10. Погожих, М. І. Використання методу ЕПР-спінових міток під час дослідження стану вологи в харчовій сировині [Текст] : Міжнародна науково-практична конференція, 19 травня 2011 р.: [тези: у 4 ч.]. / М. І. Погожих, А. О. Пак // Прогресивні техніка та технології харчових виробництв, ресторанного та готельного господарств і торгівлі. Економічна стратегія і перспективи розвитку сфери торгівлі та послуг. — Харків : ХДУХТ, 2011. — Ч. 2. — С. 83—84.
11. Погожих, М. І. Методика дослідження стану вологи в капілярно-пористих колоїдних тілах методом ЕПР-спінових міток [Текст] / М. І. Погожих, І. С. Ромоданов, А. О. Пак // Східно-Європейський журнал передових технологій. — 2011. — Т. 2, № 6(50). — С. 22—24.
12. Потапов, В. О. Структурно-енергетичний метод аналізу ізотерм сорбції-десорбції харчової сировини [Текст] : зб. наук. пр. / В. О. Потапов // Прогресивні техніка та технології харчових виробництв, ресторанного господарства та торгівлі. — Харків : ХДУХТ, 2005. — Вип. 1. — С. 313—322.

ИССЛЕДОВАНИЯ СИСТЕМНОЙ ВОДЫ КРАХМАЛОВ ТЕНЗОМЕТРИЧЕСКИМ И ЭПР-МЕТОДАМИ

Отмечена актуальность развития фундаментальных представлений о форме, структуре и состоянии воды в пищевых системах. Методом ЭПР-спиновых меток исследована кинетика удаления влаги из модельных тел из различных крахмалов с разной мольной концентрацией. Проведены тензометрические исследования модельных тел из различных крахмалов с разной мольной концентрацией.

Ключевые слова: системная вода, ЭПР метод, тензометрический метод.

***Погожих Микола Іванович**, доктор технічних наук, професор, завідуючий кафедри енергетики та фізики, Харківський державний університет харчування та торгівлі,*
***e-mail: drpogozhikh@mail.ru**.*

***Пак Андрій Олегович**, кандидат технічних наук, доцент, кафедра енергетики та фізики, Харківський державний університет харчування та торгівлі, **e-mail: pak_andr@mail.ru**.*
***Пак Аліна Володимирівна**, кандидат технічних наук, кафедра товарознавства в митній справі, Харківський державний університет харчування та торгівлі, **e-mail: pak_alya@mail.ru**.*
***Мольський Олександр Сергійович**, факультет обладнання та технічного сервісу, Харківський державний університет харчування та торгівлі, **e-mail: Molsky@gmail.com**.*

***Погожих Николай Иванович**, доктор технических наук, профессор, заведующий кафедрой энергетики и физики, Харьковский государственный университет питания и торговли.*
***Пак Андрей Олегович**, кандидат технических наук, доцент, кафедра энергетики и физики, Харьковский государственный университет питания и торговли.*
***Пак Алина Владимировна**, кандидат технических наук, кафедра товароведения в таможенном деле, Харьковский государственный университет питания и торговли.*
***Мольский Александр Сергеевич**, факультет оборудования и технического сервиса, Харьковский государственный университет питания и торговли.*

***Pogozhikh Micola**, Kharkiv State University of Food Technology and Trade, **e-mail: drpogozhikh@mail.ru**.*
***Pak Andrey**, Kharkiv State University of Food Technology and Trade, **e-mail: pak_andr@mail.ru**.*
***Pak Alina**, Kharkiv State University of Food Technology and Trade, **e-mail: pak_alya@mail.ru**.*
Molsky Alexander**, Kharkiv State University of Food Technology and Trade, **e-mail: Molsky@gmail.com

УДК 004.056

Петров А. О.

АНАЛІЗ НАУКОВО-ТЕОРЕТИЧНОЇ ПРОБЛЕМИ РОЗРОБКИ СИСТЕМ УПРАВЛІННЯ ЗАХИСТОМ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Розглядаються аспекти розробки систем управління захистом інформації в комп'ютерних системах та мережах. Проведено дослідження технологій, методів і засобів, що дозволяють в реальному часі оцінювати ризик порушення інформаційної безпеки в комп'ютерних мережах корпоративних інформаційних систем, а також прогнозувати рівень захисту інформації при проектуванні систем захисту інформації.

Ключові слова: *управління захистом інформації, комп'ютерні мережі, корпоративні системи, системний аналіз, прогнозування.*

1. Вступ

Наступив новий етап у розвитку обміну інформацією, що характеризується інтенсивним впровадженням сучасних інформаційних технологій, широким розповсюдженням комп'ютерних мереж, та створює нові можливості та якість інформаційного обміну [1].

Корпоративні інформаційні системи (КІС) стають сьогодні одним з головних інструментів управління бізнесом, найважливішим засобом виробництва сучасного підприємства, використовуються в банківській, фінансовій сферах, у сфері державного управління. КІС включає в себе інфраструктуру та інформаційні сервіси.

Однак застосування інформаційних технологій неможливе без підвищеної уваги до питань інформаційної безпеки через наявність загроз захищеності інформації [2].

Для сучасного етапу розвитку теорії та практики забезпечення захисту інформації (ЗІ) характерна наступна

суперечлива ситуація: з одного боку, посилена увага до безпеки інформаційних об'єктів, істотне підвищення вимог щодо ЗІ, прийняття міжнародних стандартів у галузі інформаційної безпеки (ІБ), постійно зростаючі витрати на забезпечення захисту, з іншого — настільки ж неухильно зростаючий збиток, що заподіюється власникам інформаційних ресурсів, про що свідчать опубліковані регулярно дані про збитки світовій економіці від комп'ютерних атак [3—5].

