточного сеансу зв'язку, у тому числі – чи передається його розмова відкрито, чи з використанням алгоритму шифрування.

EAGLE Security. Потужна програмний засіб для захисту мобільних телефонів від прослуховування, який шляхом перевірки сигнатур та ідентифікаторів базових станцій допомагає уникнути підключення до фальшивих базових станцій. Також, він здатний відзначати базові станції як підозрілі шляхом відстежування їх розташування, якщо вони переміщаються по місту або періодично зникають зі свого місця дислокації. Додаток дає можливість отримати перелік програмного забезпечення, встановленого на телефоні, яке має доступ до мікрофона та відеокамери, а також заборонити доступ небажаних програм до камери.

Android IMSI-Catcher Detector. Програмний комплекс, який дає змогу захистити смартфон від підключення до фальшивих базових станцій.

GSM SpyFinder. Дана програма здатна захистити смартфон від різного типу шпигунського устаткування, зокрема від активного GSM перехоплювача з дешифратором A5.x, який може перехоплювати вхідні та вихідні GSM дзвінки і SMS з будь-яким типом шифрування в реальному часі. Також додаток може захистити від 3G IMSI/IMEI/TMSI кетчера, який призначений для впливу на обраний телефон, щоб змусити його переключитися в режим GSM, для можливості перехоплення даних з такого телефону пасивним інтерцептором. GSM Spy Finder дає можливість оминути загрози, які виникають через блокувальними стільникових телефонів (стільниковий брандмауер), для вибіркового або масового придушення GSM/UMTS цілей.

Технологія GSM, яку використовують стільникові телефони володіє рядом вразливостей, які можуть порушити конфіденційність будь-якої інформації, яка передається мобільним зв’язком. Але завдяки створеним ресурсам та додаткам існує можливість зменшити кількість таких порушень або, навіть, звести імовірність таких порушень до мінімуму.

Література

1. Прослуховування мобільних телефонів [Електронний ресурс] Режим доступу:
http://it-tehnolog.com/statti/prosluhovuvannya-mobilnogo-telefonu/

2. Хома В. В., загрози інформаційній безпеці абонентів стаціонарних телефонних мереж, Вісник Національного університету "Львівська політехніка". – 2008. – № 608: Автоматика, вимірювання та керування. – С. 74-85.

УДК 004.056.55

ВИКОРИСТАННЯ ФРАКТАЛЬНИХ ПЕРЕТВОРЕНЬ ДЛЯ ПРИХОВУВАННЯ ІНФОРМАЦІЇ В НЕРУХОМИХ ЗОБРАЖЕННЯХ

Кошеленко Ю.В.
Лагун А.Е., канд. техн. наук, доцент
Львівський державний університет безпеки життєдіяльності

Проблема захисту інформації від несанкціонованого доступу в основному вивчається двома науками – криптографією та стеганографією. Метою криптографії є приховування вмісту повідомлень за рахунок їхнього шифрування. На відміну від цього, в стеганографії приховується сам факт існування таємного повідомлення. Історично стеганографія з'явилася швидше, проте пізніше була витиснена криптографією. При криптографії наявність шифрованого повідомлення привертає увагу супротивників, а при стеганографії наявність прихованого зв'язку залишається непомітною.

На цей час на зміну класичній стеганографії прийшла комп'ютерна стеганографія, для якої характерно приховування інформації у цифрових даних, що мають аналогову природу. Такими даними є мова, аудіозаписи, нерухомі зображення (фото), відеопослідовності.

В стеганографії використовується математичний апарат, який подібний до опису алгоритмів стиснення інформації з втратами, оскільки, як і при стисненні даних, здійснюється нехтування певними незначущими областями контейнера, в якому міститься прихована інформація [2]. Зокрема, для приховування інформації в нерухомих зображеннях використовуються фрактальне кодування і вейвлет перетворення.

Методи фрактального кодування використовують два різних підходи до виявлення структури даних зображення [1]. Один із них використовує теорію ітерованих функцій. Проте значно кращим є метод фрактального кодування, в якому використовуються системи доменних і рангових блоків зображення. Згідно з цим підходом зображення розбивається на множину рангових підзображень, які не перекриваються, а також визначається множина доменних підзображень, які перекриваються. Для кожного рангового блоку алгоритм кодування знаходить найбільш властивий доменний блок і афінне перетворення для відображення цього доменного блоку в ранговий. Результуюча структура зображення є системою рангових блоків, доменних блоків та перетворень.

Структуру алгоритму фрактального кодування наведено на рис. 1. Код закодованого фрактальними методами зображення – це список, який містить інформацію про розташування рангового блоку, домен, який відображається в цей ранговий блок і параметри, які описують перетворення доменного блоку в ранговий.

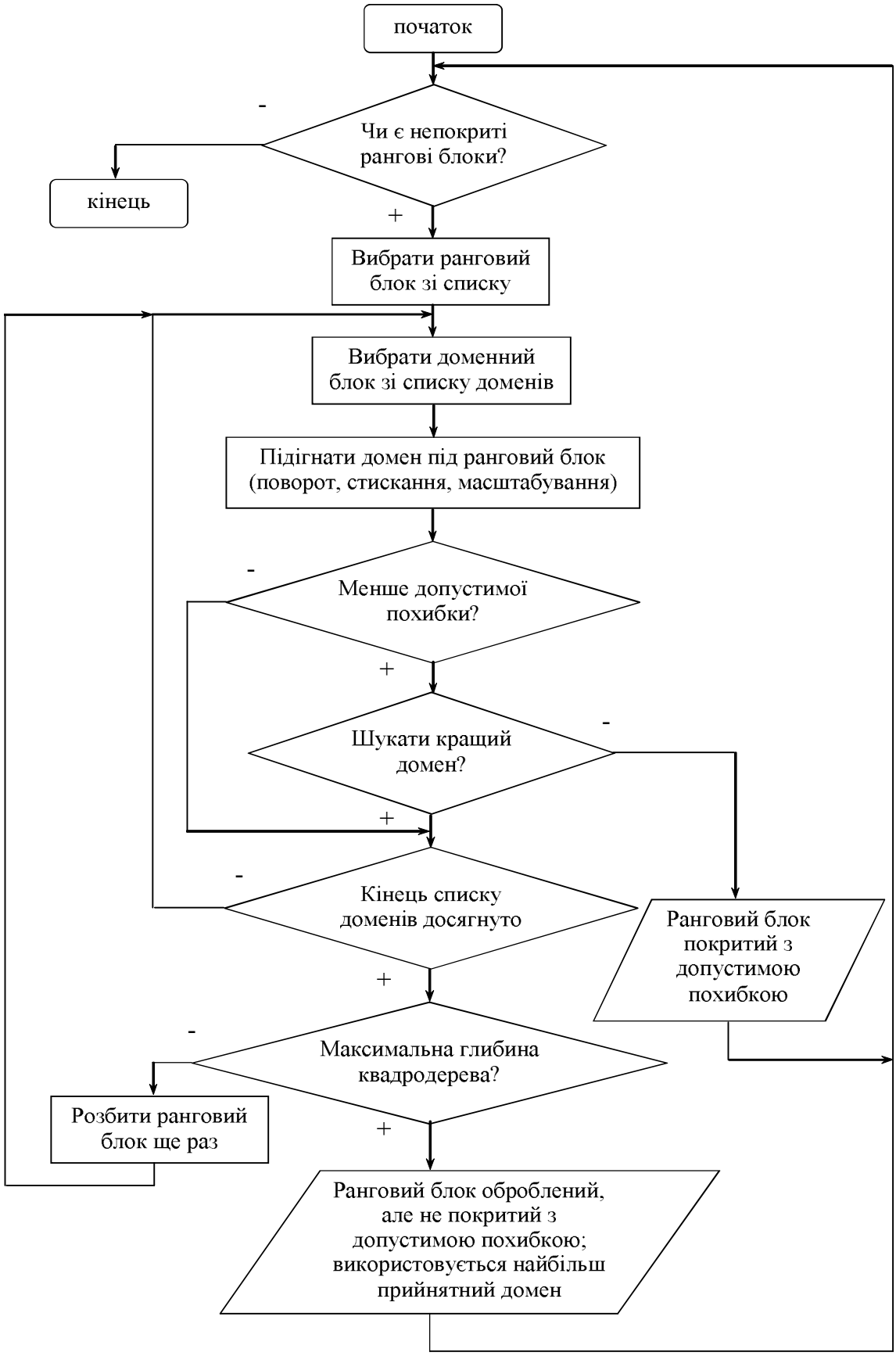

Рис. 1. *Алгоритм фрактального кодування*

Розглянемо стеганографічний алгоритм, що використовує фрактальне кодування зображення [3].

Нехай прихована інформація є рядком біт. Секретним ключем є вибір рангового блоку. Кількість рангових блоків, на які розбивають зображення визначає максимальну кількість прихованих бітів. Доменний простір поділяють на дві частини, одна з яких відповідає вбудовуванню нулів, а інша – вбудовуванню одиниць.

Відповідно до секретного ключа рангового блоку в доменному просторі шукається відповідний блок, а саме для приховування одиниці пошук відбувається в одній частині простору, а приховування нуля – в іншій. Для рангових блоків, в які не приховують інформацію (біти), пошук відбувається в цілому доменному просторі.

Після фрактального кодування зображення здійснюється його декодування для отримання початкового зображення і секретної інформації. Декодер, знаючи секретний ключ, виконує зворотні перетворення видобуваючи приховану інформацію.

Недоліком алгоритму фрактального кодування є значні затрати часу при збільшенні розміру прихованої інформації через збільшення кількості рангових блоків. Проте, за рахунок можливості розпаралелювання процесу фрактального кодування (доменно-рангове порівняння можна проводити паралельно для множини фрагментів зображення), швидкість процесу приховування інформації значно збільшується.

Література

[1] С.Уэлстид. Фракталы и вейвлеты для сжатия изображений в действии. Учебное пособ. – М.: Издательство Триумф, 2003 – 320 с.

[2] В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. Цифровая стеганография. – М.: СОЛОН-Пресс, 2002.

[3] Davern P., Scott M. Fractal based image steganography // Lecture Notes in Computer Science. 1996. Vol. 1174. P. 279-294.

УДК 004.415.24:004.056.5

ПРИХОВУВАННЯ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ У ДОКУМЕНТІ МЕТОДОМ ЗМІНИ КІЛЬКОСТІ ПРОПУСКІВ МІЖ СЛОВАМИ ВИРІВНЯНОГО ЗА ШИРИНОЮ ТЕКСТУ

Крижановська О.Л.
Кухарська Н.П., канд. фіз.-мат. наук, доцент
Львівський державний університет безпеки життєдіяльності

На сучасному етапі розвитку інформаційних систем і технологій, глобальних комп'ютерних мереж і засобів мультимедіа як ніколи є актуальною проблема передачі інформації з обмеженим доступом незахищеними каналами зв'язку. При цьому необхідним є виконання такої вимоги: інформація, яка передається від одного абонента іншому, не має стати доступною третій особі. Для розв'язання сформульованої задачі інформаційної безпеки недостатньо зробити інформацію недоступною для порушника; часто треба приховати сам факт її передачі чи зберігання. Цим і займається наука стеганографія.

Розглянемо процедуру стеганографічного приховування інформації у текстовому файлі методом зміни кількості пропусків між словами. Згідно цього методу конфіденційна інформація вбудовується у відкритий текст шляхом вкраплення додаткових символів пропуску, місцезнаходження яких визначається на основі алгоритму [1], який нагадує алгоритм манчестерського кодування.

Розглянемо суть методу на нижче наведеному прикладі.

Фрагмент порожнього текстового контейнера подано на рис. 1. Приховуване повідомлення – "життя". Стеганографічний захист конфіденційної інформації передбачає розгляд ASCII-кодів символів конфіденційного повідомлення у двійковому їх представленні. Тоді текст приховується окремими бітами.

```
Хвиля радісно плюскоче та й леститься до човна, мов
дитя, цікава, шепче і розпитує вона: "Хто ти, човне?
Що шукаєш? Відки і куди пливеш? І за чим туди шукаєш?
Що пробув? Чого ще ждеш? І повзе лінивоо човен, і вор-
коче, і бурчить: "Відки взявся я - не знаю; чим прийде-
ться закінчить. Біг мій вічний - тож не знаю. Хвиля но-
сить, буря рве, скали грозять, надять-просять к собі
берегим мене. Хвилі - то життя, то гріб мій, пестощі і
смерть моя; понад власним гробом вічно ховзаюсь три-
вожно я. Поки лиш живу правдиво, поки гріб той підо
мнов: Вітер гонить, хвиля ломить - і я вже на дно пішов.
Що ж тут думать, що тужити, що питатися про ціль! Нині
жити, завтра гнити, нині страх, а завтра біль. Кажуть,
що природа - мати нас держить, як їм там тре, а в кінці
мене цілого знов до себе відбере.
```

Рис. 1. *Фрагмент порожнього (до вбудовування) текстового контейнера*

Згідно алгоритму методу зміни кількості пропусків між словами визначається рядок текстового контейнера, що має найбільшу кількість символів. У нашому випадку це 11-ий рядок. До нього дані не вбудовуватимуться. До всіх інших рядків (назвемо їх короткими) між словами додаватиметься така кількість пропусків, щоб на виході отримати текст вирівняний за шириною.

Процедура вбудовування кожного біту даних конфіденційного повідомлення до текстового контейнера передбачає виокремлення у коротких рядках пар пропусків, якими відділяються слова. Додатковий пропуск додається на початок або в кінець слова, в залежності від значення приховуваного біту: після першого пропуску, якщо приховується біт із значенням 1 або після другого, якщо біт, який слід приховати, дорівнює 0.

