Висновки дослідження. Управлінські дії завжди з процесами виявлення, розпізнавання територіальних об'єктів (процесів, явищ). Тому наявність вбудованої в РГІС системи підтримки й прийняття рішень (СППР) дозволить аналізувати інформацію, яка надходить до РГІС у режимі реального часу і видавати особі, що приймає рішення (ОПР) цілісне уявлення (виражене у графіках, моделях, цифрах) про ситуацію в регіоні. Такі системи можуть ефективно використовуватись при різноманітних управлінських операціях, діях і заходах різного виду і масштабів, моделюванні заходів з попередження і ліквідації надзвичайних ситуацій тощо.

Запропонований підхід до ухвалення рішень в умовах невизначеності на основі дерева цілей, заснований на математичній моделі, в якій використовуються лінгвістичні змінні, надає можливість спростити процес прийняття рішень і наблизити його до розуміння ОПР. За рахунок цього можуть істотно розширюватись функціональні можливості технології прийняття рішень у РГІС.

Список використаних джерел

1. Геоинформатика / Е. Г. Капралов, А. В. Кошкарев, В. С. Тикунов [и др.] – М.: Академия, 2005. – 480 с.

2. Тихонов А. Н. Методы решения некорректных задач: учеб. пособие для вузов / А. Н. Тихонов, В. Я. Арсенин. – М.: Наука, 1986. – 288 с.

3. Бурачек В. Г. Основи ГІС / В. Г. Бурачек, О. О. Железняк, В. І. Зацерковний. – Ніжин: Аспект-Поліграф, 2011. – 512 с.

4. Цветков В. Я. Основы геоинформатики: электронный учебник / В. Я. Цветков. – М.: М-во общ. и проф. образования РФ. Центр информатизации, 1998. – 627 с.

5. Зацерковний В. І. Методика створення еталонних моделей місцевості просторових об'єктів ГІС за допомогою комбінаторного алгоритму / В. І. Зацерковний, С. В. Кривоберець, Ю. С. Сімакін // Вісник ЧДТУ. Серія «Технічні науки». – 2010. – № 45. – С. 206-213.

6. Зацерковний В. І. Методика створення еталонних моделей просторових об'єктів ГІС за допомогою регуляризуючого функціоналу / В. І. Зацерковний, С. В. Кривоберець, Ю. С. Сімакін // Вісник ЧДТУ. Серія «Технічні науки». – 2011. – № 1 (47). – С. 240-246.

7. Бочарников В. П. Fuzzy-технологія: математические основы. Практика моделирования в экономике / В. П. Бочаров. – СПб.: «Наука» РАН, 2011. – 328 с.

8. Балашов О. В. Система поддержки принятия решений с адаптацией алгоритма вывода / О. В. Балашов, Е. М. Грубник, В. В. Круглов // Математическая морфология. – 2006. – № 1. – С. 12-18.

9. Цветков В. Я. Методы прогнозирования в геоинформационных технологиях / В. Я. Цветков // Информатика-машиностроение. – 1999. – № 4. – С. 44-47.

УДК 004.056.5 (045)

Б.Я. Корнієнко, канд. техн. наук,
О.К. Юдін, д-р техн. наук
В.С. Величко
Національний авіаційний університет, м. Київ, Україна

КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ АВТОМАТИЗОВАНОЇ СИСТЕМИ КЛАСУ «1»

Стаття присвячена порівнянню двох комплексних систем захисту інформації в автоматизованих системах класу «1». Проведено аналіз функцій і складових комплексних систем захисту інформації. Виконано порівняння засобів захисту інформації двох систем та розглянуто особливості їх застосування.

У сучасних умовах інформатизації суспільства не викликає сумніву необхідність захисту інформаційних ресурсів. Однією з найбільш важливих особливостей інформації є можливість існування в різноманітних формах та здатність поширюватися по різних

каналах. Крім того, негативні наслідки може спричинити не лише факт втрати інформацією конфіденційності, що захищається, але і порушення її цілісності та доступності. У зв'язку з цим найбільш доцільним видається комплексний захист інформації на об'єкті інформатизації в цілому. При цьому одним із найважливіших завдань оптимальної побудови комплексної системи захисту інформації (КСЗІ) є вибір із безлічі наявних засобів такого їх набору, який дозволить забезпечити нейтралізацію всіх потенційно можливих інформаційних загроз із найкращою якістю і мінімально можливими витраченими на це ресурсами.