Очевидно, що сучасні підходи до організації ЗІ не в повній мірі забезпечують виконання вимог щодо захисту інформації. Основні недоліки систем захисту інформації (СЗІ) визначаються сформованими жорсткими принципами побудови архітектури і застосуванням в основному оборонної стратегії захисту від відомих загроз. Критична ситуація у сфері ІБ посилюється у зв'язку з використанням глобальної мережі для зовнішніх і внутрішніх електронних транзакцій підприємства і постійною наявністю невідомих раніше типів деструктивних інформаційних впливів.

Тому для успішного використання сучасних інформаційних технологій необхідно ефективно управляти не тільки мережею, але і СЗІ, при цьому на рівні комп'ютерної мережі КІС автономно повинна працювати система, що реалізує управління складом подій інформаційної безпеки, планування модульного складу СЗІ та аудит. Оскільки об'єкт управління — СЗІ є досить складною організаційно-технічною системою, що функціонує в умовах невизначеності, суперечливості та неповноти знань про стан інформаційного середовища, управління такою системою повинне бути засноване на застосуванні системного аналізу, методів теорії прийняття рішень та необхідної інтелектуальної підтримки.

Разом з тим в області розробки методів захисту інформації в даний час практично відсутні дослідження, спрямовані на забезпечення автоматизованої підтримки управління ЗІ для вирішення проблеми забезпечення необхідного рівня захищеності інформації протягом усього періоду функціонування СЗІ.

Постійна розробка нових методів і засобів спеціальних програмно-технічних впливів призводить до тенденції постійного зростання кількості випадків успішної реалізації атак [6].

Ускладнення сучасних ІС веде до появи в них все більшої кількості мережевих пристроїв і різноманітних засобів захисту (ЗЗ) інформації, які генерують величезне число подій безпеки: десятки, а то й сотні тисяч повідомлень в день [7], розібратися в яких адміністратору безпеки фізично неможливо. Один міжмережевий екран може за день згенерувати більше 1 Гігабайта даних, сенсор система виявлення аномалій — до 50 тисяч повідомлень, причому з них до 95 % помилкових [8]. Крім того, порівняти сигнали про події безпеки від різних систем практично неможливо; в той же час, дії у відповідь на атаки повинні бути негайними.

2. Постановка проблеми у загальному вигляді та її зв'язок з важливими науковими та практичними завданнями

Очевидно, що технологічний процес істотно випереджує теоретичне осмислення того, що відбувається в області створення і застосування інформаційних технологій і використання нових комунікаційних можливостей. Отже, є підстави зробити припущення про неповну адекватність докладених зусиль при вирішенні існуючих завдань захисту інформації не тільки в практичному, але і в теоретичному аспекті [9].

Основні недоліки систем захисту інформації визначаються сформованими жорсткими принципами побудови архітектури [10] і застосуванням в основному оборонної або наступальної стратегії захисту від відомих і найбільш небезпечних загроз.

Для вирішення сформульованої вище проблеми і успішного використання сучасних інформаційних технологій необхідне ефективне і надійне управління не тільки мережами, але і системою захисту інформації, засобами мережевої безпеки [2, 12].

Таким чином, на сьогодні на перший план виходить завдання створення комплексної системи управління засобами мережної безпеки, яка охоплює всю інфраструктуру компанії і, незалежно від масштабу КІС дозволяє надавати керуючі впливи на інформаційну інфраструктуру.

3. Аналіз досліджень і публікацій, мета роботи

Масштаби, застосування інформаційних технологій і проблема захисту від несанкцыонованого доступу до циркулюючої в КІС інформації викликає зростання інтересу до теоретичних досліджень в області інформаційної безпеки [6, 21—25]. Основам комп'ютерної безпеки присвячені роботи [16, 22, 25]. У працях дослідників в області інформаційної безпеки, у статтях та монографіях обговорюються проблеми криптографії [16—18]; криптографічні методи і засоби отримали швидке і широке поширення. Проблема виявлення вторгнень розглядається в [13, 15, 19—23].

Як наголошується в ряді робіт [10—15], генеральним напрямком пошуку шляхів підвищення ефективності захисту інформації є неухильне підвищення системного підходу до проблеми захисту інформації, пізнання суті досліджуваної проблеми, декомпозиція СЗІ на підсистеми, виявлення всього різноманіття факторів і зв'язків, встановлення повного переліку загроз, що впливають на ІС, розробка і застосування якісних і кількісних показників, що характеризують СЗІ; створення засобів розв'язання наявних протиріч.

Відзначається, що для ефективного забезпечення, безпеці інформації потрібне проведення досліджень, пов'язаних з адаптивною організацією СЗІ, створення методологічного базису, що дозволяє вирішувати проблему управління захистом інформації та її автоматизації [11—29].

Одним з перших, хто став розглядати завдання управління ЗІ, був Герасименко В. А. Як пише автор у своїй роботі [17], основою для управління ЗІ служать плати обробки інформації на об'єкті захисту, а на основі аналізу критичності обробки інформації обґрунтовуються вимоги до захисту. Виходячи з цих вимог, визначаються оптимальні набори засобів захисту, що забезпечують необхідний рівень захищеності. Відзначається, що обґрунтування таких наборів СРЗ є спільним завданням механізмів управління ЗІ; для визначення дійсного рівня захищеності повинен здійснюватися відповідний контроль. Питання управління безпекою інформації розглядаються в [11], питання проектування СЗІ розглядаються

в [17]. На сьогодні існують два основні підходи до побудови системи захисту: продуктний і проектний [24]. У рамках продуктного підходу проводиться вибір засобів захисту інформації, з подальшим формуванням політики безпеки на основі реалізованих вибраними засобами захисту функцій. У рамках проектного підходу проводиться спочатку формування політики безпеки і далі на її основі здійснюється вибір засобів захисту. Як зазначається в [24], проектний підхід більш повний, системи, побудовані на його основі, більш оптимізовані, він більше підходить для гетерогенних мереж і дозволяє проектувати більш довготривалі рішення. У [18, 19] наводиться загальна методика вибору засобів захисту при використанні критерію оптимальності по мінімуму витрат, при заданій ефективності захисту. Методика заснована на оцінці ефективності виконання засобами захисту різних функцій. У [17] зазначається, що даний розрахунок ускладнений таким фактором, як складність виділення кількісного показника безпеки інформації; тому пропонується вибирати засоби захисту виходячи з вимог захисту. Аналогічний підхід пропонується в методиках, заснованих на стандартах. У роботах [11, 13] до основних макропроцесів управління віднесені оперативне управління та стратегічне планування використання засобів захисту. Оперативне управління — це динамічне управління в ході автоматизованої обробки інформації, коли використовуються лише засоби захисту, що входять до складу СЗІ.