Фрагмент результату вбудовування з використанням розробленої MathCad-програми повідомлення до текстового контейнера наведено на рис. 2. У даному фрагменті приховано 24 біти повідомлення, що відповідає його першим трьом символам ("жит"). Так, у 1-му рядку приховано біти 011, у 2-му – 001, у 3-му –110 (маємо символ "ж"), у 4-му – 001,у 5-му – 0, у 6-му – 1, у 7-му – 11 (маємо символ "и"), у 8-му – 010 у 9-му – 01, у 10-му – 111 (маємо символ "т").

***Рис. 2**. Фрагмент тексту заповненого методом зміни кількості пропусків між словами вирівняного за шириною (кожна тріада пропусків позначених приховує нульовий біт повідомлення, а тріада пропусків позначених – одиничний біт)*

Пропускна здатність цієї стеганосистеми – 0,8%.

Розглянутий метод є ефективним за умови, що текст представлено у форматі ASCII. Деякі приховані дані можуть виявитися втраченими після роздрукування тексту.

Література

1. Bender W. Techniques for Data Hiding / Bender W., GruhlD., MorimotoN., Lu A. // IBM Systems Journal. – 1996. –№ 35. – PP. 313-336.

2. Конахович Г.Ф. Компьютерная стеганография. Теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. – К. : Изд-во "МК-Пресс", 2006. – 288 с.

УДК 681.3.06

ЗАСТОСУВАННЯ АЛГОРИТМУ КОЛОНІЇ МУРАХ ДЛЯ КРИПТОАНАЛІЗУ ШИФРІВ ПЕРЕСТАНОВКИ

Куровець Б.І.
Гриник Р.О.
Львівський державний університет безпеки життєдіяльності

В останні роки інтенсивно розвивається новий науковий напрям який використовує математичні методи які містять принципи природних механізмів прийняття рішення, даний напрям називають «Природні обчислення». Напрям об'єднює в собі такі розділи як еволюційні алгоритми, обчислення з допомогою нейронних мереж, алгоритми ройового інтелекту та алгоритм мурашиних колоній. В [1,2] розглядаються методи атак на традиційні симетричні алгоритми з використанням інтелектуальних систем побудованих на еволюційних алгоритмах оптимізації.

Основною ознакою класу шифрів перестановки є те що символи відкритого тексту при шифруванні тільки міняються місцями між собою за певним правилом. У загальному випадку результатом роботи таких шифрів є криптограма котра містить тільки ті символи котрі містяться у відкритому тексті тільки у зміненому порядку. З цього випливає, що задача крипто аналізу полягає у визначенні позиції для призначення символів криптограми таким чином, щоб цільова функція, яка визначає оптимальність вихідного повідомлення, досягла свого екстремуму. Тобто дана задача зводиться до часткового випадку «Задачі про призначення», яка є однією з базових задач комбінаторної оптимізації і полягає в знаходженні парування мінімальної (або максимальної) ваги між елементами двох скінчених множин. Вона може бути подана як знаходження парування у зваженому дводольному графі [3]. Задачу про призначення можна сформулювати наступним чином: присвоємо $X_{ij} = 1$, якщо об'єкт *i* призначений в пункт *j*, і $X_{ij} = 0$ в іншому випадку, C_{ij} – витрати на передачу обсягу ресурсів з пункту *i* в пункт *j*. В цьому випадку модель оптимызації буде мати наступний вигляд:

$$R_{i=1}^{n} = \sum_{j=1}^{n} \sum C_{ij} X_{ij} \rightarrow \text{екстр},$$

де *n* – число об'єктів та місць їх розташування.

Якщо застосувати дану модель до задачі криптоаналізу потокового шифру, то необхідно вважати, що C_{ij} – ймовірність того, що за символом в позиції *i* повинен слідувати символ в позиції *i+1*, крім цього необхідно ввести параметр Q_i, який буде відповідати за осмисленість тексту. В такому випадку наша оптимізаційна модель буде мати наступний вигляд:

$$R = \sum_{i=1}^{n} \sum_{j=1}^{n} Q_i C_{ij} X_{ij} \rightarrow max.$$

Таким чином, загальне значення цільової функції *R*, отримане в кожному конкретному варіанті призначення символів в позиції, може бути визначено як довжина маршруту котрий з'єднує вибрані елементи, тобто:

$$R = \sum_{\substack{i=1,\dots,n-1 \\ j=2,\dots,n}} C_{ij}.$$

Очевидно, маршруту з великим значенням *R* повинна відповідати більш висока концентрація феромону *F*, яка використовується в якості ймовірності вибору чергового маршруту та представляє черговий варіант призначення позиції для символу.

Задача криптоаналізу буде вирішуватись у шість етапів:

1. Випадковим чином обирається задана кількість *m* варіантів маршрутів і обчислюються значення фітнес-функцій $R_1, R_2, \dots, R_m$.
2. Комбінаціям ik_1 розміщення символів *k* присвоюють ваговий коефіцієнт.
3. Для кожної комбінації ik обчислюється концентрація феромону F_{ik}.
4. Проводиться імітація випаровування феромону з комбінацій *ik* по яким пройшли мурахи.
5. Після визначення нової кількості феромону виконується повернення мурах в початкові позиції і визначається ймовірність розміщення символу *k* в позиції *i* у новому маршруті P_{ik}.
6. У відповідності з P_{ik} формується $d * m$ нових маршрутів $(d < 1)$, для котрих обчислюється значення фітнес-функцій, після чого проводиться вибірка із *m* кращих варіантів. Якщо оптимальне значення фітнес-функції не змінюється протягом декількох ітерацій то пошук маршруту закінчується, в іншому випадку довжина маршруту обнулюється і проводиться повернення до другого кроку.

З вище сказаного можна зробити висновок, що комбінування алгоритму мурашиних колоній з алгоритмом вирішення задачі про призначення може істотно підвищити ефективність та швидкість вирішення задачі по крипто аналізу шифрів перестанови.

Література

1. Сергеев А.С. Исследование возможности организации криптографической атаки с использованием эволюционной оптимизации и квантового поиска при разработке систем передачи и защиты информации / А.С. Сергеев // Теоретические и прикладные вопросы современных информационных технологий: материалы 6-й всерос. науч.-техн. конф. – Улан-Удэ: Изд-во ВСГТУ, 2005. – С.61-65.

2. Сергеев А.С. Применение методов генетического поиска для организации криптоанализа блочных криптосистем на примере стандарта шифрования DES / Сергеев А.С. // Научная мысль Кавказа. Прил. – Ростов н/Д: Изд-во СКНЦ ВШ. – 2006. – №15. – С.185-193.

3. Задача про призначення [Електронний ресурс]. Режим доступу: https://uk.wikipedia.org/wiki/ Задача_про_призначення

УДК 004.056.5

РЕАЛІЗАЦІЯ ПРОТОКОЛІВ ЦИФРОВОГО ПІДПИСУ НА ЕЛІПТИЧНИХ КРИВИХ

Лавренюк Ю.Ю.
Лагун А.Е., канд. техн. наук, доцент
Львівський державний університет безпеки життєдіяльності

Сучасний світ характеризується тенденцією постійного підвищення ролі інформації, яка має усе більш вагоме значення у функціонуванні державних і суспільних інститутів в житті кожної людини. Інформатизація веде до створення єдиного світового інформаційного простору. Сьогодні багато людей спілкуються не особисто, а використовуючи комп'ютерну мережу. Для тих саме речей, які люди роблять не замислюючись, комп'ютерам потрібні протоколи.

Протокол – це послідовність дій, які роблять дві або більше сторін, призначена для виконання певного завдання [2]. Протоколи дають змогу абстрагуватися під час розв'язання задачі від способу розв'язування.

Часто виникає питання, як головний комп'ютер дізнається, що до нього під'єднався саме той користувач, що потрібно, а не зловмисник. Зазвичай цю проблему вирішують за допомогою паролів. Цілком достатньо, щоб головний комп'ютер міг відрізняти правильні паролі від неправильних, а саме виконував задачу аутентифікації.

Цю задачу можна вирішити за допомогою криптографічних методів захисту інформації, зокрема, використовуючи відкриті та закриті ключі і односпрямовані функції.

Односпрямованою називається функція $F(x)$: $X \to Y$, $x \in X$, яка має дві властивості [1]:

– існує поліномний алгоритм обчислення значень $y = F(x)$;

– не існує поліномного алгоритму інвертування функції $F(x) = y$.

Спрощений протокол аутентифікації користувача за допомогою односпрямованих функцій має вигляд:

1) користувач надсилає головному комп'ютеру свій пароль;
2) головний комп'ютер обчислює односпрямовану функцію пароля;
3) головний комп'ютер порівнює одержане значення з тим, що зберігається і, за умови співпадіння, надає доступ до інформації.

При використанні наведеного протоколу виникають серйозні проблеми з безпекою. Наприклад, коли користувач надіслав свій пароль головному ком'ютеру, то кожен, хто має доступ до шляху передавання його даних, зможе прочитати даний пароль.

Криптографія з відкритим ключем може легко вирішити таку проблему [2]:

1) головний комп'ютер відсилає до користувача випадковий рядок;
2) користувач шифрує цей рядок своїм закритим ключем і відсилає його назад разом зі своїм ім'ям;
3) головний комп'ютер знаходить в базі даних відкритий ключ користувача і розшифровує повідомлення;
4) якщо відісланий спочатку і розшифрований рядки збігаються, то головний комп'ютер надає користувачу доступ до системи.

В криптографії з відкритим ключем ефективно використовується математичний апарат на основі еліптичних кривих.

При використанні алгоритмів на еліптичних кривих вважається, що не існує субекспонентних алгоритмів для розв'язання задачі дискретного логарифмування в групах їх точок. При цьому порядок групи точок еліптичної кривої визначає складність завдання. Однією з проблем криптографічного застосування еліптичних кривих є вибір надійної випадкової кривої.

В роботі було досліджено протокол аутентифікації користувача, що використовує еліптичні криві. В протоколі використано двох учасників **A** і **B**, яким відома спільна еліптична крива $E_p(a,b)$ і генеруюча точка G. Протокол має вигляд:

1) учасник **A** відсилає до **B** випадковий рядок M;

2) учасник **B** шифрує даний рядок своїм закритим ключем k, проводячи обчислення: $R = k \cdot G$ (додати точку G k разів); $P = k \cdot R = (x, y)$; шифротекст $C = (Mx) \bmod p$;

3) учасник **B** відправляє до **A** трійку (R, C, <ім'я_B>);

4) знаючи R і генеруючу точку G, учасник **A**: обчислює k'; за допомогою <ім'я_B> знаходить відомий відкритий ключ **B** – Y і обчислює $Q = k' \cdot Y = (x', y')$; розшифровує шифротекст $M' = (Cx') \bmod p$.

5) якщо M і M' збігаються, то учасника протоколу **B** ідентифіковано.

Стійкість наведеного протоколу повністю визначається складністю задачі дискретного логарифмування на еліптичних кривих.

В подальших дослідженнях планується реалізувати наведений протокол аутентифікації з використанням різних еліптичних кривих і визначити оптимальні параметри кривої для забезпечення необхідної криптографічної стійкості.

Література

[1] Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке Си / Б. Шнайер. – М.: Триумф, 2002. – 816 с.

[2] Лагун А.Е. Криптографічні системи та протоколи // Навч. посібник. – Львів : Вид-во Львівської політехніки, 2013. – 96 с.

УДК 004.056.53

АНАЛІЗ СУЧАСНИХ КОМПЛЕКСНИХ СИСТЕМ САНКЦІОНОВАНОГО ДОСТУПУ ДЛЯ ПІДПРИЄМСТВА

Лукіянюк Я.В.
Мандрона М.М. канд. техн. наук
Львівський державний університет безпеки життєдіяльності

На сьогоднішній день актуальним питанням є безпека підприємств, створення їх систем захисту від несанкціонованого доступу та контролю за працівниками. Це зумовлено тим, що сучасні інформаційні та комп'ютерні технології, засоби несанкціонованого доступу до інформації, засоби електронного обміну та засоби захисту інформації – стрімко розвиваються. Внаслідок цього постійно вдосконалюються вже існуючі та з'являються нові організаційні, програмні та технічні способи, які б допомогли побудові комплексних систем санкціонованого доступу та в захисті інформації загалом.

Для розв'язання завдань комплексної безпеки підприємства найефективнішим методом є використання комплексних систем санкціонованого доступу (КССД).

Санкціонований доступ на підприємстві переважно створюється для захисту від антропогенних джерел загроз, якими являються суб'єкти, дії яких можуть бути кваліфіковані як навмисні або випадкові злочини.

Системи санкціонованого доступу використовуються для вирішення таких завдань, як розмежування прав доступу в приміщення, облік робочого часу та моніторинг місцезнаходження працівників [1]. Їх класифікацію наведено на рис. 1.

Сучасна система управління і контролю санкціонованим доступом повинна [2]:

- забезпечувати контроль доступу та управління ним на різних типах контрольно-пропускних пунктів (людських, автомобільних, залізничних);
- унеможливити перевезення заборонених предметів (зброї, вибухових речовин, матеріалів і т. п.);
- перешкодити проникнення потенційних порушників;
- для покращення ефективності систему потрібно оснащувати багаторівневими видами ідентифікації осіб (парольна, біометрична, магнітні картки, кодова;
- володіти високими адаптивними властивостями;
- забезпечувати автоматизацію процесів управління службами безпеки об'єкта та координацію їх діяльності;
- функціонувати в умовах ураження компонентів системи і в інших надзвичайних ситуаціях.

