управления бизнес-процессами// Промышленные АСУ и контроллеры. – 2006. – № 12. 9. SOA Development Using the IBM Rational Software Development Platform: A Practical Guide. [Електронний ресурс]. – Режим доступу: http://www07.ibm.com/sg/soa/downloads/SOA_Development_ using_ Rational_Software.

УДК 004.78

Л.Б. Чирун, О.Р. Гарасим
Національний університет "Львівська політехніка",
кафедра інформаційних систем та мереж

АНАЛІЗ ЗАХИЩЕНОСТІ МЕРЕЖІ НА ОСНОВІ КОНСОЛІДОВАНИХ РЕСУРСІВ ЗАГРОЗ

© Чирун Л. Б., Гарасим О.Р. , 2011

Проведено аналіз захищеності мережі з використанням консолідованих ресурсів загроз, які були виявлені й зареєстровані в БД. Складено діаграму аналізу загроз та оцінено ризики поширення їх у мережі, запропоновано виявлення слабких ланок мережі.
Ключові слова: загроза, мережа, ризик, консолідація.

In the paper conducted analysis the network security using a consolidated threats resources that were found and registered in the database. Build diagram of analysis threats and assessed risks in distribution network, suggested identifying weak links in the network.
Key words: threat, network, risk, consolidation.

Вступ. Загальна постановка проблеми

Діяльність будь-якої корпорації тісно пов'язана з використанням інформаційних мереж зв'язку, які будуються із застосуванням електронних технологій передавання, збереження, опрацювання, використання корпоративної інформації. Надійне функціонування цих систем безпосередньо впливає на економічну діяльність та фінансовий стан корпорації. В управлінні корпоративною діяльністю разом із фінансовими ризиками необхідно враховувати і ті, які пов'язані із використанням інформаційних систем. Тому для управління ризиками повинна проводитися консолідація інформації системи обліку і вивчення усіх подій, що спричиняють збитки, визначення ймовірностей їх настання, ризики поширення, способи їх упередження. Це завдання є надзвичайно важливим у сучасній корпоративній діяльності, його виконання має першочергове значення.

Система менеджменту інформаційної безпеки корпоративної мережі пов'язана із впливом різних чинників діяльності користувачів мережі і є основою економічної стабільності та збереження високого рівня безпеки корпорації. Для захисту корпоративної інформації, особливо конфіденційної, адміністраторам необхідно приймати своєчасні та зважені управлінські рішення, опрацьовуючи консолідовану інформацію загроз та слабких місць мережі.

Консолідована інформація діяльності системи безпеки корпоративної мережі дає змогу отримати вичерпну інформацію про стан мережі та здійснювати ефективний моніторинг подій, виявляти атаки, несправності та слабкі місця, ізолювати загрози безпеці корпоративної інформації. На основі консолідованої інформації проводиться діагностика, контроль та адаптація менеджменту інформаційної безпеки, проведення прямого контролю безпеки. Адаптація менеджменту інформаційної безпеки необхідна для задоволення бажаних результатів, незважаючи на зміну цілей управління корпорації, технологічних умов або розширення діяльності корпорації.

На основі консолідованої інформації створюється оцінка уразливості мережі та запобігання можливим вторгненням, корегується у відповідному напрямі стратегія менеджменту інформаційної безпеки корпорації, визначення методів та засобів захисту даних, прийняття відповідних рішень для виявлення прихованих загроз інформації.

Зв'язок висвітленої проблеми із важливими науковими та практичними завданнями

Класифікація функціональних елементів мережевої безпеки та категоріювання технологій мережевої безпеки базових функціональних елементів забезпечують основу структурованого підходу до вивчення різнорідних технологій, які стрімко розвиваються. Організований, ієрархічний погляд використовується для представлення усіх традиційних, сучасних і тих, що розвиваються технологій мережевої безпеки. На рис. 1 показано структуру, що відображає організований, ієрархічний погляд на технології функціонування систем захисту інформації корпоративних мереж зв'язку [1, 2].