Постановка задачі. Метою дослідження є порівняння двох комплексних систем захисту інформації в автоматизованій системі – ЛОЗА - 1, версія 3, та Страж NT (версія 3.0).

Автоматизована система (АС) – організаційно-технічна система, що реалізує інформаційну технологію й об'єднує засоби обчислювальної техніки й зв'язку, методи та процедури, програмне забезпечення, фізичне середовище, персонал та інформацію, яка обробляється.

За сукупністю характеристик АС виділено три ієрархічні класи:

- клас «1» – одномашинний однокористувачевий комплекс;
- клас «2» – локалізований багатомашинний багатокористувачевий комплекс;
- клас «3» – розподілений багатомашинний багатокористувачевий комплекс.

Слід відзначити істотні особливості АС класу «1»: у кожний момент часу з комплексом може працювати тільки один користувач, хоч у загальному випадку осіб, що мають доступ до комплексу, може бути декілька, але всі вони повинні мати однакові повноваження (права) щодо доступу до інформації, яка оброблюється; технічні засоби з точки зору захищеності відносяться до однієї категорії і всі можуть використовуватись для збереження всієї інформації.

Система захисту інформації ЛОЗА - 1, версія 3

Система ЛОЗА-1 – програмний засіб захисту інформації від несанкціонованого доступу в автоматизованих системах класу "1" [1]. Система ЛОЗА-1 може працювати під управлінням операційних систем Windows XP/Vista/7. Система ЛОЗА-1 реалізує всі стандартні функції, необхідні для надійного захисту інформації від несанкціонованого доступу і для побудови комплексної системи захисту інформації. Система ЛОЗА-1 може використовуватися для захисту інформації, яка складає державну таємницю, що підтверджено експертним висновком № 240, яке видане Державною службою спеціального зв'язку і захисту інформації України 17 вересня 2010 р.

Система ЛОЗА-1 має дві конфігурації (залежно від інформації, яка обробляється в АС):

- "Підвищена безпека" – для захисту інформації з грифом "Таємно" і "Цілком таємно";
- "Стандартна безпека" – для захисту інформації з грифом "ДБК", конфіденційної і відкритої інформації.

Захист від несанкціонованого доступу до інформації система ЛОЗА-1 забезпечує таким чином:

- реалізований надійний захист документів Microsoft Word і Microsoft Excel за рахунок тісної інтеграції з Microsoft Office (відключаються небезпечні команди, макроси, шаблони і так далі); підтримуються версії Microsoft Office XP/2003/2007/2010;
- система ЛОЗА-1 може захистити будь-які інші дані; захист здійснюється на рівні тек Windows і знімних дисків для окремих носіїв;
- система ЛОЗА-1 дозволяє встановлювати дозволи або заборони на запуск процесів;
- система ЛОЗА-1 дозволяє контролювати роботу зі зовнішніми носіями: дискетами, компакт-дисками і флеш-накопичувачами, для флеш-накопичувачів дозволу на доступ до диска можуть встановлюватися для окремих носіїв (вони ідентифікуються по "залізних" серійних номерах).

Контроль друку та експорту реалізований таким чином:

- система ЛОЗА-1 забезпечує можливість установки дозволу/заборони друку й експорту на рівні окремих документів;
- для посилення контролю система ЛОЗА-1 дозволяє забезпечити присутність адміністратора або іншої уповноваженої особи під час друку та експорту (за рахунок необхідності введення додаткового пароля).

Контроль входу користувачів до системи забезпечується:

- у конфігурації "Підвищена безпека" вхід виконується тільки після введення пароля й установки ключового диска (як ключовий диск може використовуватися звичайна дискета або флеш-накопичувач); діє жорстка політика паролів і політика блокування користувачів, яке протистоїть підбору паролів;
- у конфігурації "Стандартна безпека" для входу досить ввести пароль; політика паролів менш жорстка, ніж у конфігурації "Підвищена безпека".