Рис. 1. *Класифікація систем санкціонованого доступу*

Види ідентифікаторів, що використовуються для КССД [1]:

– *механічний* – використання елементів конструкції у приміщенні (елементи механічних ключів, турнікети);
– *магнітний* – використання намагнічених ділянок поверхні (магнітні катки та картки Віганда);
– *оптичний* – використання різноманітного маркування ідентифікатора, які мають різні оптичні характеристики (голографічні мітки чи картки з штрих-кодом);
– *біометричний* – використання фізіологічних характеристик людини (відбитки пальців, колір очей, геометрія руки, сітківка ока, тощо);
– *комбінований* – вид ідентифікації, який побудовано на основі декількох методів ідентифікації одночасно.

Грамотне створення та коректна експлуатація КССД на підприємстві дає змогу вберегти його від несанкціонованого доступу на територію, у будівлю організації та окремі кабінети. В той час експлуатація системи не стає завадою для повноцінної роботи персоналу, не перешкоджаючи їхньому доступу на підприємство.

Література

1. Гарасимчук О.І. Комплексні системи санкціонованого доступу: навч. посібник / Гарасимчук О.І., Дудикевич В.Б., Ромака В.А. – Львів : Вид-во НУ «Львівська політехніка», 2010. – 212 с.

2. Системи контролю та управління доступом. [Електронний ресурс]. – Доступно з: http://sheriff.com.ua/uk/uslugi_ua/sistemi-kontrolia-dostupa-2.

УДК 514.18

ПРАКТИЧНЕ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ЗАХИСТІ ЛЮДСЬКОГО ЖИТТЯ

Луцук С.М.
Кузиляк В.Й.
Львівський державний університет безпеки життєдіяльності

Рішення сучасних проблем управління суспільством безпосередньо пов'язане з розвитком інформаційних технологій.

Інформаційні технології – це сукупність програмних, технічних засобів які утворюють ланцюжок по збереженню, обробці та передаванню інформації, за допомогою якого, людина може скористатися будь-яким доступним ресурсом інформації.

Безпека життєдіяльності – це дисципліна спрямована на ознайомлення з знаннями пов'язаними з вирішенням проблем, побутового, виробничого, природного та техногенного походження.

Інформаційні технології, увірвалися в наше життя в середині минулого століття, і з того часу, вони не тільки розвинулись, вдосконалились та порозумнішали, вони стали ефективнішими. Вони проникли у всі види нашої діяльності, максимально при цьому захищаючи людину від шкідливого, на неї, впливу.

Щодня люди створюють різні технології, як програмного так і технічного захисту людини. Це починаючи з антивірусних програм, для захисту банківських рахунків та персональної інформації і до екзоскелетів, що дозволяють переносити набагато тяжчі речі, з мінімальними силовими затратами (впровадження розпочалося в Іспанії; призначений в першу чергу для пожежників). Завдяки інформаційним технологіям служби призначені для захисту життя людини мають в своєму арсеналі пристрої миттєвої передачі інформації, планування, та захисту. Це починаючи від навігаційних пристроїв, сигналізації, до приладів, які допомагають визначати склад речовини, і вплив їх на людину.

Вивчення інформаційних знань в сфері життєдіяльності має свої особливості. Інформаційні технології, невпинно розвиваються і в людей з'являються нові прилади захисту. Давно відома пожежна сигналізація, помалу відходить в історію, на ринку набирає популярності програмне забезпечення «Розумний дім», що представляє собою централізоване керування всіма електроприладами, та вузлами забезпечення дому з одного місця, одним користувачем. У випадку виникнення пожежі, система, відповідно реагує, автоматично набираючи найближчу пожежну службу, та перекриваючи подачу струму в палаюче приміщення. Це і ще багато інших корисних функції виконує комп'ютерна автоматизована система. Також інформаційні технології здатні слідкувати за станом власного здоров'я в реальному часі. Компанія Samsung та інші відомі бренди електроніки, давно здіяними бурю на ринку електроніки,

представивши свій комп'ютеризований годинник, що має функції не просто рахувати калорії та кроки, а ще повідомляти користувача про зміни його фізіологічних властивостей(тиск, серцебиття, та ін.), а також викличе вам швидку при втраті свідомості чи у критичній ситуації.

Вже зараз робляться прогнози про майбутні технології які врятують людині життя, чи допоможуть в критичній ситуації. І це стануть: 1) машини на автопілоті; 2) створення штучного інтелекту; 3)повна автоматизація промисловості та сільського господарства; 4) створення нових ліків; 5) подолання проблем забруднення, та ще багато іншого. Але, як скоро ми зможемо користуватися цими благами інформаційних технологій, залежить лише від нас.

Література

1. Грицунов О. В. Інформаційні системи та технології: навч. посіб. для студентів за напрямом підготовки «Транспортнітехнології» / О. В. Грицунов; Харк. нац. акад. міськ. госп-ва. – Х.: ХНАМГ, 2010. – 222 с.

2. Зеркалов Д.В. Безпека життєдіяльності. Навч. посіб. – К.: Основа, 2011. – 526 с.

3. Безпека життєдіяльності: Навчальний посібник / Березуцький В.В., Васьковець Л.А., Вершиніна Н.П. та ін.; За ред. проф. В. В. Березуцького. — Х.: Факт, 2005. — 384 с.

УДК 65.012.12+504.064.3

АНАЛІЗ ПОКАЗНИКІВ ПРОГРАМ РЕІНЖИНІРИНГУ СИСТЕМИ ЛОКАЛЬНОГО МОНІТОРИНГУ ТОРФОВИЩ

Максютинський О.П.
Мартин Є. В., д-р техн. наук, професор
Львівський державний університет безпеки життєдіяльності

Управління програмами реінжинірингу систем локального моніторингу торфовищ базується на результатах прогнозування та оцінювання їх функціональних показників. Чинні методи їх визначення не можна вважати обґрунтованими, оскільки вони характеризуються великою кількістю недоліків, зокрема, некоректно враховують зону виїздів пожежних підрозділів. Отже, постає науково-практична проблема обґрунтування адекватних моделей функціонування систем щодо об'єктивного оцінювання показників їх ефективності [1] та дотримання певних заходів при улаштуванні системи:

- проведення відбору територій, а саме земельних ділянок деградованих торфовищ для їх поступового відновлення;
- пошук ефективних підходів для управління територіями, які перебувають під контролем;

– довготривалий контроль за відновленими торфовищами стане можливий тільки при постійній підтримці роботи системи моніторингу з боку місцевого населення.

Отож, необхідне створення системи моніторингу, яка дозволить продемонструвати позитивний вплив проектних заходів на скорочення викидів парникових газів, вплив відновлених територій на зменшення кількості лісових пожеж на торфовищах.

Система локального моніторингу торфовищ призначена для передачі сигналів множині пожежних частин, територіально розташованих у межах Київської області. Кожна з них має певну територіальну зону дії, яка включає велику кількість належних до її району виїзду торф'яних територій. За умови виникнення пожежі на тому чи іншому торфовищі її гасіння має виконуватися пожежним підрозділом, до зони дії якого це торфовище належить. Зони дії пожежних частин здебільшого визначаються за адміністративно-територіальним принципом. Водночас, території адміністративних районів є нерівномірними як за площею і кількістю торфовищ, так і конфігурацією та мережею доріг. Це є однією з причин значної нерівномірності рівня пожежної безпеки окремих торфовищ. Знизити цю нерівномірність можна шляхом реалізації проектів реінжинірингу систем моніторингу. Визначення пріоритетності цих проектів має базуватися на результатах оцінювання рівня пожежної безпеки, який зумовлюється функціонуванням пожежних частин.

До показників функціонування систем моніторингу торфовищ належать:

– матеріальні збитки від пожеж (*Мз*);
– кількість людей, загиблих на пожежах (*Lз*).

Ці показники є узагальненими. Вони оцінюються як стосовно окремих територіальних зон дії пожежних частин, так і адміністративних областей та держави загалом.

Означені узагальнені показники функціонування автоматичних систем локального моніторингу торфовищ є функцією таких аргументів:

$$(Мз, Lз) \leftarrow (\lambda n, t, Мо), \quad (1)$$

де λn річне число торф'яних пожеж;

t – середня тривалість горіння торфовищ;

Мо – витрати на паливно-мастильні матеріали, необхідні для локалізації пожеж на торфовищах та доставки особового складу до місця виникнення пожеж.

Проаналізуємо суть цих аргументів. Річне число пожеж на торфовищах λn переважно залежить від людського фактору через нецільове використання земель, території, які часто засмічені. Це безумовно ускладнює процес гасіння пожежі. Горіння прилеглих територій *Гпт*, розмір покладу торфу, який знаходиться на території пожежі *П*, а також рівень дотримання жителями прилеглих територій правил пожежної безпеки *Ппб* пов'язані залежністю [2]:

$$\lambda n = f\,(Гпт,\ П,\ Ппб), \qquad (2)$$

Середня тривалість горіння пожежі на торфовищі *Тг* складається із таких елементів:

$$Тг = Тп + Тд + Тр + Тга, \qquad (3)$$

де *Т* – час від моменту загоряння торфовища до отримання пожежними частинами повідомлення про пожежу, хв.;

Тп – тривалість підготовки пожежного караулу до виїзду, хв.;

Тд – тривалість перебування пожежних у дорозі, хв.;

Тр – тривалість розгортання пожежно-рятувальних підрозділів, хв.;

Тга – тривалість гасіння пожежі, хв.

Час отримання пожежною частиною інформації про виникнення пожежі залежить від багатьох чинників. Він є малокерованим у зв'язку з відсутністю системи локального моніторингу на торфовищі. Час підготовки пожежно-рятуваних підрозділів до виїзду на пожежу залежить від підготовленості пожежних рятувальників. Час перебування пожежно-рятувальних підрозділів у дорозі залежить від середньої віддалі *Lпг* між пожежною частиною і торфовищем, горіння та середньої швидкості *Vп* руху пожежно-рятувальних підрозділів на пожежу

Означені і розкриті показники функціонування системи локального моніторингу на торфовищі та з'ясовані причинно-наслідкові зв'язки між ними складають основу для прогнозування ефективності програм їх реінжинірингу.

Література

1. Пономаренко Л.А., Цюцюра С.В. Реінжиніринг та інноваційні ділові процеси в енергоємних галузях промисловості // Л.А.Пономаренко, С.В. Цюцюра / Автоматизація виробничих процесів. 2006. – №2(23). – С.11–17.

2. Суков Я. В. Дослідження параметрів запалювання і горіння торфу за допомогою фізичного та математичного моделювання./Я.В.Суков// – Лісові і степові рідини // Журнал прикладної механіки і технічної фізики.: 2010. – С.110–121с.

УДК 004.94

РОЗРОБЛЕННЯ КОМПЛЕКСУ ІНТЕРАКТИВНИХ СИМУЛЯТОРІВ РОБОТИ З ПОМПОВИМ УСТАТКУВАННЯМ СУЧАСНОГО ЗРАЗКА

Мозоль Д. Б.
Придатко О.В., канд. тех. наук
Львівський державний університет безпеки життєдіяльності

Євроінтеграційний розвиток вітчизняної освіти вимагає кардинально нової орієнтації її процесів на функціонування в умовах розвиненої економіки, де якість освітнього продукту визначатиме попит навчального закладу на ринку освітніх послуг. В цьому напрямі вже зроблено низку вагомих кроків, зокрема у попередніх дослідженнях проаналізований світовий досвід створення інноваційних технологій підготовки сучасного рятувальника, заснованих використанням сучасних інтерактивних тренажерів, групових симуляторів, імітаційних моделей тощо. Проте вони володіють одним суттєвим недоліком – це відсутність можливості інтерактивної роботи з рятувальним устаткуванням.

На вирішення цієї проблеми науковим товариством курсантів і студентів кафедри експлуатації транспортних засобів та пожежно-рятувальної техніки Львівського державного університету безпеки життєдіяльності розпочата робота над створенням комплексу інтерактивних симуляторів роботи з помповим устаткованням сучасного взірця – НВПН-40/100. У порівнянні з традиційними технологіями підготовки, використання означеного комплексу не потребує значних фінансових витрат. Лише за наявністю комп'ютера та певного програмного забезпечення, перед користувачами освітнього процесу постає змога відпрацювання практичних вправ. Інтеграція даного комплексу в будь-яке віртуальне освітнє середовище надаватиме можливість користувачам здобувати практичні уміння та навички у будь-який зручний для них час.

В рамках реалізації проекту розроблено симулятори із відпрацювання низки практичних вправ з насосом сучасного взірця, зокрема: перевірка герметичності; нагнітання води; забір та нагнітання з відкритої водойми; забір та нагнітання за допомогою гідроелеватора; забір та нагнітання з водогінної мережі. А також завершується робота над вправою "Подача повітряно-механічної піни". Для наочності робочі вікна деяких із розроблених симуляторів представлено на рисунку.

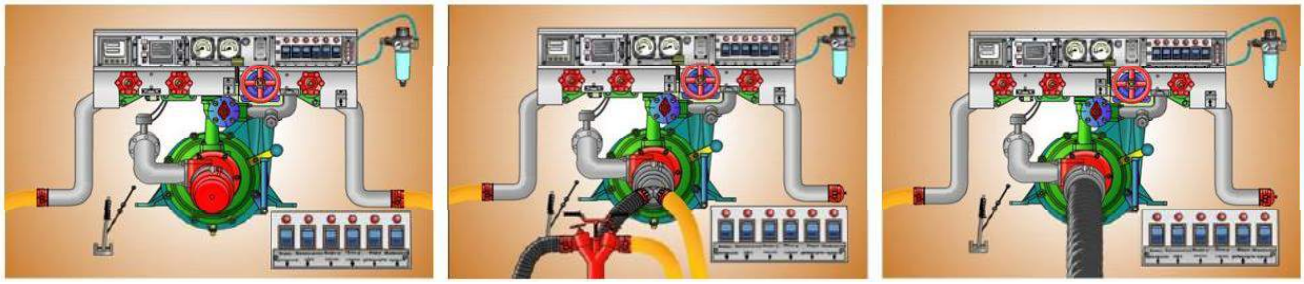

Рисунок 1 *– Робочі вікна інтерактивного симулятора по роботі з сучасним помповим устаткуванням*

Отже, як показує світовий досвід, в процесі глобальної інформатизації процесів навчання розроблення сучасних засобів тренування майбутніх рятувальників є одним із перспективних напрямків розвитку освітнього середовища. Наближаючись до світових тенденцій нами також зроблено низку кроків у заданому напрямі, зокрема завершується розроблення комплексу оновлених інтерактивних комп'ютерних симуляторів роботи із сучасних насосним устаткуванням протипожежних автомобілів. Перспективою подальшої роботи є дослідження їх інтеграційних процесів в освітній простір та визначення ефективності за різних умов і методів використання.