У процесі оперативного управління здійснюється безперервне розпізнавання ситуацій, що відносяться до захисту інформації, та прийняття рішень на оперативне втручання у функціонування СЗІ, реалізація прийнятих рішень. Завдання прийняття рішень, на думку автора [51], може зводитися до вибору деякого рішення з наперед сформованої безлічі невеликого числа рішень.

Планування — процес вироблення програми оптимального використання засобів захисту в плановий період обробки інформації. При цьому під оптимальністю розуміється досягнення максимальної захищеності при заданих витратах на захист або досягнення заданої захищеності при мінімальних витратах. У рамках розгляду завдань управління ЗІ зазначається, що проблема прийняття рішень є однією з найбільш складних і особливо важливою для автоматизації управління ЗІ.

Робота [20] присвячена розробці основ організаційного управління ЗІ. Автор зазначає, що реалізація зростаючих вимог до захищеності інформації в складних ІС стримується на сьогодні через відсутність відповідного науково-технічного забезпечення, що враховує як динаміку управління стратегіями інформаційного протиборства, так і динаміку середовища, в якому це протиборство здійснюється. На даний час концептуальний підхід до захисту інформації носить вступний характер і потребує конкретизації стосовно складних розподілених ІС, з урахуванням реальних процесів інформаційного протиборства. При цьому стримуючим фактором у становленні теорії організаційного управління ЗІ і використанні її результатів на практиці є відсутність системних науково-методичних досліджень.

У роботах [13, 14] наводиться формалізований опис методів синтезу оптимальних стратегій організаційного управління ЗІ в ігрових моделях прийняття рішень, а також управління квантуванням пакетів, при передачі категорованої інформації, управління відновленням цілісності інформації (алгоритм вибору оптимальної стратегії резервування), методи оцінювання захищеності інформації в умовах впливу вірусних програм.

У роботі [15] управління розглядається в основному як організаційне. Завдання управління вирішуються адміністративною групою: адміністратор безпеки, менеджер безпеки і оператори. Поняття управління ЗІ визначається як контроль за розподілом інформації в ІС, забезпечення функціонування засобів і механізмів захисту, фіксація виконуваних функцій, фіксація подій, пов'язаних з порушенням захисту, періодичне внесення змін до бази даних захисту.

Основні науково-теоретичні проблеми синтезу адаптованих систем забезпечення інформаційної безпеки та їх застосування в корпоративних інформаційних системах розглядаються в роботах [6, 7, 10, 19]. У роботі [22] розглядаються принципи синтезу систем забезпечення ІБ, які закладають основу для автоматизації циклу забезпечення ІБ, адаптуючи систему до всіляких штатних і нештатних ситуацій. У роботі [7] наводиться багатокритеріальна модель оцінки і метод вибору мережевих екранів на основі непарних множин, синтез підсистем аналізу захищеності і виявлення загроз, ігровий метод прийняття рішень по боротьбі із загрозами.

Проблемі адаптивного управління процесами захисту інформації в автоматизованих системах присвячені роботи [24, 25], в яких наводяться результати розробки підсистеми адаптивного управління ЗІ, що використовує в основному контурі неявну модель налаштування об'єкта управління, приводиться метод визначення раціонального складу і структури СЗІ на етапі проектування, заснований на теоремі про мінімакс, що використовує безрозмірний показник ступеня досяжності варіантом СЗІ характеристик «еталонної» системи захисту, метод зміни структури і модифікації СЗІ в процесі експлуатації, що використовує критерій максимуму приросту показника захищеності в умовах вартісних обмежень. Слід зазначити складність формування «еталонної» системи захисту на різних етапах життєвого циклу СЗІ.

Метою статты є аналіз методологічних основ управління захистом інформації корпоративної інформаційної системи для вирішення науково-практичної проблеми забезпечення необхідного рівня захищеності інформації протягом життєвого циклу системи захисту інформації в умовах невизначеності інформаційних впливів з використанням методів оцінки ІБ.

4. Основна частина, результати

Ефективність системи оперативного управління ЗІ багато в чому залежить від застосовуваних методів аналізу отриманої інформації, для ідентифікації атаки і методів прийняття рішень з управління подіями безпеки.

Відомо, що в подібних системах використовуються наступні методи ідентифікації атак: статистичний метод експертних систем, нейромережевий.

Основна перевага статистичного методу — це використання добре розробленого апарата математичної статистики і його адаптація: до поведінки інформаційного суб'єкта. При використанні цього методу для всіх суб'єктів системи визначаються профілі. Будь-яке відхилення профілю від еталонного вважається несанкціонованою діяльністю. Статистичні методи універсальні, для проведення аналізу не потрібні знання про можливі

атаки, проте при їх використанні дуже важко задати граничні значення, що відслідковують характеристики, щоб адекватно ідентифікувати аномальну діяльність; вони непридатні до невідомих раніше атак.

Експертна система складається з набору правил, які охоплюють знання експерта. Використання експертних систем являє собою поширений метод ідентифікації атак, при якому інформація про атаки формується у вигляді правил. Ці правила можуть бути записані у вигляді послідовності дій. При виконанні правила приймається рішення про наявність несанкціонованої діяльності. База даних повинна містити сценарії більшості відомих на сьогодні атак, а також вимагає постійного оновлення. Перевагою такого підходу є практично повна відсутність помилок. З недоліків основним є неможливість відображення невідомих атак. При цьому навіть невелика зміна вже відомої атаки може стати серйозною перешкодою для функціонування системи.