Реєстрація подій виконується таким чином:

- система ЛОЗА-1 має захищений журнал, в якому реєструються всі події, пов'язані із захистом інформації;
- аналіз журналу і протоколів роботи не вимагає спеціальної кваліфікації;
- журнал подій ніколи не перезаписується, – після досягнення граничного розміру журналу всі події зберігаються у файлі на жорсткому диску;
- система ЛОЗА-1 забезпечує детальну реєстрацію подій друку й експорту; разом із стандартною інформацією в журналі фіксуються гриф і обліковий номер документа, а також серійний номер носія, на якому зберігається документ, і носія, на який виконується експорт; адміністратор має можливість формування протоколу друку документів.

Після проведення експертизи був сформований профіль захищеності системи ЛОЗА-1: КД-2, КА-2, До-0, ЦД-1, ЦА-1, ДВ-1, ДЗ-1, НР-2, НІ-3, ПК-1, АЛЕ-2, НЦ-2, НТ-2. Профіль захищеності системи ЛОЗА-1 відповідає рівню гарантії: Г-3 [2,3].

Система захисту інформації «Страж NT», (версія 3.0)

Система захисту інформації від несанкціонованого доступу "Страж NT" (версія 3.0) є комплексом засобів захисту інформації в автоматизованих системах на базі персональних комп'ютерів. СЗІ "Страж NT" призначена для комплексного захисту інформаційних ресурсів від несанкціонованого доступу під час роботи в розрахованих на велику кількість користувачів автоматизованих системах на базі персональних ЕОМ [4].

СЗІ "Страж NT" може встановлюватися на автономних робочих станціях, робочих станціях у складі робочої групи або домена, серверах, у тому числі у складі кластера. СЗІ "Страж NT" може функціонувати на одно- і багатопроцесорних комп'ютерних системах на базі архітектури x86 під управлінням 32-х розрядних операційних систем Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008 і Windows 7. Комп'ютер, на якому встановлюється СЗІ "Страж NT", повинен відповідати вимогам, необхідним для завантаження операційної системи.

У силу особливостей реалізації захисних механізмів СЗІ "Страж NT" існують додаткові вимоги до апаратного забезпечення комп'ютера :

- завантажувальний жорсткий диск повинен мати 63 сектори на доріжку і не менше 63 секторів перед початком першого розділу;
- під час використання USB-клавіатури та USB-ідентифікаторів користувачам у деяких випадках потрібна наявність не менше 2 контролерів USB;
- у разі застосування як ідентифікаторів користувачів USB флеш-накопичувачів у BIOS комп'ютера має бути включена підтримка таких пристроїв.

У СЗІ “Страж NT” реалізована змішана дозвільно-заборонна модель захисту інформації із жорстким адмініструванням. Система захисту є сукупністю таких основних підсистем:

- ідентифікації та аутентифікації;
- розмежування доступу;
- контролю потоків інформації;
- управління запуском програм;
- управління захистом;
- реєстрації подій;
- маркування документів;
- контролю цілісності;
- стирання пам’яті;
- обліку носіїв інформації;
- перетворення інформації на відчужуваних носіях;
- контролю пристроїв;
- тестування системи захисту.

Підсистема ідентифікації та аутентифікації забезпечує впізнавання користувачів при вході на комп’ютер за персональним ідентифікатором і підтвердження достовірності шляхом запиту з клавіатури особистого пароля. Ця підсистема також забезпечує блокування екрана комп’ютера та ідентифікацію користувача після такого блокування.

Підсистема розмежування доступу реалізує дискретний і мандатний принципи контролю доступу користувачів до ресурсів, що захищаються. Функціонування цієї підсистеми засноване на присвоєнні об’єктам атрибутів захисту, що захищаються. До атрибутів захисту ресурсу, що мають відношення до розмежування доступу, належать:

- ідентифікатор безпеки власника ресурсу;
- список контролю доступу;
- режим запуску (для виконуваних файлів);
- мітка конфіденційності (гриф для невиконуваного файлу або допуск для виконуваного файлу).

Дискретний принцип заснований на зіставленні повноважень користувачів і списків контролю доступу ресурсів (логічних дисків, тек, файлів, принтерів). Мандатний принцип контролю доступу реалізований шляхом зіставлення під час запита на доступ до ресурсу міток конфіденційності користувача, програми і ресурсу, що захищається. Підсистема контролю потоків інформації призначена для управління операціями над ресурсами, що мають різні мітки конфіденційності.