Література

1. Рак Ю. П. Пути усовершенствования профессиональной подготовки специалистов подразделений МЧС с использованием информационно-телекоммуникационных технологий / Ю. П. Рак, О. Б. Зачко, Т. Є. Рак // Управляющие системы и машины : Междунар. науч. журнал. – К. : ІК ім. В. М. Глушкова НАН України, 2011. – № 4. – С. 37-43.

2. Ренкас А. Г. Інноваційні технології управління якістю в проектах підготовки рятувальників / А. Г. Ренкас, О. В. Придатко, Д. Б. Мозоль, Т. П. Гангур // Вісник ЛДУБЖД: Зб. наук. праць. Львів: ЛДУ БЖД, 2015. – №11. – С.80-88.

УДК 004.056.5

АНАЛІЗ ЦІЛЕЙ АТАК НА МЕРЕЖІ МОБІЛЬНОГО ЗВ'ЯЗКУ СТАНДАРТУ LTE З ІНТЕГРОВАНИМИ ФЕМТОСОТАМИ

Нікітенко К.О.

Кухарська Н.П., канд. фіз.-мат. наук, доцент

Львівський державний університет безпеки життєдіяльності

Ринок мобільного зв'язку на даний час перебуває у стані радикальних змін, зумовлених стрімким ростом попиту з боку абонентів на комплексні мультимедійні послуги. На сьогоднішній день мільйони пристроїв підключені до Інтернету і хмарних технологій з використанням 4G і LTE мереж рухомого радіотелефонного зв'язку. Проте з високим рівнем урбанізації стільниковий зв'язок у певних точках не може задовольнити всіх потреб користувача. У зв'язку з цим постає питання про надання якісного каналу зв'язку в будь-якому місці. Одним з ефективних варіантів вирішення цієї проблеми є використання інтегрованих фемтосот (ІФ) для створення локальної мережі передачі даних в межах приміщення – інноваційної технології поліпшення якості зв'язку, що використовує у ролі транспорту протокол IP. У зв'язку з цим, забезпечення конфіденційності, цілісності та доступності циркулюючої в фемтосотах інформації, є одним з найбільш важливих аспектів для користувачів пристроїв з підтримкою стільникових систем мобільного зв'язку (ССМЗ) нового покоління.

При проведенні атак на стільникові мережі характерна така послідовність дій [1]:

1. вивчення мережі і її зони покриття;
2. планування методики огляду місця розгортання і проведення атаки;
3. збір, підготовка та конфігурація обладнання та програмного забезпечення, необхідних для виконання запланованих дій;
4. огляд місця розгортання мережі, визначення її кордонів і рівня сигналу уздовж периметра;
5. аналіз трафіку в мережі і подолання виявлених заходів протидії;
6. підключення до мережі та аналіз її структури;
7. пасивний аналіз трафіку від хостів і оцінка безпеки протоколів, використовуваних в мережі;
8. проведення активних атак проти абонентів, що представляють інтерес.

Розглянемо основні цілі атак як джерела загрози інформаційної безпеки ССМЗ стандарту LTE з ІФ. На рис. 1 стрілками позначені три вразливі елементи: (а) повітряний інтерфейс між мобільним пристроєм (UE) і фемтостільниковою базовою станцією (БС); (Б) безпосередньо фемтостільникова базова станція (БС) (H(e)NB); (В) широкосмугове з'єднання між фемтосотою і шлюзом безпеки (SecGW).

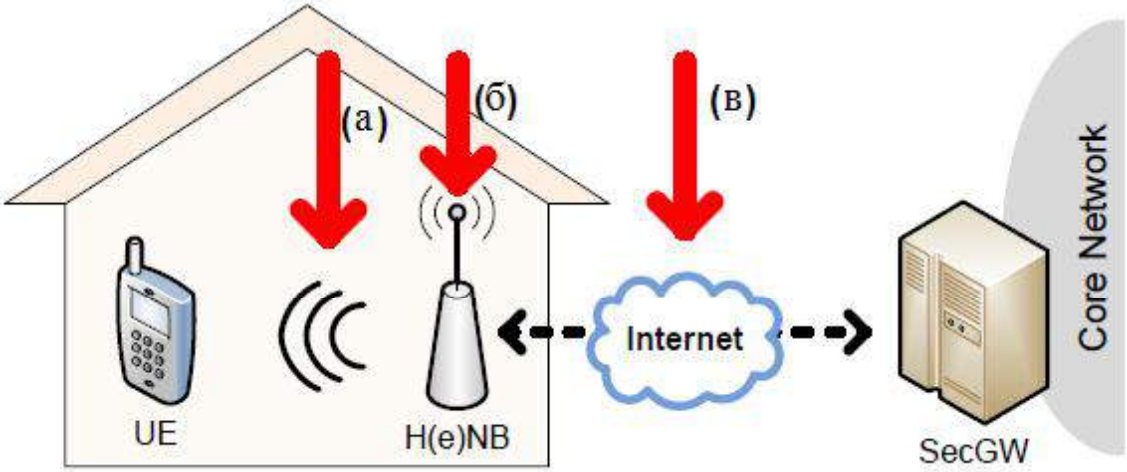

Рис. 1. *Цілі атак зловмисників на стільникові мережі з ІФ*

Атаки на повітряний інтерфейс. У пасивному варіанті зловмисник прослуховує канал зв'язку між мобільним пристроєм і базовою станцією; в активному – на додачу до прослуховування, зловмисник здійснює несанкціонований вплив на вже циркулюючий трафік. Щоправда, можливості активних атак істотно знижені за рахунок застосування криптографічного захисту інформації, яка передається. Позаяк, пасивні атаки, такі як аналіз трафіку і відстеження місця розташування користувачів, все ще можливі [2].

Атаки на фемтостільникові базові станції. З точки зору зловмисника фемтосоти відкривають нові можливості для реалізації деструктивних впливів. Наприклад, зловмисникові набагато легше отримати доступ до фемтосоти розташованої в

приміщенні, ніж до БС розташованої на даху. Фізичний розмір, якість матеріалів, більш дешеві компоненти і IP-інтерфейс фемтосоти роблять її більш вразливою для атак зворотного проектування і несанкціонованого доступу, в порівнянні з традиційними, дорожчими і висококласними БС. Оскільки шифрування даних користувача, що транслюються через ефір, припиняється на рівні фемтосоти, апаратне втручання в пристрій дає змогу розкрити конфіденційну інформацію користувача, який нічого не запідозрить. Наприклад, якщо зловмисник деактивує систему Closed Subscriber Group (CSG) і тим самим змусить фемтосоти приймати всіх зовнішніх користувачів без необхідності попередньої реєстрації, то він отримає можливість несанкціоновано аналізувати їх трафік. Крім того, атаки на кшталт підміна довіреного об'єкта, атаки на мережеві служби з використанням протоколів Інтернет, атаки-повідомлення помилкового позиціонування або атаки несанкціонованої переконфігурації радіоапаратури ускладнюють оператору мобільного зв'язку процес управління інтерференцією і засобами контролю живлення, що несприятливо позначиться на якості обслуговування [3].

Атаки на опорну широкосмугову мережу. Витік інформації про точку доступу ядра мережі в мережу Інтернет має серйозні наслідки: це провокує велику кількість мережевих атак на операторів стільникового мережі мобільного зв'язку, таких як відмова в обслуговуванні (DoS) або підміна довіреного об'єкта.

Література

1. Елисеев Н. Фемтосоты в мобильной связи – преимущества и решения [Электронный ресурс] / Н. Елисеев // Первая миля. Выпуск #2/2007. – Режим доступа : http://www.lastmile.su/journal/article/2154.

2. Borgaonkar R., Redon K., and J. Seifert. Security analysis of a femtocell device. In Proceedings of the 4th international conference on Security of information and networks, SIN ’11, ACM, 2011. – pp. 95–102.

3. Shwetha H.K, Prof. D. Jayaramaiah Study and Analysis of Security Issues in Next Generation Mobile Network // International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 3, Issue 4, Jul-Aug 2013. – pp. 942-946.

УДК 004.056

РОЗРОБЛЕННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ, ЩО ОЗВУЧУЄТЬСЯ

Панасюк А.В.
Мандрона М.М., канд. техн. наук
Львівський державний університет безпеки життєдіяльності

У сучасному світі найбільше цінується інформація, адже хто володіє інформацією, той володіє світом. Завжди існує ризик, що будь-яка цінна інформація може бути викрадена. Найновітніші технології дозволяють зробити це навіть на великій відстані без прикладання великих зусиль. Тому інформація повинна бути захищена, як на законодавчому рівні, так і від витоків технічними каналами та іншими способами.

Проаналізувавши нормативно-правову базу України можна зробити висновок, що вона є досить розвиненою і насиченою. В цій базі є досить багато законів, актів, указів Президента, постанов, розпоряджень, державних стандартів, – які в свою чергу передбачають обґрунтовані покарання.

Інформація з обмеженим доступом – інформація, доступ до якої має обмежене коло осіб і розповсюдження, якої заборонено розпорядником інформації [1].

Основними каналами витоку інформації з обмеженим доступом, що озвучується є: акустичний, віброакустичний, лазерно-акустичний, акустоелектричний, параметричний, оптичний.

Відповідно до чинного законодавства інформація з обмеженим доступом повинна озвучуватися у виділеному приміщенні, тобто спеціальному приміщені призначеному для проведення нарад. Основними заходами під час таких нарад є захист від витоків каналами через, які може бути витік інформації, що озвучується, а також захист від несанкціонованого доступу.

Для захисту інформації з обмеженим доступом на об'єкті інформаційної діяльності має бути створено комплекс технічного захисту інформації (КТЗІ). Створюється такий комплекс у декілька етапів [2]:

- визначення вищого ступеня обмеження доступу до інформації;
- формування наказу про проведення робіт з атестації ОІД та комісії з обстеження;
- проведення категоріювання та обстеження ОІД;
- розроблення моделі загроз для ІзОД, що буде оброблятися на ОІД.

Розроблення та впровадження заходів із захисту:

- розроблення технічного завдання на створення КТЗІ;
- визначення виконавців робіт ТЗІ;
- розроблення кошторису робіт та придбання засобів ТЗІ;
- впровадження на ОІД інженерних та технічних заходів в ТЗІ.

Випробування комплексу ТЗІ:

- затвердження програм та методик випробувань;
- проведення випробувань підготовка протоколів;
- підготовка та затвердження висновків випробувань;
- проведення атестації КТЗІ;
- заповнення паспорта та введення(подовження) в експлуатацію ОІД наказом.

Брати участь у таких нарадах можуть лише, ті хто мають відповідний допуск до тих документів чи інформації, яка буде озвучуватися залежно від грифу таємності документа. Відповідний допуск може надати лише СБУ.

Для захисту інформації з обмеженим доступом, що озвучується усі прилади повинні бути сертифікованими та мати відповідну ліцензію. У табл. 1 наведено короткий перелік сертифікованих приладів та від якого каналу витоку інформації вони захищають. Більше інформації щодо використання приладів можна отримати на офіційній сторінці Державної служби спеціального зв'язку та захисту інформації України [3]. Використання будь-яких приладів і систем не сертифікованих і без відповідних ліцензій вважається незаконним і карається як штрафами, так і кримінальною відповідальністю.

Таблиця 1

Перелік пристроїв призначених для захисту акустичної інформації

Канал витоку інформації	**Пристрій призначений для захисту**
Акустичний	Генератор шумових сигналів «МАРС-ТЗО-4-2»
Віброакустичний	Прилад віброакустичного захисту інформації «ОЦЗІ-ВА»
Лазерно-акустичний	Вібровипромінювач «ВИЗ»
Акустоелектричний	Колонка акустична захищена «МАРС-АКЗ»
Параметричний	Трансформатори розділові з екраною обмоткою «РІАС-4ТР/5»
Оптичний	Комплекс автоматизований радіомоніторингу і пошуку закладних пристроїв АКОР-3

Література

1. Закон України «Про інформацію». [Електронний ресурс]. Доступно з: http://zakon5.rada.gov.ua/laws/show.

2. НД ТЗІ 1.1-005-07 «Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення».

3. Перелік засобів технічного захисту інформації, дозволених для забезпечення технічного захисту державних інформаційних рисунків та інформації, вимога щодо захисту якої встановлена законом. [Електронний ресурс]. Доступно з: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=234237&cat_id=39181.