Більшість сучасних методів виявлення атак використовують форму аналізу контрольованого простору на основі правил або статистичного підходу. Через велику різноманітність атак і їх методів навіть постійні оновлення бази даних правил експертної системи не дають гарантії точної ідентифікації всього діапазону атак.

Кожен з описаних методів володіє перевагами і недоліками. Загальний недолік полягає в тому, що системи управління ЗІ, в яких реалізовані описані технології та методи ідентифікації атак, є продуктами зарубіжних компаній, вони запатентовані, коди їх програм невідомі; методи прийняття рішень по формуванню командної інформації також невідомі.

Зазначимо, що методичні та технологічні основи створення інтелектуальних засобів попередження комп'ютерних атак в КІС поки знаходяться в початковій стадії розвитку. На сьогодні потрібні комплексні рішення і практична реалізація засобів оцінки підозрілої активності та різних подій у мережі, підготовки даних для прийняття рішень по управлінню засобами безпеки та мережевим обладнанням для своєчасного реагування на мінливі умови середовища функціонування в режимі реального часу.

При створенні інфраструктури КІС на базі сучасних комп'ютерних мереж неминуче виникає питання про захищеність цієї інфраструктури від загроз безпеки інформації. Ці питання на сьогодні розглядаються значним числом авторів [1—28].

Вибір формалізованих заходів (критеріїв) оцінки рівня захищеності відноситься до числа концептуальних завдань створення захищених систем. Формалізованими заходами зазвичай називають способи оцінки «сили» яких-небудь характеристик реальних систем, які засновані на використанні числових шкал — використання критеріїв оцінки рівня захищеності, яка вперше була запропонована в Помаранчевій книзі стосовно операційних систем і СУБД.

При наявності шкали порівняння систем зводиться до порівняння відповідних їм числових показників. Криптографія та радіоелектронна захист володіють такими заходами, що не можна сказати про область ЗІ від несанкцыонованого доступу (НСД).

Теоретично формальну оцінку рівня захищеності системи від НСД можна звести до обчислення інтенсивності атак на систему, ймовірності реалізації атаки в заданий проміжок часу і т. д. Однак подібні апостеріорні критерії мають низьку практичну цінність, так як для оцінки ймовірності характеристик реальних атак необхідно враховувати складний комплекс факторів: технологію обробки даних, умови застосування систем, кваліфікацію користувачів і т. д. Більше того, повний перелік атак на систему неможливо навіть точно визначити. Апостеріорні критерії представляють, в основному, академічний інтерес.

Для практичної оцінки рівня захищеності систем слід використовувати апріорні критерії. Вони засновані на зіставленні системи з набором еталонних профілів сервісів захисту, що забезпечують при певних умовах деякий рівень безпеки інформації. Якщо системи А і В мають однакові рівні захищеності, то вони реалізують однаковий набір механізмів захисту та всі механізми мають однакову «силу». Система А домінує за рівнем захищеності, якщо системою А реалізуються механізми, відсутні в системі В, або «сила», принаймні, одного з механізмів у системі А, вища, ніж для аналогічного механізму системи В.

З викладеного випливає, що загальний показник захищеності інформації для ресурсу інформаційної системи (ІС) в цілому може бути отриманий із значень приватних ймовірностей успішності різних загроз. Разом з тим, в даній роботі не розкривається детально методика визначення рівня захищеності, фактично, в ній міститься тільки загальна постановка задачі розробки такої методики, яка ще вимагає свого рішення.

На сьогодні поширення набули підходи до аналізу ризиків, органічно пов'язані з рівнем захищеності. Фактично, знаючи ризики, можна визначити рівень захищеності системи, і навпаки. Наявність системи керування ризиками порушення інформаційної безпеки є обов'язковою умовою організації режиму ІБ на підприємстві.

Основоположними роботами, присвяченими дослідженню питання управління ризиками, є [13, 17], відповідно до яких аналіз ризиків рекомендується проводити у випадках:

— поновлення КІС або істотних змін у її структурі;
— переходу на нові ІТ побудови КІС;
— організації нових підключень в компанії; підключення до глобальних мереж;
— зміни в стратегії і тактиці ведення бізнесу; перевірки ефективності СЗІ.

У даних роботах наводяться наступні етапи управління ризиками: оцінка можливих втрат; аналіз потенційних загроз і вразливих місць системи, які впливають на оцінки можливих втрат; вибір оптимальних за ціною заходів і засобів захисту, які скорочують ризик до прийнятного рівня.

При розгляді кожного з цих етапів більш детально наводиться список дій, які повинні бути виконані для їх реалізації, тобто по суті, пропонується послідовність необхідних дій, реалізація яких може бути можлива при використанні спеціальних засобів аналізу ризику.

Під «управлінням ризиками» будемо розуміти вибір комплексу необхідних контрзаходів, що забезпечують достатній рівень захищеності ІС відповідно до виконаних аналізом ризиків. На всіх стадіях життєвого циклу ІС при виробленні рекомендацій щодо управління ризиками має бути запропонований комплекс адекватних контрзаходів по окремим аспектам безпеки: внесення змін в політику ІБ; зміни в посадових інструкціях

і регламентах обслуговування; застосування додаткових програмно-технічних засобів захисту.

При оцінюванні ризиків повинні враховуватися такі фактори, як: цінність ресурсів, оцінка значимості загроз, вразливостей, ефективність існуючих і планованих СРЗ. Якісно виконаний аналіз ризиків повинен дозволити провести порівняльну оцінку різних варіантів захисту, що особливо важливо, коли до ІС пред'являються підвищені вимоги в області ІБ.

У міжнародному стандарті ISO/IEC 15408 «Загальні критерії оцінки безпеки ІТ» вимоги по ІБ добре структуровані і сформульовані для великого числа класів ІС. З практичної точки зору, істотним є те, що в документі формулюються тільки критерії оцінки і не містяться методики її проведення.