Підсистема запуску програм призначена для забезпечення цілісності і замкнутості програмного середовища й реалізована шляхом дозволу для виконуваних файлів режиму запуску. Якщо режим запуску програми не дозволений, то файл не є виконуваним і не може бути запущений користувачем ні за яких умов.

Підсистема реєстрації забезпечує реєстрацію запитів на доступ до ресурсів комп’ютера і можливість вибіркового ознайомлення з реєстраційною інформацією та її роздрукування.

Підсистема маркування документів забезпечує автоматичне проставляння облікових ознак у документах, що видаються на друк, а також реєстрації фактів друку документів. Підсистема контролю цілісності призначена для налаштування і періодичної перевірки параметрів цілісності системи захисту, програмного забезпечення та постійних інформаційних масивів.

Підсистема стирання пам’яті реалізує механізм заповнення нулями, що виділяються програмам областей оперативної пам’яті і стирання файлів на диску по команді вида-

лення. У рамках цієї підсистеми також реалізовано стирання файлу підкочування сторінок після закінчення сеансу роботи.

Підсистема обліку носіїв інформації дозволяє управляти доступом до носіїв інформації відповідно до дозволів і параметрів, прописаних у журналі обліку носіїв.

Підсистема перетворення інформації на зовнішніх носіях дозволяє включити додатковий захист для зовнішніх носіїв за допомогою режиму прозорого перетворення всієї інформації на носії.

Підсистема контролю пристроїв дозволяє формувати необхідну конфігурацію пристроїв для користувачів відповідно до встановлених дозволів.

Підсистема тестування системи захисту призначена для комплексного тестування основних механізмів системи захисту як на локальному комп'ютері, так і на віддаленому з використанням локальної обчислювальної мережі.

Висновки. Система захисту інформації ЛОЗА-1 має ряд переваг, які визначаються унікальністю її роботи з документами Microsoft Office: з'явилась можливість підвищити захист окремих документів, а не системи в цілому, та покращився контроль за експортом та друком важливих документів. Система ЛОЗА-1 проста у використанні і не потребує кваліфікованого персоналу, в той час як «Страж NT» має адміністратора системи безпеки, який повинен навчати персонал, а це призводить до додаткових витрат.

Система «Страж NT» має чіткі вимоги до апаратної і програмної частини, що призводить до незручностей у використанні. До того ж після запуску системи небажано встановлювати інше програмне забезпечення.

Таким чином, проведено дослідження комплексних систем захисту інформації автоматизованих систем класу «1», розглянуто їх функціональні можливості та особливості використання.

Список використаних джерел

1. Режим доступу: http://kiev.prom.ua/p314203-sistema-zaschity-informatsii.html.
2. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.
3. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.
4. «СЗИ «Страж NT» руководство администратора», ЗАО НПЦ «Модуль», 2009.

УДК 004.02

Є.В. Нікітенко, канд. фіз.-мат. наук
Чернігівський державний технологічний університет, м. Чернігів, Україна

АЛГОРИТМ АВТОМАТИЗОВАНОГО ПЛАНУВАННЯ БЕЗДРОТОВОЇ СЕНСОРНОЇ МЕРЕЖІ З ВРАХУВАННЯМ ЗАЙНЯТИХ ДІЛЯНОК ПРОСТОРУ

Досліджено методи позиціонування вузлів бездротової сенсорної мережі (БСМ). Розглянуто існуючі алгоритми планування БСМ. Запропоновано алгоритм автоматизованого планування БСМ із врахуванням ділянок, де неможливо або дуже складно розмістити вузли мережі.

Постановка проблеми. Стан електроніки та комп'ютерних технологій на сьогодні привів до широкого розповсюдження бездротових автономних пристроїв. Бездротові мережі складаються із множини вузлів, які здатні збирати дані про навколишній світ, обробляти і передавати інформацію через радіозв'язок.

Конфігурування великих мереж мініатюрних пристроїв вручну не є практичним підходом. Для цього інженерам має надаватися можливість адміністрування і програмування мережі, як єдиного цілого, за допомогою системи автоматизованого проектування.