УДК 34.096

БАТЬКІВСЬКИЙ КОНТРОЛЬ ЯК СКЛАДОВА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЛЮДИНИ

Пилипенко В.М.
Гриник Р.О.
Львівський державний університет безпеки життєдіяльності

На сьогоднішній день під поняттям «Батьківський контроль» розуміють не тільки прямий контроль батьків за життєдіяльністю дитини, а й використання відповідного програмного забезпечення призначеного забезпечити захист дитини від негативного впливу використання аморальних або таких, що негативно впливають на опікувану особистість, інтернет-ресурсів, комп`ютерних ігор, прикладних програм і т.п. Для якісного функціонування даного програмного забезпечення необхідно виконати цілий ряд організаційних завдань по налаштуванню програмного забезпечення. Основне завдання даного програмного забезпечення зробити неможливим відвідування різних неприйнятних інтернет-ресурсів, які можуть зашкодити користувачу, а також для того, щоб обмежити час роботи за персональним комп'ютером. Зазвичай під користувачем розуміється дитина, однак обмеження може використовуватися стосовно будь-якого іншого користувача незалежно від віку для контролю відвідуваності сайтів і використання локальних функцій комп'ютера. Батьківський контроль допомагає наглядати за тим з якою метою діти використовують комп'ютер та які інтернет-ресурси відвідують. Коли функція батьківського контролю блокує доступ до гри, програми чи інтернет-ресурсу, на екрані висвітлюється відповідне повідомлення . Доступ можна надати, ввівши відомості батьківського облікового запису.

Існує активний і пасивний контроль. Пасивний «батьківський контроль» передбачає обмеження часу користування персональним комп'ютером. Наприклад, у будні ви можете виставити час з 16:00 до 18:00, а у вихідні та святкові дні - з 13:00 до 18:00. Таким чином, тільки в цей час користувач буде мати доступ до комп'ютера. Крім того, пасивний «батьківський контроль» на комп'ютері дозволяє обмежити доступ до певного програмного забезпечення. Крім усього перерахованого, адміністратор комп'ютера може встановити обмеження і на використання комп'ютерних ігор, що в наш час є дуже актуальним. Наприклад, певна комп'ютерна гра чи прикладна програма може знаходитись в активному режимі не більше трьох годин на день. Пасивний метод захисту також передбачає заборону відвідування певних інтернет-ресурсів[1].

Завдання активного «батьківського контролю» полягає в тому, щоб в реальному часі відстежувати всі дії дитини. Для реалізації такого підходу необхідно встановити відповідне програмне забезпечення. Користувач даного програмного забезпечення буде мати змогу контролювати потік файлів на персональному комп'ютері, а також відстежувати листування по електронній пошті та весь трафік. Все це дозволяє переконатися в тому, що «батьківський конт-

роль» на комп'ютері дійсно працює і є потужним захистом для вашого комп'ютера. Розглянемо кілька способів обмеження доступу до певних ресурсів комп'ютера та Інтернету. Найбільш актуальний спосіб це автоматичне створення бази даних інтернет-ресурсів, з якою буде працювати утиліта. Програмне забезпечення відстежує потоки інформації та формує базу заборонених для доступу сайтів, при необхідності користувач (адміністратор) має можливість внести небажані інтернет-ресурси в базу самотужки. Існує ще один спосіб, за допомогою нього користувач створюєте свій «білий список», тобто список ресурсів до яких дозволяється доступ з даного персонального комп'ютера, все що не входить до даного списку автоматично блокується. Перевага способу в тому, що не потрібно закривати «сайти для дорослих», працювати з базою даних і т.п. Створити базу даних, яка містить всі корисні сайти, досить складно, тому використання такого комп'ютера обмежує користувача не тільки переглядом заборонених сайтів, але й сайтів, які б принесли користь для нього. Слід зазначити, що «батьківський контроль» такого роду досить ефективний.

На сьогоднішній день є достатня кількість програм за допомогою яких можна встановити батьківський контроль. Наприклад, програма під назвою Crawler Parental Control, дане програмне забезпечення є безкоштовним, тому кожен користувач може завантажити і встановити його на свій ПК.

Дана програма передбачає п'ять рівнів обмежень по доступу до персонального комп'ютера, програмного забезпечення та інтернет-ресурсів . Перший рівень орієнтований на дітей молодше 10 років та передбачає роботу з персональним комп'ютером кілька годин в день, також даний рівень контролю блокує «сайти для дорослих», нецензурну лексику та інші шкідливі ресурси. Другий і третій рівень дозволяють користуватися персональним комп'ютером більш тривалий час, але блокує доступ до перегляду «сайтів для дорослих», а також до іншого шкідливого контенту. На четвертому етапі повністю зникають системні обмеження, комп'ютером можна користуватися досить довгий період часу, але не вночі, доступ до «сайтів для дорослих» також заборонений. П'ятий рівень практично марний, оскільки він тільки забороняє користуватися персональним комп'ютером у нічний час доби. Також дана програма має таку функцію як електронний звіт «Spy Mode», ця функція нічого не забороняє, але все запам'ятовує. Звіт містить всю необхідну інформацію про діяльність дитини за комп'ютером.

Можна зробити висновок, що обмеження доступу до певних ресурсів комп'ютера в тому числі і мережі Internet за допомогою «батьківського контролю» не є складною задачею і під силу будь-якому користувачу. Хоча система не є досконалою при правильних налаштуваннях користувач може бути впевненим, що його дитина чи працівники його компанії використовують персональний комп`ютер з користю.

Література

1. Батьківський контроль [Електронний ресурс] Режим доступу: https://ru.wikipedia.org/wiki/Родительский_контроль

УДК 614.8

АСПЕКТИ ПРОЕКТОВАНИХ СИСТЕМ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ПРИ ХІМІЧНИХ АВАРІЯХ

Пластун М. Є.
Мирошник О. М., канд. техн. наук, доцент
Черкаський інститут пожежної безпеки ім. Героїв Чорнобиля НУЦЗУ

Аварії на хімічних підприємствах несуть велику небезпеку, оскільки вражаюча дія проявляється при малих концентраціях небезпечних хімічних речовин (НХР), а швидкість поширення є порівняно високою. Адекватність і своєчасне прийняття рішень у таких умовах буде сприяти зменшенню кількості жертв і потерпілих, проведенню відповідних заходів. Їхньою основою є планування запобігання та ліквідації надзвичайних ситуацій (НС).

Автори [1] пропонують для розв'язання задач планування запобігання та ліквідації надзвичайних ситуацій використовувати технології обчислювального інтелекту, а саме системи підтримки прийняття рішень (СППР). Проблеми побудови ефективних СППР досить повно відображені в сучасній науковій літературі. Множина підходів і пропозицій по конструктивній реалізації таких систем приводить до закономірного питання про їхню систематизацію й доцільності використання в практиці роботи відповідних підприємств і служб.

Однієї з нових і перспективних ідей при побудові СППР при хімічних аваріях є інтеграція елементів експертних систем і геоінформаційних систем (ГІС). Автор [2] пропонує покласти в основу такої інтеграції продукційно-фреймові моделі знань і використовувати об'єктно-орієнтований підхід. Але, як і в інших роботах, не відображено яким чином буде здійснена взаємодія з компонентами ГІС і яка інформація буде використовуватись для підтримки прийняття розв'язків.

Інтелектуальна СППР, запропонована у [3], складається з моделюючої підсистем, що включає у себе ситуаційно-рекомендуючий модуль на основі нечітких мереж Петрі та алгоритмів нечітких логічних висновків, а також управляючої підсистеми, яка функціонує на основі використання продукційних правил. Зважаючи на те, що СППР орієнтована на використання персоналом підприємства й базується на експертних висновках, було б раціонально використовувати її основні елементи для прогнозування наслідків аварії.

У роботі [4] наведена типова структура комплексу інформаційного й програмного забезпечення для аналізу ризику й наслідків аварій на хімічно небезпечних об'єктах, що включає в себе інформаційну підсистему, підсистему для аналізу виробничої небезпеки, оцінки ризику й наслідків аварій, а також підсистему для керування безпекою. Комплексний характер розробки є її безсумнівною перевагою, але без можливості використання в режимі реального часу й обліку особливостей аварії система втрачає актуальність.

Таким чином, аналіз принципів і конструктивних особливостей проектованих СППР дозволяє зробити висновок про різноманітність прийомів і способів їх створення. Присутність елементів штучного інтелекту є умовою здійснення об'єктивізації прийнятих розв'язків, спрощення їх інтерпретації, інтелектуалізації процесів прийняття рішень. Разом з тим, залишаються проблеми інтеграції сучасних обчислювальних засобів, програмного забезпечення, інтелектуальних методів та існуючих методик визначення концентрації НХР у післяаварійний період.

Література

1. Терехов В.И. Проблемы применения вычислительного интеллекта при планировании задач по предотвращению и ликвидации последствий чрезвычайных ситуаций / В.И. Терехов, И.М. Тетерин, Н.Г. Топольский // Материалы XV межд. научн.-практ. конф. «Системы безопасности». – М.: Академия МЧС России, 2006. – С. 49-52.

2. Исаев С.В. Инструментальные средства проектирования интегрированных систем поддержки принятия решений по ликвидации химических аварий : автореф. дисс. … канд. техн. наук: спец. 05.13.06 «Применение вычислительной техники, математического моделирования и математических методов в научных исследованиях (по отраслям наук)» / Исаев Сергей Владиславович ; ИВМ СО РАН. – Красноярск, 1999. – 22 с.

3. Левушкина С.А. Интеллектуальная система поддержки принятия решений по управлению качеством атмосферного воздуха на химических предприятиях: автореф. дисс. … канд. техн. наук: спец. 05.13.01 «Системный анализ, управление и обработка информации» / Левушкина Светлана Анатольевна ; РХТУ им. Д. Менделеева. – М., 2010. – 20 с.

4. Егоров А.Ф. Комплекс программных средств для анализа риска и последствий аварий на химически опасных объектах // А.Ф. Егоров, Т.В. Савицкая, П.Г. Михайлова / Программные продукты и системы. – 2008. – № 4. – С. 138-140.

АЛГОРИТМ КАНОНІЧНОГО РОЗКЛАДУ ЧИСЛА НА МНОЖНИКИ

Поліщук О.
Процько І.
Львівський державний університет безпеки життєдіяльності

Розглянуто алгоритм для програмної реалізації канонічного розкладу числа на множники з використанням залишків кожного вагомого коефіцієнта значення простого числа, оцінено обчислювальну складність алгоритму.

Ключові слова: ефективний алгоритм, розклад числа, обчислювальна складність.

Функція розбиття одновимірної величини до простіших розмірно-компактних обсягів є актуальним в криптографічних методах та інших різноманітних застосуваннях.

В класичному розумінні [1] задача складеного значення величини на прості числа подається у виді

$$N = p_1^{s1} * p_2^{s2} * \dots p_i^{si} \dots * p_k^{sk}, \quad (1)$$

де канонічний розклад (1) числа на прості множники $p_1^{s1}, p_2^{s2}, \dots p_k^{sk}$. а s_i - степінь повторюваності простих множників p_i ($i=1,2,\dots,k$), потребує ефективних засобів реалізації.

Найпоширенішою реалізацією розкладу числа на множники є виконання елементарної перевірки на ділення без залишку даного обсягу N на послідовний вибір дільників з множини простих чисел 2,3,5,7,9,11,13,17…. Однак послідовне виконання операцій ділення для перевірки на кратність в сучасних комп'ютерних моделях виконується за допомогою мікропрограми або спеціалізованих арифметичних вузлів, що збільшує тривалість обчислення канонічного розкладу.

В роботі для підвищення швидкодії обчислення канонічного розкладу числа на множники запропоновано підхід з використанням залишків кожного вагового коефіцієнта числа для простих чисел p_i та їх можливих повторень [2]. В основі ефективного підходу обчислення канонічного розкладу використовується заміна арифметичної операції ділення операціями додавання.

Так, загальнопоширене визначення подільності десяткового числа, коли залишок дорівнює нулю, у випадку представлення в двійковій системі числення матиме вигляд:

$$A \bmod i = (a_n * 2^n + a_{n-1} * 2^{n-1} + a_{n-2} * 2^{n-2} + \cdots a_1 * 2 + a_0) \bmod i = (a_n(2^n \bmod i) + a_{n-1}(2^{n-1} \bmod i) - a_{n-2}(2^{n-2} \bmod i) + \cdots a_1(2 \bmod i) + a_0) \bmod i. \quad (2)$$

Тобто у цьому підході канонічний розклад базується на використанні залишків кожного вагового коефіцієнта 2^i (i=0,1,…n) числа, за формулою (2), для послідовності простих чисел Mi та x степенів, накоплене значення

яких по вибраній вазі у випадку кратності дорівнює *Mi*. Організувавши накопичення значень залишків за вибраними вагами, порівнюємо накопичену суму з Mi за умови більше або дорівнює. Залежно від виконання умови визначаєм подальший режим роботи. У випадку більше – знову накопичується значення залишків від попереднього одержаного накопиченого числа, а у випадку дорівнює – виводиться елемент канонічного розкладу та виконується перехід до наступного значення з послідовності простих чисел Mi. Отже, формується послідовність елементів канонічного розкладу (1) числа одновимірної величини N.

На програмному рівні мов Сі та асемблера запропонований підхід достатньо просто реалізується з використанням команд зсуву, додавання і порівняння. Це дозволило створити оптимізовану ефективну програму канонічного розкладу числа на множники в асемблерному коді іх86, що може застосовуватись в багатьох прикладних програмних продуктах

Література

1. Виноградов И.М., Основы теории чисел. – М.: Наука, 1972. 2. Патент 19531А Україна, G06F07/04. Пристрій канонічного розкладу числа на множники / Процько І.О., Рашкевич Ю.М. (Україна), Опубл. 02.12.97, Бюл. № 6.

ПРОГРАМНЕ ВІДНОВЛЕННЯ

Рибак В.В.
Марченко А.П.
Черкаський інститут пожежної безпеки ім. Героїв Чорнобиля НУЦЗУ

В наш час у зв'язку з важким становищем у державі, падінням національної валюти, великими цінами на нові жорсткі диски та надання послуг з діагностики та відновлення HDD, збільшенням обсягу та важливості інформації в структурі ДСНС – використання систем діагностування для попередження виходу з ладу диску, а також відновлення їх у разі відмови є дуже необхідним. Існує багато, як платних, так і безкоштовних програм, найкращі з яких широко застосовуються в повсякденному житті. До уваги брались тільки безкоштовні програми, їх існує велика кількість, функціональні можливості яких дозволяють зробити в повній мірі все необхідне.