Аналіз зарубіжних і сучасних вітчизняних стандартів в області управління ризиками ІБ показав, що положення описаних вище стандартів не містять важливих деталей, які необхідно конкретизувати на практиці, і їх успішне застосування для управління ризиками вимагає додаткових методик оцінювання, враховують різні кількісні та якісні показники [20—28].

Відзначимо, що проблема створення наукової методології забезпечення заданого рівня захищеності протягом усього періоду експлуатації ІС є важливою і актуальною. Рішення проблеми забезпечення заданого рівня захищеності пов'язано з послідовним вирішенням двох приватних завдань:

— кількісного оцінювання рівня захищеності;
— прийняття рішення про необхідність зміни властивостей і параметрів СЗІ з метою підтримки заданого рівня захищеності.

Необхідність отримання кількісних значень рівня захищеності інформації викликана тим, що для прийняття обґрунтованого рішення про необхідність проведення заходів по ЗІ потрібен аналіз динаміки зміни рівня захищеності ІС в залежності від зміни як умов функціонування, так і параметрів СЗІ.

Інструментальні засоби оцінки рівня захищеності (ризиків порушення ІБ) повинні бути засновані на сучасних базах даних і знань в області ЗІ, дозволяти будувати структурні об'єктно-орієнтовані моделі ІС, а також моделі ризиків окремих сегментів КІС. Рішення проблеми забезпечення заданого рівня захищеності пов'язано з послідовним вирішенням двох приватних завдань: кількісного оцінювання рівня захищеності та автоматизованого прийняття рішення про необхідність перерозподілу ресурсів або зміни параметрів СЗІ.

Враховуючи, що ІС є досить складним технічним об'єктом, а процес захисту інформації характеризується великою кількістю і різноманіттям факторів, що впливають на його результат, вплив яких часто не вдається однозначно виявити і описати строго математично, проблема захисту інформації відноситься до числа складних слабоструктурованих і слабосформульованих проблем.

У науці є досвід щодо вирішення слабосформульованих проблем — це системний підхід до їх вирішення та системний аналіз об'єктів дослідження. У системному аналізі акцентується увага на труднощах формулювань завдань, на способах подолання цих труднощів. З практичної сторони системний аналіз є теорія і практика поліпшуючого втручання в проблемну ситуацію. Застосування методів системного аналізу до дослідження проблеми ЗІ диктується вимогами практики, яка поставила фахівців із захисту інформації перед необхідністю проектувати складні системи захисту інформації, вивчати процеси, управляти ними в умовах невизначеності, неповноти інформації, дефіциту часу і обмеженості ресурсів. Специфічною особливістю існуючих на даний момент методик системного аналізу є те, що вони використовують закономірності побудови, функціонування і розвитку систем, формування варіантів структури системи і вибір найкращого варіанта. Методи системного аналізу — декомпозиція, аналіз і синтез системи, що знімає або ослаблює проблему практики.

Отже, перший етап системного аналізу пов'язаний з формулюванням проблеми. Необхідність системного аналізу виникає, коли проблема не тільки існує, але і вимагає вирішення.

У системному аналізі систему, в діяльності якої проявилася проблема, називають проблемомістка. У даному випадку це система захисту інформації. Проблемомістка СЗІ пов'язана з іншими системами і входить як частина в деяку надсистему. Сама СЗІ в свою чергу складається з частин-підсистем, причетних до даної проблеми.

Застосування системного підходу до вирішення проблеми забезпечення повноти та ефективності реалізації функцій СЗІ на різних етапах її життєвого циклу викликає необхідність розробки керуючої системи, покликаної не тільки забезпечити раціональні ресурсні, фінансові та часові характеристики, але і підвищити ступінь наукової обгрунтованості та оперативності прийнятих управлінських рішень. При цьому проектування, модернізація і забезпечення ефективного функціонування СЗІ є нетривіальними завданнями. Очевидно, що й керування ЗІ так само не є тривіальною задачею.

Модель проблемної ситуації в ЗІ містить сукупність трьох взаємодіючих систем: проблемомісткої системи — СЗІ; проблемовирішуючої системи, тобто системи, яка розробляється для того, щоб вплинути на процеси захисту інформації таким чином, щоб проблема зникла або ослабла; навколишнього, або істотного середовища, з якою взаємодіє СЗІ.

У відповідності з методом декомпозиції системного аналізу стосовно проблеми ЗІ наведемо модель входів СЗІ в КІС, яка включає входи: від вищестоящої системи (головної організації, установи, підприємства), від нижчестоящих систем (філій), від істотного середовища, від проблемовирішуючої керуючої системи (рис. 1).

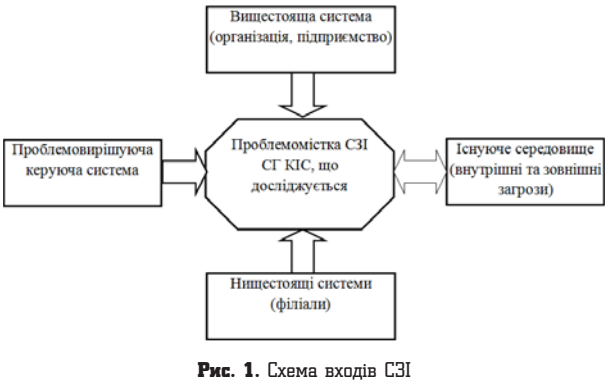

Рис. 1. Схема входів СЗІ

Проблемомістка СЗІ є об'єктом дослідження, а в якості цільової виступає керуюча проблемовирішуюча система. Дана модель дозволяє не тільки підвищити повноту набору цілей, але й структурувати їх сукупність, що

згодом дозволить здійснити постановку задач прийняття раціональних рішень з управління ЗІ.

Метою вищестоящої системи: організації, державного чи комерційного підприємства, — є підвищення ефективності процесу інформатизації, яка на сьогодні недостатня через щорічний збиток від злочинів у сфері ІТ, вчинених з використанням засобів обчислювальної техніки.

Для проблемомісткої системи головне — вирішити проблему, цілі проблемовирішуючої системи пов'язані з раціональним витрачанням ресурсів на вирішення проблеми. Цілі істотного середовища та СЗІ протилежні.

Спільною метою захисту інформації є запобігання або зниження шкоди, що завдається власнику, власнику чи користувачу системи внаслідок реалізації загроз безпеки інформації. Приватними цілями захисту інформації, що забезпечують досягнення загальної мети, є:

— забезпечення правового режиму використання масивів, даних і програм обробки інформації;

— запобігання несанкціонованого знищення, спотворення, копіювання інформації, блокування доступу до інформації;

— збереження можливості управління процесом обробки та використання інформації в умовах несанкціонованих (програмно-технічних) впливів на інформацію, що захищається.

— запобігання витоку інформації технічними каналами.

Таким чином, існує необхідність вирішення проблеми забезпечення заданого рівня захищеності, яка пов'язана з послідовним вирішенням двох приватних завдань: кількісного оцінювання рівня захищеності та автоматизованого прийняття рішення про необхідність перерозподілу ресурсів СЗІ або зміни властивостей і параметрів з метою підтримки заданого рівня захищеності інформації.

Тому показником ефективності досягнення мети ЗІ будемо вважати рівень захищеності інформації (φ) на об'єкті захисту, або відносний ризик порушення інформаційної безпеки (R). Значення j задається замовником залежно від максимального рівня критичності оброблюваної на об'єкті захисту інформації, і може приймати значення від 0,9 до 1. Час актуальності мети визначається планами обробки інформації на об'єкті захисту. У практиці системного аналізу в якості глобального об'єкта декомпозиції береться досліджувана проблема і проблемомістка система. В якості підстав декомпозиції беруться моделі проблемовирішуючої системи. Для цілей аналізу проблеми захисту інформації необхідна модель СЗІ. В якості фрейма для неї можна використовувати модель діяльності, надавши відповідну інтерпретацію компонентам, які входять до моделі (рис. 2).

Для аналізу процесів ЗІ необхідні моделі, які деталізують компоненти: об'єкт захисту, середовище, комплекс засобів захисту. Метод декомпозиції є одним із способів спрощення складної СЗІ. Він полягає в постійно наростаючій деталізації базових моделей системи захисту, в розкладанні складного цілого на все більш дрібні та прості частини. Після розробки фреймової моделі необхідно у відповідності з методом декомпозиції системного аналізу здійснити багаторівневий процес від початкової декомпозиції (рис. 2) до завершального рівня.

Застосування технології системного проектування до побудови моделі керуючої системи дозволить визначити її підсистеми, компоненти і способи їх з'єднання, задати обмеження, при яких система повинна функціонувати, вибрати найбільш ефективне поєднання людей (експертів, спеціалістів ІБ, аналітиків), ЕОМ і програмного забезпечення.

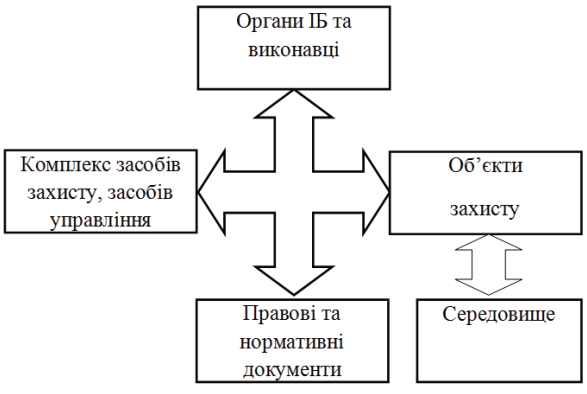

Рис. 2. Схема компонент СЗІ

Модель входів організаційно-технічної системи рекомендує визначити, що розуміти під терміном «істотне середовище». Функціонування СЗІ пов'язано з процесами інформаційного протиборства, спрямоване на протидію зовнішнім і внутрішнім загрозам. Тому в даному випадку під істотним середовищем розуміється безліч потенційно можливих загроз інформаційному середовищу СГ КІС, зовнішніх і внутрішніх.

Таким чином, рішення актуальної наукової-технічної проблеми управління СЗІ в КІС пов'язано з необхідністю розробки комплексу науково-обґрунтованих і практично-застосовних методів і методологій в рамках створення теорії інтелектуального забезпечення безпеки.

5. Висновки

1. Незважаючи на інтенсивні дослідження в області розробки методів і систем захисту інформації, на сьогодні практично відсутні наукові публікації про результати теоретичних досліджень зі створення методології побудови інтелектуальних засобів підтримки прийняття рішень з управління захистом інформації, що потребує комплексного вирішення низки наукових завдань, спрямованих на створення науково обгрунтованих і практично застосовних моделей і методів теорії інтелектуального забезпечення управління процесами захисту інформації на основі системного аналізу.

2. Суть управління ЗІ полягає в ухваленні рішення на вироблення стратегії захисту на всіх етапах життєвого циклу СЗІ. Зростаючі вимоги щодо розроблення та впровадження технології управління ЗІ суперечать існуючому на сьогодні стану нормативно-методичної бази, яка не дозволяє адекватно вирішувати завдання вибору раціонального модульного складу СЗІ. Існуючі керівні документи і стандарти визначають функціональні вимоги відносно засобів захисту і не пропонують методик порівняльного аналізу різних наборів засобів захисту інформації, сертифікованих за одним класом, з метою виявлення найбільш раціонального цілісного варіанту СЗІ.

3. Найбільш перспективними на сьогодні є дослідження та розробка технологій, методів і засобів, що дозволяють в реальному часі оцінювати ризик порушення

інформаційної безпеки в комп'ютерних мережах КІС, а також прогнозувати рівень захисту інформації при проектуванні СЗІ. При цьому показник рівня захисту повинен формуватися з мінімальним залученням експертів на основі відомостей про інформаційну цінність ресурсів, що потребують захисту, даних про технічні характеристики застосовуваних або планованих засобів захисту, з урахуванням безлічі реальних загроз і особливостей функціонування конкретного об'єкта захисту.