В більшості випадків цінність інформації на носіях пам'яті набагато перевищує їх вартість. Відновлення цих носіїв на програмному та фізичному рівнях задля збереження інформації зумовлює актуальність даної роботи.

В даній роботі було розглянуто будову й принцип дії жорстких дисків, показано, як теоретично та практично здійснити діагностику та відновлення жорстких дисків за допомогою програмного засобу Victoria. Програма Victoria здійснює пошук і усунення дефектів у роботі дисків, відображення повної технічної інформації по різним накопичувачам, швидке отримання точної online-оцінки стану дисків, вбудована довідкова система, а також файловий менеджер, пошук пошкоджених контактів в шлейфі шляхом тестування інтерфейсу, автоматичне виявлення контролерів, кілька режимів тестування поверхні, оцінювання продуктивності накопичувачів, очистка повністю всього вінчестера або його окремих частин, копіювання даних по секторам, пошук дефектів на поверхні HDD та ін. Даний програмний продукт має простий інтерфейс, працює з контролерами SATA, IDE. Немає необхідності в установці, має високу швидкість виконання робочих операцій. Також є такі надійні програми як MHDD, HDDRegenerator.

Проте було розглянуто далеко не весь перелік програм, які можуть відновити жорсткий диск, особливо платних, однак даний перелік використовується найбільш часто і в багатьох випадках дозволяє вирішити проблеми. Кращу программу назвати складно. У кожної з них є свої переваги і недоліки. Узагальненої програми, яка відновлює в усіх випадках, немає. Тому, якщо відновити жорсткий диск відразу за допомогою певної програми не вдалося, спробуйте використовувати іншу.

Розроблені теоретичні та практичні основи можуть бути використані для діагностування жорстких дисків всіх типів з метою виявлення їх пошкоджень та визначення доцільності відновлення жорсткого диску з програмними та фізичними пошкодженями.

Література

1. https://uk.wikipedia.org
2. http://comp-team.narod.ru
3. http://ua-referat.com

УДК 004.89:614.841.4

ІНФОРМАЦІЙНО-АНАЛІТИЧНА ПІДТРИМКА ПРОЦЕСУ КОМПЛЕКТУВАННЯ АВАРІЙНО-РЯТУВАЛЬНОЇ ТЕХНІКИ

Секрет В. О.
Лагно Д. В.
Черкаський інститут пожежної безпеки імені Героїв Чорнобиля НУЦЗУ

Відомо, що задача комплектування аварійно-рятувальної техніки (АРТ) є складною багатокритеріальною задачею. Головними критеріями, які використовуються при її розв'язанні, є функціональність, потужність та ціна. Важливу роль відіграють також габаритні розміри АРТ.

Процес розв'язання задачі її комплектування базується на основі використання інформаційної бази (ІБ). Оскільки постійно з'являються нові зразки АРТ та носіїв, на які вона встановлюється, то необхідно враховувати фактор динамічності ІБ. Крім того, його розробка повинна базуватись на таких принципах:

- системності, що передбачає впорядкування номенклатури АРТ за певним переліком типів та іншими критеріями;
- мобільності, в якому відображено можливість встановлення АТР на різні види носіїв;
- відкритості, що дозволить здійснювати корекцію ІБ у залежності від необхідності, а також додавати чи вилучати дані про певні типи АРТ;
- інформаційної єдності, що визначає єдиний формат представлення даних для різних варіантів техніки.

Реалізація вказаних принципів дозволить сформувати ІБ та запропонувати його структуру у вигляді кортежу таких елементів:

$$ІБ = < N, ID, A, B, C, S, R, P, Z, t >, \quad (1)$$

де N – номер виробу, ID – його назва (ідентифікатор), A, B, C – габаритні розміри, S – тип аварійної ситуації, де використовується виріб (можливо, S є вектором, що пов'язано з багатофункціональністю окремих виробів), R – визначає рівень функціональності виробу (очевидно, що $R = R(S)$), P – потужність виробу (можливо враховувати різні одиниці потужності), Z – ціна виробу, t – час формування запису про виріб. Останній параметр потрібен для відстеження тенденцій про ціну АРТ. Зауважимо, що записи, про один вид техніки та його різні ціни в різні моменти часу повинні залишатись в ІБ. Розробка принципів ведення ІБ, а також його структури є необхідною умовою розв'язання задачі комплектування АРТ.

Література

1. Кучер П., Снитюк В.Е. Формализация задачи комплектования и эволюционные аспекты ее решения / Штучний інтелект. – 2009. – № 4. – С. 268-273.

УДК 005.8+614.8

ПРОЕКТНО-ОРІЄНТОВАНЕ УПРАВЛІННЯ РЕСУРСАМИ ПРИ РЕАГУВАННІ НА НАДЗВИЧАЙНІ СИТУАЦІЇ У СІЛЬСЬКІЙ МІСЦЕВОСТІ

Сеник Ю.Я.
Івануса А.І., канд.техн. наук
Львівський державний університет безпеки життєдіяльності

На сьогоднішній день функціонування системи реагування на надзвичайні ситуації в містах України є досить ефективним. Завдяки її успішному функціонуванні та героїзму рятувальників щороку в нашій державі рятуються життя сотні громадян, а збитки від пожеж та надзвичайних ситуацій (НС) зводяться до мінімуму. Проте доволі «сумна картина» спостерігається у статистичних даних при ліквідації загроз життю та здоров'ю людей, котрі проживають у сільській місцевості. Це зумовлено тим, що важливим фактором успішної ліквідації будь-якої надзвичайної події є мінімальний час реагування на неї, який становить інтервал від отримання повідомлення про виклик рятувальних служб до моменту їх прибуття на місце виклику. Саме цей показник при реагуванні на НС в умовах сільської місцевості має досить велике значення і коливається в діапазоні декількох десятків хвилин, у той час коли його значення у розвинених містах країни, в більшості випадків, не перевищує 9 хвилин.

Таке вагоме значення даного показника зумовлено тим, що застосування сил і засобів рятувальних служб у перші хвилини розвитку пожежі чи НС значно підвищують можливість забезпечення безпеки людей, довкілля та мінімізують матеріальні збитки і ресурси, які спрямовані на ліквідацію НС [1, 2].

На жаль у сьогоднішніх умовах складного соціально-економічного розвитку нашої держави реалізація проектів, спрямованих на підвищення рівня безпеки у сільській місцевості здійснюється частково у зв'язку із браком коштів. Враховуючи те, що кількість зацікавлених сторін такого роду проектів є доволі значною, а саме це – місцеві жителі окремого регіону, органи місцевого самоврядування та виконавчої влади, Державна служба України з надзвичайних ситуацій (ДСНС України), підприємства різних форм власності тощо, то вирішення питання фінансування можна шляхом раціонального управління ресурсами [3]. Для вирішення цієї проблеми було розроблено модель-схему проектно-орієнтованого управління ресурсами системи реагування на НС у сільській місцевості, яка відображає взаємозв'язки зацікавлених сторін проекту, їх фінансові та функціональні зобов'язання, вплив турбулентного середовища та регіональної складової на проект тощо, з метою проведення мінімізації ресурсів, що представлена на рис. 1.

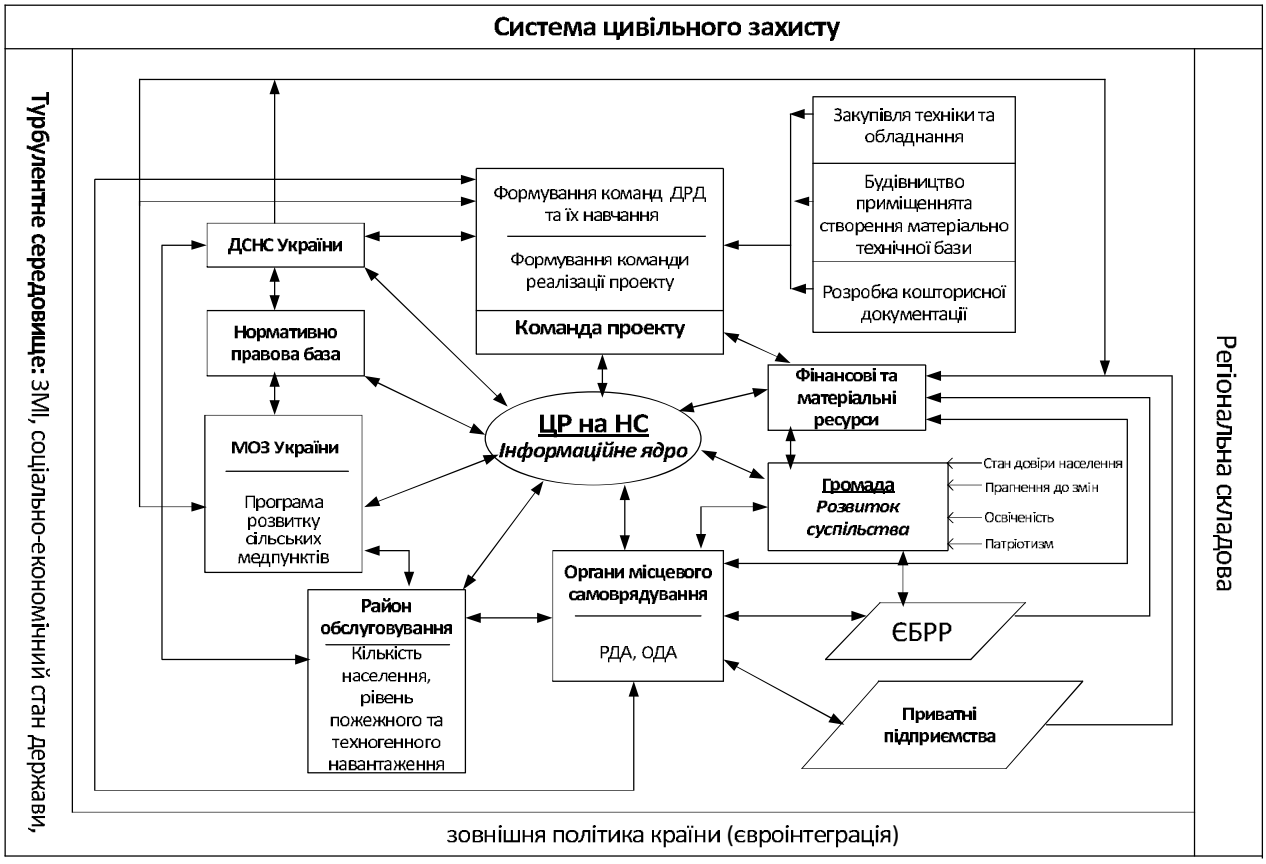

Рис. 1. *Модель-схема проектного середовища раціонального розподілу ресурсів при створенні та управлінні центром реагування на НС в турбулентному середовищі цивільного захисту*

Отже, в результаті проведеного дослідження було розроблено проектне середовище створення центру реагування на НС в умовах турбулентного середовища цивільного захисту, що відображає взаємозв'язки між зацікавленими сторонами даного проекту та дозволяє раціонально розподілити ресурси при його практичній реалізації.

Література

1. Рак Ю. П. Офісне управління регіональними портфелями проектів безпеки людей з урахуванням синергетики природно-техногенної небезпеки / Ю. П. Рак, В.П. Квашук // Вісник ЛДУБЖД. – Львів, 2012. – №6 – С. 36-41.

2. Гуліда Е.М., Войтович Д.П. Аналіз методів визначення кількості і розташування пожежно-рятувальних депо та автомобілів в містах // Пожежна безпека, №12, 2008. – С. 161-169.

3. Бушуєв С. Д. Креативные технологии управления проектами и программами / С. Д. Бушуєв, Н. С. Бушуєва, И. А. Бабаєв [и др.] – К. : «Самит-Книга», 2010. – 768 с.

УДК 004.6

ХМАРНІ АНТИВІРУСИ – НОВЕ ПОКОЛІННЯ АНТИВІРУСНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Старенький М.І.
Полотай О.І., канд. техн. наук
Львівський державний університет безпеки життєдіяльності

Сучасне суспільство швидкими темпами наближається до визнання його інформаційним. Інформаційне суспільство, це суспільство, в якому домінує ефективне використання, накопичення та оброблення знань. Поняття інформаційне суспільство та суспільство знань виступають свого роду синонімами. Інформаційне суспільство не можливе без всебічного використання інформаційного технологій – технологій, які дають змогу їх користувачам економити багато часу, який в вищезгаданому інформаційному суспільстві стає все більш цінним. Інформаційні технології розвиваються неймовірними темпами, і такими, що навіть саме це інформаційне суспільство не здатне слідкувати за всіма нововведеннями у цій сфері. Щодня до всесвітньої мережі підключається безліч пристроїв, які роблять істотний вплив на спосіб існування інформаційного суспільства, та й загалом суспільства як такого. Інформація, та знання, що з неї випливають, виступають основною цінність інформаційного суспільства. Саме розвиток інформаційного суспільства та необхідність збереження інформації, стало поштовхом до збільшення інтересу та попиту до такого виду нових послуг як хмарні технології.

Хмарні технології – технології, котрі забезпечують користувачеві доступ до інформації, що зберігається на сервері постачальника послуг у будь-який момент часу та у будь-якому місці, за тієї умови, що користувач цих послуг має доступ до мережі Інтернет з персонального комп'ютера або ж з мобільного пристрою.

Під час використання цих технологій, користувачеві надаються необхідні йому послуги у вигляді інтернет-сервісу. Особливість збереження даних за допомогою хмарних технологій є те, що користувач має доступ до своїх даних, працює з ними в режимі онлайн, але йому немає потреби піклуватись про програмне забезпечення та операційну систему з якою він працює.

Важливим моментом при користуванні даними технологіями є захист інформації від можливих загроз. Шкідливе програмне забезпечення вдосконалюється майже щодня, саме через це виникає потреба у вдосконаленні антивірусного програмного забезпечення. В останні роки розробники антивірусів почали звертати увагу на хмарні обчислення. Дані обчислення поділяються на два типи: платформні хмари та хмари послуг [2]. Платформні хмари надають доступ до операційної системи, яка забезпечує зберігання даних з можливістю її налаштування користувачем під власні потреби, а

звичайні хмари надають у користування лише місце для збереження даних, тобто користувач не має змоги широко їх налаштовувати, а лише використовувати для власних цілей.

Антивірусне програмне забезпечення, що ґрунтується на хмарному середовищі (їх ще називають хмарними антивірусами), є комплексом двох компонентів: додатку, який встановлений на комп'ютері користувача, та веб-сервісу, доступ до якого здійснюється через мережу Інтернет. Обидва компоненти працюють як єдине ціле. Веб-сервіс хмарного антивірусу розташований на серверах компанії, що надає послуги, саме він виконує значну частину роботи, тобто зберігання антивірусних баз, обробка інформації якою володіє користувач. Важливою відмінністю додатку, що встановлений на машині користувача є те, що він потребує значно менше ресурсів комп'ютера на відміну від традиційного антивірусного ПЗ.

Як серед традиційних антивірусів є свої лідери, так і серед хмарних антивірусів є свій – Panda Cloud Antivirus [1], котрий повністю працює на хмарному середовищі в режимі реального часу. Він пропонує нову технологію асинхронного сканування в хмарному середовищі. При мінімальному впливі на продуктивність, цей спосіб поєднує традиційні методи виявлення шкідливого коду з перевіркою в хмарному середовищі. Завдяки використанню хмарних технологій антивірусне програмне забезпечення Panda Cloud Antivirus аналізує одночасно неймовірно велику кількість різноманітних загроз, накопичені користувачами глобального товариства продуктів Panda та відразу шукає вирішення для нейтралізації нових загроз в режимі реального часу. Окрім цього, при виявленні нової загрози система автоматично та оперативно шукає вирішення проблеми і як тільки вона буде вирішена, відбувається оновлення бази, що б в майбутньому дає змогу унеможливити виникнення подібної проблеми в інших користувачів.

Отже, дані антивіруси мають ряд переваг: підвищення продуктивності, завжди актуальні бази вірусів, значно скорочений час реакції на потенційну загрозу, швидке впровадження актуальних засобів боротьби з шкідливим кодом. Проте як і будь-який продукт, він має свої недоліки : неможливе повноцінне функціонування без підключення до мережі Інтернет, проблемне завантаження даних із-за повільних підключень по каналах зв'язку.

Література

1. Веб сайт «Антивірус. Програмне зебезпечення. [Електронний ресурс]. – Режим доступу з http://www.antivirus.if.ua/news/antivirus-with-clouds.html

2. Веб сайт компанії «Бізнес-технології онлайн». [Електронний ресурс]. – Режим доступу з http://cbto.com.ua/antyvirusni-systemy-z-hmarnoyu-arhitekturoyu.html

УДК 004.056

ВРАЗЛИВІСТЬ ПРОТОКОЛУ HTTPS ДО АТАК ТИПУ LOGJAM

Султанова С.Ф.
Гриник Р.О.
Львівський державний університет безпеки життєдіяльності

Як правило, обмін даними між абонентами в інтернеті відбувається по протоколу HTTP, цей протокол не тільки встановлює правила обміну інформацією, а й служить транспортом для передачі даних - з його допомогою браузер завантажує вміст сайту на ваш комп'ютер або смартфон. Протокол HTTP має один суттєвий недолік, він передає інформацію у відкритому вигляді, що дає змогу зловмиснику перехопити дані котрі передаються. Для встановлення безпечного з'єднання використовується протокол HTTPS з підтримкою шифрування. Захист даних в протоколі HTTPS забезпечує криптографічній протокол SSL/TLS, який використовує асиметричну криптографію для встановлення з'єднання, симетричну криптографію для шифрування повідомлення та коди автентифікації повідомлення для забезпечення цілісності інформації. Проте на даний час використання протоколу HTTPS не гарантує високої ступені захищеності, оскільки він вразливий на транспортному рівні.

На транспортному рівні безпеку забезпечує протокол TLS який в 2008 році замінив протокол SSL v.3.0. Вразливість протоколу полягає в тому, що ще в середині дев'яностих років на вимогу США розробники протоколу ввели обмеження щодо алгоритму Діффі-Хеллмана, а протокол TLS використовує даний алгоритм для захисту спільного секретного ключа підчас передачі його по незахищеним каналам зв'язку. Дана вразливість отримала назву Logjam, вона дає змогу зловмиснику підключитись до каналу зв'язку і стати посередником між абонентом мережі та сервером з підтримкою обміну секретними ключами по алгоритму Діффі-Хеллмана. Для цього зловмиснику необхідно надсилати на сервер модифіковані запити для того, щоб заставити сервер використовувати у всіх з'єднаннях слабкий ключ довжиною 512 біт. Після цього атака зводиться до алгоритмів факторизації великих цілих чисел, для цього можна використати як загальний метод решета числового поля, так і інтелектуальні моделі факторизації великих простих чисел побудовані на еволюційних алгоритмах [1,2].

Особливість атаки Logjam полягає втому, що вона протягом довгого часу залишається непомітною і може виконуватись у режимі реального часу. По оцінкам Надії Хенінджер з Пенсільванського університету атака на протокол HTTPS зачіпає приблизно 8,4 % з першого мільйона найпопулярніших сайтів і трохи більший процент поштових серверів. Зокрема, ті з них, які підтримують протокол StartTLS, а також безпечну авторизацію POP3 або IMAP, за її оцінками, серед них зараз уразливі відповідно 14,8%, 8,9% і 8,4% поштових серверів [3].

Проблема полягає ще і в тому, що подібний спосіб компрометації ключів може використовуватися проти будь-яких серверів, які підтримують обмін ключами по протоколу Діффі-Хеллмана (DH). У теорії він дозволяє двом сторонам передати секретний ключ по незахищеному каналу зв'язку, але на практиці не

повинен використовуватися як самодостатній метод. Для високої надійності систем передачі даних рекомендується додатково використовувати двосторонню автентифікацію або реалізовувати DH на еліптичних кривих (ECDHE). Перевірити сайт на уразливість до атаки Logjam можна на сайті WeakDH.

Література

1. Гриник Р.О., Застосування генетичного алгоритму для вирішення задач криптоаналізу, Інформаційно-комунікаційні технології в сучасній освіті: досвід, проблеми, перспективи : IV Міжнар. наук.-практ. конф., 21-22 жовт. 2015 р. : зб. наук. пр. – Ч. 1. – Львів, Вид-во ЛДУ БЖД, 2015. – С. 168-170

2. Гриник Р.О., Шадий В.І. Побудова моделі інтелектуальної системи на базі генетичного алгоритму для криптоаналізу RSA, "Захист інформації в інформаційно-комунікаційних системах": збірник тез доповідей І Міжвузівської науково-практичної конференції. – Львів: ЛДУ БЖД, 2015. С. 23-24.

3. HTTPS-crippling attack threatens tens of thousands of Web and mail servers [Електронний ресурс]. Режим доступу: http://arstechnica.com/security/2015/05/https-crippling-attack-threatens-tens-of-thousands-of-web-and-mail-servers/

УДК 630.43:662.519.6

ЧИСЕЛЬНЕ МОДЕЛЮВАННЯ ГІДРОДИНАМІЧНОГО ПРОЦЕСУ ТЕПЛОМАСОПЕРЕНОСУ ПРИ ПОШИРЕННІ ПОЖЕЖІ

Тацій М.І.
Боднар Г.Й., канд. техн. наук, доцент
Гембара Т.В., канд. техн. наук, доцент
Львівський державний університет безпеки життєдіяльності

Чисельне моделювання процесів горіння все більш часто використовується в наукових розробках, а також при розслідуванні пожеж. Розвиток теорії математичного моделювання горіння, а також збільшення обчислювальної потужності комп'ютерів дозволило істотно скоротити необхідні ресурси, а також підвищити точність чисельного моделювання. Наприклад, однією з важливих областей застосування результатів математичного моделювання динаміки пожежі є тестування інтелектуальних алгоритмів роботи автоматичної пожежної сигналізації. Математичне моделювання дозволяє отримати динаміку розвитку небезпечних факторів пожежі в різних умовах обчислювального експерименту. Як відомо, до небезпечних факторів пожежі відносяться: полум'я і іскри; тепловий потік; підвищена температура навколишнього середовища; підвищена концентрація токсичних продуктів горіння і термічного розкладання; знижена концентрація кисню; зниження видимості при задимленні.

Метою даної роботи є чисельна реалізація математичних моделей найбільш характерних вогнищ пожежі, а також встановлення характерних особливостей динаміки розвитку пожежі на початковій стадії. Існує кілька основних моделей пожежі, використовуваних для прогнозування: інтегральна; зонна; польова диференціальна модель. Інтегральна модель пожежі дозволяє отримати інформа-

цію про середні значення параметрів середовища в приміщенні для будь-якого моменту розвитку пожежі. Зонна модель дозволяє отримати уявлення про розміри характерних зон, що виникають під час пожежі в приміщенні, а також про середні параметри стану середовища всередині цих зон. Польова диференціальна модель дозволяє розрахувати для будь-якого моменту розвитку пожежі значення всіх локальних параметрів стану в будь-якій точці простору приміщення. Всі три моделі в математичному відношенні характеризуються різним рівнем складності. Найбільш просто реалізується інтегральна модель, вона ж є і найменш точною. Найбільш перспективною, з точки зору, практичного застосування є польова модель горіння, яка ґрунтується на системі диференціальних рівнянь в частинних похідних. Результатами розв'язання даної системи рівнянь є поля розподілу температур, швидкостей, концентрацій компонентів газового середовища в кожен момент часу. Відповідні програмні пакети для розрахунків та візуалізації їх результатів, розроблені Лабораторією з пожежної безпеки Національного інституту стандартів і технологій (США) та науково-дослідним центром VTT (Фінляндія), фактично використовуються як стандарти контролю пожежної безпеки об'єктів. Особливістю є те, що їх необхідно запускати з командного рядка, а вхідні параметри повинні бути записані в текстовий файл [1].

Ці пакети реалізують обчислювальну гідродинамічну модель тепломасопереносу при горінні, особлива увага приділяється поширенню диму і теплопередачі під час пожежі. Чисельно різницевими методами розв'зується рівняння Нав'є-Стокса для низькошвидкісних температурно-залежних потоків. Базовим алгоритмом є схема використання методу предиктор-коректора другого порядку точності по координатах і часу. Турбулентність досліджується за допомогою моделі Смагоринського. Головним чином нас цікавить початковий момент і інтервал часу пожежі, коли спрацьовування автоматичної пожежної сигналізації ще може привести до виконання системою своїх цільових функцій (евакуація людей, ефективне пожежогасіння). Цей інтервал є відносно малий, і в цей проміжок часу пожежа має деякі особливості, що дозволяють забезпечити високий ступінь спрощення математичної моделі. Основною особливістю даного процесу є відсутність газообміну приміщення з навколишнім середовищем. Надходження повітря в приміщення з навколишнього середовища відсутнє, і динаміка загоряння диктується виключно пожежним навантаженням. Тому польова модель пожежі, має обмежений характер за часом і справедлива виключно в початковий момент розвитку пожежі, поки відсутнє надходження повітря в приміщення. Для роботи в програмі використовується схема одноступінчастої хімічної реакції, результати передаються через двопараметричну модель частки в суміші. За замовчуванням розраховуються два параметра суміші: масова частка незгорілого палива і масова частка вигорілого палива (тобто продуктів згоряння).

Література

1. K. McGrattan, S. Hostikka, R. McDermott, J. Floyd, C. Weinschenk, and K. Overholt. Fire Dynamics Simulator, User's Guide. National Institute of Standards and Technology, Gaithersburg, Maryland,USA, and VTT Technical Research Centre of Finland, Espoo, Finland, sixth edition, September 2013,v.4, 12-15.

УДК 004.056

КОМПЛЕКС ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В ОХОРОНІ ДЕРЖАВНОЇ ТАЄМНИЦІ

Усенко Р.П.
Мандрона М.М., канд. техн. наук
Львівський державний університет безпеки життєдіяльності

Система охорони державної таємниці (ДТ) в Україні створювалась з урахуванням практичного досвіду розвинених країн та випробуваних засобів і методів. Значною мірою сучасна Україна перейняла систему захисту секретної інформації, яка існувала за часів Радянського Союзу. Велику кількість елементів цієї структури було збережено, а з часом розвинуто і вдосконалено. Заходи, які вживає держава, охороняючи свої секрети, мають бути адекватними загрозам (як зовнішнім, так і внутрішнім), що існують на даний момент. Для ефективного вирішення цього питання потрібний комплексний підхід. Формування системи охорони ДТ передбачає запровадження системи взаємодіючих адміністративно-правових режимів, функції яких, в тій чи іншій мірі, направлені на охорону державної таємниці. Запровадження ж відповідних режимів передбачає нормативно-правове регулювання відносин у цій сфері та створення державних органів, діяльність яких направлена на вирішення конкретних завдань з забезпечення вказаних режимів. Одним з таких завдань є збереження інформації що становить державну таємницю.

Інформація це – відомості, дані або факти які можна зберегти на матеріальному носієві інформації та відтворити їх [1]. Тому відомості, дані чи факти до яких доступ обмежено є цінністю для власника інформації, а у випадку втрати можуть спричинити збитки особі, суспільству чи державі, так пояснює Закон України «Про інформацію». Саме тому забезпечення охорони такої інформації є пріоритетним завданням кожної сучасної країни.