4. Одна з основних проблем створення систем управління ЗІ — забезпечення автоматизованої підтримки прийняття рішень з управління захистом інформації протягом усього періоду функціонування інформаційної системи і при зміні умов інформаційного середовища, що викликає потребу в інфраструктурному програмному забезпеченні, в якому повинні бути реалізовані моделі та математичні методи прийняття рішень. Інструментальні програмні комплекси, що використовують можливості комп'ютерів для реалізації результатів досліджень у вигляді моделей, дозволять підвищити точність і ефективність прийняття рішень, реалізувати інтелектуальний потенціал особи, що приймає рішення, оскільки процес прийняття рішень будується на основі аналізу і прогнозу із застосуванням математичного апарату.

Література

1. Смирнов, А. К. Информационная глобализация: вызовы и возможности [Текст] / А. К. Смирнов. — М. : Издательский дом «Парад», 2005. — 392 с.
2. Галицкий, А. В. Защита информации в сети — анализ технологий и синтез решений [Текст] / А. В. Галицкий, С. Д. Рябко, В. Ф. Шаньгин. — М. : ДМК Пресс, 2011. — 616 с.
3. Тихонов, В. А. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты [Текст] : учебное пособие / В. А. Тихонов, В. В. Райх. — М. : Гелиос АРВ, 2006. — 528 с.
4. Доктрина інформаційної безпеки України. Затверджено Указом Президента України від 8 липня 2009 року № 514/2009.
5. Бородакий, Ю. В. Интеллектуальные системы обеспечения информационной безопасности [Текст] : материалы конф. / Ю. В. Бородакий, Г. В. Куликов // VII Междунар. научно-практич. конф. — Известия ТРТУ. Тематический выпуск. — Таганрог: ТРТУ, 2009. — С. 32—33.
6. Шишкин, В. М. К проблеме экспертизы безопасности сложных информационных систем [Текст] : материалы конф. / В. М. Шишкин // Международ, научно-практич. конф. «Информационная безопасность». — Таганрог: ТРТУ. 2011. — С. 15—18.
7. Бородакий Ю. В. Интеллектуальные системы обеспечения информационной безопасности [Текст] : материалы конф. // Известия ТРТУ. Тематический выпуск. — Таганрог: ТРТУ. — 2010. — № 4. — С. 65—69.
8. Остапенко, А. Г. Противодействие вредоносному программному обеспечению в информационно-телекоммуникационных системах [Текст] / А. Г. Остапенко, С. В. Скрыль, А. Г. Остапенко, С. В. Скрыль // Информация и безопасность. — 2000. — № 2. — С. 91—92. — Режим доступа: \www/ URL: http://www.technoserv.ru.
9. Девянин, П. Н. Теоретические основы компьютерной безопасности. [Текст] / П. Н. Девянин. — М. : Радио и связь, 2010. — 304 с.
10. ДСТУ 3396.2-97 — «Защита информации. Техническая защита информации. Термины и определения».
11. Гордейчик, С. В. Сравнительный анализ сканеров безопасности [Электронный ресурс] / С. В. Гордейчик, В. Б. Лепихин // Часть 2. Функциональные возможности сканеров безопасности. — Режим доступа: \www/ URL: http://www.ptsecurity.ru/download/SecScanFN.zip.
12. Гордейчик, С. В. Безопасность беспроводных сетей [Текст] / С. В. Гордейчик, В. В. Дубровин. — М. : Горячая линия-Телеком, 2008. — 288 с.
13. ГОСТ 50922-96. Защита информации. Основные термины и определения. — Режим доступа: \www/ URL: http://just.siberia.net/50922_96.htm.
14. Джон Грин. Защита сети при помощи программной NAC-технологии. Четыре продукта предлагают разные подходы [Текст] / Джон Грин // Windows IT Pro. — 2007. — № 7.
15. Кузнецов, Н. А. Информационная безопасность систем организационного управления. Теоретические основы. — 2 т. [Текст] / Н. А. Кузнецов, В. В. Кульба, Е. А. Микрин. — М. : Наука, 2006.
16. Лукацкий, А. В. Обнаружение атак [Текст] / А. В. Лукацкий. — СПб.: БХВ — Петербург, 2009. — 608 с.
17. Герасименко, В. А. Сущность и пути перевода процессов защиты информации на интенсивные способы [Текст] / В. А. Герасименко, А. А. Малюк // Безопасность информационных технологий. — 1998. — № 4.
18. Скиба, В. Ю. Руководство по защите от внутренних угроз информационной безопасности [Текст] / В. Ю. Скиба, В. А. Курбатов. — СПб.: Питер, 2008. — 320 с.
19. Климов, С. М. Методы и интеллектуальные средства предупреждения и обнаружения компьютерных атак на критически важные сегменты информационно-телекоммуникационных систем [Текст] : материалы конф. / С. М. Климов // Международ, научно-практич. конф. «Информационная безопасность». — Известия ТРТУ. — 2009. — № 4(48). — С. 74—82.
20. Симонов, С. В. Анализ рисков в информационных системах. Практические советы [Текст] / С. В. Симонов // Конфидент. — 2011. — № 2.
21. Алгулиев, Р. М. Методы синтеза адаптивных систем обеспечения информационной безопасности корпоративных [Текст] / Р. М. Алгулиев. — М. : УРСС, 2001. — 248 с.
22. Бабенко, Л. К. Новые технологии электронного бизнеса и безопасности [Текст] Л. К. Бабенко, В. А. Быков, О. Б. Макаревич, О. Б. Спиридонов. — М. : Гелиос АРВ, 2011. —374 с.
23. Воробьев, А. А. Теоретико-игровой подход к оцениванию качества системы защиты информации от несанкционированного доступа в АС [Текст] / А. А. Воробьев // Информатика-машиностроение. — 2009. — № 3. — С. 12—17.
24. Доценко, С. М. Аналитические информационные технологии и обеспечение безопасности корпоративных сетей [Текст] / С. М. Доценко // Конфидент. — 2010. — № 2. — С. 16—21. — Режим доступа: \www/ URL: http://www.confident.ru.
25. Остапенко, А. Г. Противодействие вредоносному программному обеспечению в информационно-телекоммуникационных системах [Текст] / А. Г. Остапенко, С. В. Скрыль, А. Г. Остапенко, С. В. Скрыль // Информация и безопасность. — 2010. — № 2. — С. 91—92.
26. Нестеренко, В. А. Статистические методы обнаружения нарушений безопасности в сети [Текст] / В. А. Нестеренко // Информационные процессы. — 2006. — т. 6. — Вып. 3. — С. 208—217.
27. Симонов, С.В. Анализ рисков, управление рисками / У СП «Компьюлинк» [Электронный ресурс]. — Режим доступа: \www/ URL: http://www.compulink.ru.
28. Тарасюк, М. В. Защищенные информационные технологии. Проектирование и применение [Текст] / М. В. Тарасюк. — М. : СОЛОН — Пресс, 2004. — 192 с.