Найціннішою інформацією з обмеженим доступом є державна таємниця. Згідно з ст. 1 Закону України «Про державну таємницю», державна таємниця – це вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України [2].

Для забезпечення охорони ДТ розроблено систему охорони державної таємниці, яка є комплексом організаційно-правових заходів, інженерно технічних засобів, криптографічних та оперативно-розшукових заходів [2].

Відповідно до вимог законодавства ДТ повинна оброблятися в інформаційно-телекомунікаційній системі, в якій встановлено комплексну системи захисту інформації (КСЗІ) із атестатом відповідності. Така система

повинна забезпечувати захист інформації від витоку технічними каналами, захист від несанкціонованого ознайомлення з даними та від спеціальних впливів на активні системи.

Для цього у складі КСЗІ повинні бути комплекс технічного захисту інформації (КТЗІ), комплекс засобів захисту від несанкціонованого доступу (КЗЗ від НСД) [3].

Комплекс технічного захисту інформації – це сукупність організаційних, інженерних і технічних заходів та засобів, призначених для захисту від витоку інформації з обмеженим доступом технічними каналами на об'єктах інформаційної діяльності [4].

У створенні КТЗІ беруть участь:

- установа, яка є замовником створення КТЗІ;
- виконавець робіт зі створення КТЗІ;
- виконавець проведення випробувань щодо створення КТЗІ;
- виконавець проведення атестації КТЗІ.

КТЗІ повинні взаємодіяти з іншими системами, які наявні в установі, таких як охоронна та протипожежна сигналізації, спеціальна система енергоживлення, а також повинна забезпечувати виконання норм ефективності захищеності інформації та відповідати вимогам щодо необхідності перевірок цієї захищеності.

Основними заходами щодо організації створення КТЗІ є підготовка і подання підрозділом технічного захисту інформації на затвердження керівнику установи-замовника заявки про створення КТЗІ, яка складається з протоколу про визначення вищого ступеня обмеження доступу до інформації та проекту рішення щодо створення КТЗІ на об'єкті інформаційної діяльності (ОІД). Також установа-замовник повинна підготувати пропозиції щодо термінів проведення обстеження на ОІД, створити модель загроз та організувати розроблення технічних завдань щодо створення КТЗІ. Після цього створюються відповідні умови для виконання випробувань і проведення атестації КТЗІ.

Література

1. Закон України «Про інформацію» ВР України [Електронний ресурс]. – Доступно з: http://zakon4.rada.gov.ua/laws/show/3855-12.

2. Закон України «Про державну таємницю» ВР України [Електронний ресурс]. – Доступно з: http://zakon0.rada.gov.ua/laws/show/3855-12.

3. НД ТЗІ 3.7.-003-2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» від 28.12.2012 № 806.

4. НД ТЗІ 1.1-005-07 «Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення».

УДК 005.8

ЕЛЕКТРОННА СИСТЕМА ОПЕРАТИВНОГО УПРАВЛІННЯ РЕСУРСАМИ В ПРОЕКТАХ ЛІКВІДАЦІЇ НАДЗВИЧАЙНИХ СИТУАЦІЙ

Цибульський М.М.
Зачко О.Б., д-р техн. наук, доцент
Львівський державний університет безпеки життєдіяльності

Проаналізувавши масиви карток обліку пожеж за 12 місяців 2015 року в Україні [1] можна побачити, що Івано-Франківська область посідає третє місце серед обласних центрів держави за збільшення кількості пожеж та друге місце за збільшення кількості загиблих внаслідок пожеж (табл. 1).

Таблиця 1

Ранжування областей України, в яких зареєстровано збільшення кількості загиблих внаслідок пожеж

№ з/п	Області	2015 рік	2014 рік	+/-, в %
1.	Закарпатська	32	20	60,0
2.	Івано-Франківська	57	49	16,3
3.	Чернівецька	38	34	11,8
4.	Миколаївська	78	72	8,3
5.	Вінницька	89	85	4,7
6.	Львівська	72	69	4,3
Всього в Україні		**1947**	**2246**	**-13,3**

Перед пожежно-рятувальними підрозділами поставлене завдання, щодо підвищення ефективності роботи під час профілактики та ліквідації пожеж.

Відповідно виникає потреба у модернізації роботи підрозділів під час взаємодії з оперативно-диспетчерскою службою та підрозділами, що прямують до місця виклику. Встановлення та використання у своїй діяльності цифрової системи оперативного управління дозволить істотно зменшити часовий проміжок, який необхідний для пошуку джерел водопостачання, адреси розташування місця виклику та інших умовних позначень протипожежного характеру.

Після запровадження даної цифрової системи оперативного управління можна буде проаналізувати подальшу ефективність використання, лічильник відвідувань за добу відображатиме ефективність системи, що в подальшому надасть поштовх до всеукраїнського застосування та використання пожежними підрозділами.

Особливістю є те, що дану систему можна використовувати з будь-якого пристрою, який має доступ до інтернет-мережі, а якщо такої можливості немає, – то користувач завантажує попередньо виділений регіональний діапазон, та користується даною електронної картою в off-line режимі.

Як видно з рис. 1 після повідомлення про надзвичайну ситуацію диспетчер формує запит про адресу виникнення та місця розташування надзвичайної ситуації.

Рис. 1. *Принципова схема роботи цифрової системи оперативного управління*

Отримані дані диспетчер пункту зв'язку частини роздруковує у форматі А4 на якому відображатимуться реквізити заповнення "дорожнього листа" та раніше заданий пошуковий регіон з уже усіма необхідними даними. Отримавши даний лист підрозділ прямує до місця н/с. Таким чином підрозділ отримує широкий спектр інформації про район виїзду та всі необхідні умовні позначення про розташування засобів пожежогасіння.

Література

1. Електронна адреса: "Аналіз масиву карток обліку пожеж (POG_STAT) за 12 місяців 2015 року" – http://www.undicz.mns.gov.ua/files/2016/1/20/AD_12_2015.pdf
2. Модели и методы проактивного управления программами организационного развития : монографія / Н.С. Бушуева. – К. : Наук. світ, 2007. – 200 с.

УДК 004.056

ЗАСТОСУВАННЯ АЛГОРИТМУ КОЛОНІЇ БДЖІЛ ДЛЯ КРИПТОАНАЛІЗУ АСИМЕТРИЧНИХ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ

Шадий В.І.
Гриник Р.О.
Львівський державний університет безпеки життєдіяльності

Усі асиметричні алгоритми шифрування використовують два ключі: відкритий K_{pub} та закритий K_{priv}.Кожен ключ складається з пари чисел, власне самого ключа та модуля N, $N = p \times q$, де p і q випадкові великі прості числа. Існує декілька варіантів атак на такі шифри, але найбільш оптимальним варіантом атак є розклад числа N на співмножники p і q.

Так як в даному випадку необхідно знайти екстремум не монотонної функції $F(x)$, то дослідження можливості застосування для вирішення даної задачі евристичних методів, що не використовують безпосередньо апарат математичного аналізу, є актуальним завданням. Таким чином, на основі математичної моделі алгоритму, заснованого на поведінці колонії бджіл, і його опису алгоритм факторизації числа сформулюємо в наступній формі:

1. Визначаються параметри алгоритму: кількість бджіл-розвідників D, кількість бджіл-робочих B, кількість ділянок для дослідження околиць Z, точність знаходження дільника E.
2. Вибираються на відрізку $[n_i, n_j]D$ значень аргументу $x_1, ..., x_D$.
3. У вибрані точки x_i відправляються бджоли-робочі для пошуку в їхніх околицях простих чисел, у відповідності з алгоритмом [1]:
   3.1. Визначити для кожного значення x_i значення околиці $r = n / 1,442695$, де n – число біт в двійковому записі числа.
   3.2. Кожне число $y \in [x_i - r, x_i + r]$ послідовно перевіряється на ділення з простими числами з інтервалу $[2, 2 \times r]$.
   3.3. До чисел які пройшли тест на ділення застосовується тест Міллера-Рабіна [2].
4. Після визначення множини простих чисел Y для кожного $y_i \in Y$ обчислити значення функції $F(y_i)$, знайти $\min F(y_i)$. Визначити y_i для яких $F(y_i) < E$.
5. З множини Y вибираються випадковим чином Z елементів, дані значення позначаються як $x_1, ..., x_Z$. Далі відправляються бджоли-розвідники для пошуку на відрізку $[n_i, n_j]$ D значень аргументу $x_{Z+1}, ..., x_{Z+D}$. Якщо умова виходу з алгоритму не виконана необхідно перейти до пункту 3, якщо виконана до пункту 6.

6. Завершити роботу алгоритму.

Умовою зупинки алгоритму може бути закінчення часового ресурсу, визначення величини x_i для яких $F(x_i)=0$ або $F(x_i)<E$, визначення значення функції $F(x_i)$ для всіх $x_i \in [n_i, n_j]$.

Таким чином, в даному алгоритмі вибір значень аргументу $x_i \in [n_i, n_j]$ імітує поведінку бджіл-розвідників, а пошук в околиці найбільш ймовірних простих чисел імітує поведінку робочих бджіл (бджіл-фуражирів). Оскільки в даному випадку визначається екстремум не монотонної функції, то вибір точок x_i на відрізку $[n_i, n_j]$ для пошуку простих чисел в їх околиці проводиться на кожній ітерації випадковим чином, що призводить в загальному випадку до рівно ймовірної можливості отримання глобального оптимуму на кожній ітерації (на відміну від спрямованого сходження до екстремуму в класичному бджолиному алгоритмі, описаному в [3]).

Література

1. Кажаров А.А. Разработка модели криптоанализа RSA при помощи генетических алгоритмов / А. А. Кажаров, Х. А. Кажаров.

2. 20. Аврутин, В. А. Алгоритм поиска простых чисел в заданном интервале / В. А. Аврутин. Электрон, ресурс. Режим доступа: http://library.mephi.ru/data/scientific-eessions/2003/12/024.html

3. Курейчик В. В. Роевой алгоритм в задачах оптимизации / В. В. Курейчик,Д. Ю. Запорожец // Известия ЮФУ. — 2010. — № 7 (108). — С. 28—32.

УДК 004.89:614.841.4

ЕЛЕМЕНТНИЙ БАЗИС ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ КОМПЛЕКТУВАННЯ АВАРІЙНО-РЯТУВАЛЬНОЇ ТЕХНІКИ

Яцишин О. О.
Кучер П. П.
Черкаський інститут пожежної безпеки імені Героїв Чорнобиля НУЦЗУ

Промисловий ріст, зміна клімату, інші фактори об'єктивної та суб'єктивної природи зумовлюють підвищену увагу до оптимізації функціонування аварійно-рятувальних підрозділів. У доповіді показано, що однією з головних задач є комплектування техніки засобами для рятування людей, гасіння пожеж, мінімізації збитків від техногенних та екологічних катастроф. Оскільки на теперішньому етапі основним технічним засобом, на якому розміщується аварійно-рятувальна техніка є пожежний автомобіль, то оптимальне його комплектування є актуальною науковою задачею.

Концептуальні особливості її розв'язання були досліджені в [1]. Визначення ефективності компонувальних рішень запропоновано здійснювати за рядом критеріїв [2]. Водночас зауважимо, що пропоновані рішення є час-

тковими, в той час як задача комплектування вимагає системного підходу, що пов'язано з такими особливостями:

- комплектування однієї окремої одиниці здійснюється, виходячи із комплектування підрозділів, що обслуговують певну територію, на якій проживає певна кількість населення, яка має свої особливості природного і штучного середовища і на якій передбачаються наслідки тієї чи іншої катастрофи;
- задача комплектування є багатокритеріальною, що визначається необхідністю забезпечення максимальної функціональності обладнання, мінімізації його габаритних розмірів, максимізації потужності та мінімізації вартості;
- необхідною умовою розв'язання наведеної вище складної задачі є розв'язання задачі комплектування одного пожежного автомобіля аварійно-рятувальними засобами;
- потрібно передбачити врахування якісних особливостей процесу прийняття рішень, що дозволить одержувати прийнятні розв'язки на базі теорії нечітких множин .

Таким чином, в доповіді вказано на те, що одним з перших кроків розв'язання задачі комплектування є технологічне передбачення можливих техногенних та екологічних катастроф в регіоні та їх наслідків, що можливо здійснювати як в умовах наявності ретроспективних даних, так і на базі моделювання майбутніх процесів з використанням нормативної інформації (унікальне моделювання). Статистичні дані складуть основу прогнозування різноманітних аварійних ситуацій, які викликані повторюваними природними факторами та результатами людської діяльності. Передбачення масштабів надзвичайних ситуацій та наявність певної кількості пожежних автомобілів дозволить здійснити визначення необхідної кількості елементів аварійно-рятувального обладнання.

Формалізація наведених вище задач та їх відображення в категорії моделей дозволить здійснити структурну та параметричну ідентифікацію потрібних залежностей, а також забезпечити можливість пошуку області компромісу. Оскільки їх розв'язання відбувається в умовах, що динамічно змінюються, то раціональним є застосування методів еволюційного моделювання для розв'язання вказаних задач оптимізації.

Література

1. Кучер П.П. Концепція комплектування пожежного автомобіля на базі еволюційного моделювання // Інтегровані комп'ютерні технології в машинобудуванні: Матеріали Міжн. наук.-техн. конф. − Харків: ХАІ, 2014. − С. 253.

2. Кучер П.П. Комплекс моделей для визначення оптимальної комплектації аварійно-рятувальної техніки // Теорія прийняття рішень − 2006: Матеріали III Міжн. школа-семінару з теорії прийняття рішень. − Ужгород: УжНУ, 2013. − С.64.