ISSN 2226-3780

АНАЛИЗ НАУЧНО-ТЕОРЕТИЧЕСКОЙ ПРОБЛЕМЫ РАЗРАБОТКИ СИСТЕМ УПРАВЛЕНИЯ ЗАЩИТОЙ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ И СЕТЯХ

Рассматриваются аспекты разработки систем управления защитой информации в компьютерных системах и сетях. Проведены исследования технологий, методов и средств, позволяющих в реальном времени оценивать риск нарушения информационной безопасности в компьютерных сетях корпоративных информационных систем, а также прогнозировать уровень защиты информации при проектировании систем защиты информации.

Ключевые слова: управление защитой информации, компьютерные сети, корпоративные системы, системный анализ, прогнозирование.

***Петров Антон Олександрович**, кандидат технічних наук, доцент кафедри безпеки інформаційних систем, Східноукраїнський національний університет ім. В. Даля, **e-mail: antonpv@mail.ru**.*

***Петров Антон Александрович**, кандидат технических наук, доцент кафедри безопасности информационных систем, Восточноукраинский национальный университет им. В. Даля.*

Petrov Anton**, Volodymyr Dahl East Ukrainian National University, **e-mail: antonpv@mail.ru

УДК 004

Новоселов С. П.,
Рак Е. В.

МЕТОД ПОСТРОЕНИЯ ТАБЛИЦЫ МАРШРУТИЗАЦИИ ДЛЯ БЕСПРОВОДНОЙ СЕНСОРНОЙ СЕТИ

В работе описывается предлагаемый алгоритм маршрутизации для беспроводной сенсорной сети, а также результаты исследований, проведенных с использованием разработанных интеллектуальных датчиков (компонентов сенсорной сети). Предложенное решение может быть реализовано для построения сенсорных сетей с числом компонентов до 32 устройств, построенных на недорогих микроконтроллерах с малым объемом памяти программ и данных.

Ключевые слова: *сенсорная сеть, датчик, алгоритм, таблица маршрутизации.*

1. Введение

В настоящее время беспроводные сенсорные сети находят все большее применение в системах промышленной автоматизации для решения задач мониторинга и управления. Их основным достоинством является гибкая архитектура и минимальные затраты при их установке и эксплуатации.

Важной особенностью беспроводных сенсорных сетей является их самоорганизация. Каждый отдельно расположенный узел группируется с таким же узлом, расположенным в радиусе действия антенны и, таким образом, образуется сеть для передачи данных. Объединенные в беспроводную сенсорную сеть датчики образуют территориально-распределенную самоорганизующуюся систему сбора, обработки и передачи информации.

2. Анализ литературных источников и постановка проблемы

Проведя анализ литературы по данной теме можно выделить основные проблемы, возникающие при проектировании беспроводных сенсорных сетей [1].

Конфигурация сенсорной сети должна иметь возможность видоизменяться (самоорганизующаяся сеть) в зависимости от текущего положения в пространстве, возможностей электропотребления, деталей решаемых задач. Поскольку сенсорные узлы взаимодействуют с окружающей средой, они должны иметь возможность динамически приспосабливаться к решению конкретной задачи. Мобильность узлов, их отказы, критичные изменения во внешней среде требуют высокой степени динамичности от сенсорной сети в целом. Поэтому, топология конкретной сенсорной сети или ее части может изменяться многократно в течение срока ее функционирования. Фрагменты беспроводной сенсорной сети в связи с этим нуждаются в современных алгоритмах, которые должны быть робастными и адекватными к изменяющимся условиям.

Сенсорные узлы конструируются так, чтобы потреблять как можно меньше энергии, поскольку они могут функционировать в недружественной внешней среде и замена источника питания может быть невозможна как таковая. Поэтому, сенсорный узел может выйти из строя как по причине критической ситуации во внешней среде, так и вследствие потери возможности энергоснабжения. Однако, как уже отмечалось выше, сенсорная сеть содержит тысячи сенсорных узлов и наиболее важным свойством сенсорной сети в целом должно быть выполнение сетью своих функций даже при выходе из строя какого-то максимально возможного числа сенсорных узлов. В связи с этим, необходимо создавать такие алгоритмы управления сенсорными узлами, чтобы минимизировать энергопотребление. Число пакетов информации, передаваемых, принимаемых, обрабатываемых каждым сенсорным узлом должно быть таким, чтобы расход энергии был минимизирован.

Другой проблемой при построении беспроводных сенсорных сетей является то, что расстояние, на которое сенсорный узел передает информацию, может быть существенно меньше, чем в традиционных радиосистемах. Мощность передатчика должна быть мала (это способ-