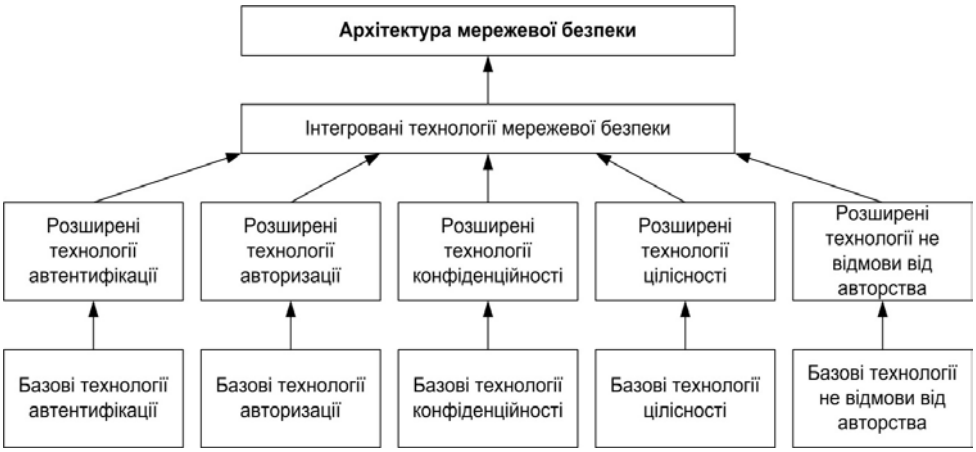

Рис. 1. Архітектура технологій функціонування систем захисту інформації корпоративних мереж зв'язку

Для підтримання такої архітектури функціонування системи захисту інформації корпоративної мережі зв'язку слід використовувати консолідовані ресурси загроз, які виникають протягом усього періоду роботи системи, щоб не допускати можливість прогресу мережевих атак. Збираючи всі дані з кожної технології захисту в єдиний консолідований ресурс, можливо виявляти слабкі сторони системи захисту та відповідно приймати своєчасні заходи з посилення безпеки уразливих ділянок, а також мати можливість прогнозування подій.

Результуючим завданням мережевої безпеки є забезпечення захисту прикладних систем та інформації, яка використовується на вході і яка формується на виході. В результаті можна визначити основні базові функціональні елементи мережевої безпеки корпорації, що є необхідними для побудови та управління системи мережевої безпеки:

- забезпечення конфіденційності;
- автентифікації;
- авторизації;
- цілісності повідомлення та неможливості відмови від причетності до авторства/отримання повідомлення [3, 4].

Ці функціональні елементи мережевої безпеки корпорації використовуються як в апаратному, так і програмному виконанні у мережевих пристроях (комутатори, сервери тощо), що знаходяться в межах шляху, який визначається двома кінцевими точками комунікаційного з'єднання (переважно клієнтський ПК або термінал та сервер) [5, 6].

Важливо зазначити, що не усі ці функціональні елементи завжди містяться в окремих елементах системи мережевої безпеки корпорації. До того ж існують послуги мережевої безпеки,

які важко зарахувати до цих функціональних елементів, але які працюють разом із ними для забезпечення бажаних можливостей мережевої безпеки [7].

Актуальність теми зумовлена необхідністю постійного контролю захищеності мережі та ефективного реагування на чинники, які порушують роботу мережі. Для менеджменту інформаційної безпеки необхідною умовою роботи є консолідація даних про загрози, які негативно впливають на стан мережі. Такий підхід забезпечує можливість вирішення управлінських проблем: прогнозування збитків від дії загроз, виявлення слабких ланок захисту інформації та відповідно сприяє створенню проектів управлінських рішень з удосконалення системи захисту. Консолідовані ресурси обліку загроз створюються не лише для оперативного і поточного управління, але й з метою прийняття довгострокових рішень та прогнозування шкідливих дій зловмисників.

Мета і завдання дослідження

Мета роботи – обґрунтувати теоретичну концепцію консолідації даних про загрози корпоративної мережі зв'язку та інтегрувати результати до системи менеджменту інформаційної безпеки на основі аналізу консолідованих ресурсів, ефективного планування, контролю та прийняття управлінських рішень системою менеджменту інформаційної безпеки.

Для досягнення мети були поставленні такі завдання:

- визначити напрями діяльності системи менеджменту інформаційної безпеки;
- визначити загрози мережі;
- провести консолідацію виявлених загроз;
- оцінити ризики поширення та впливу загроз;
- дослідити слабкі ланки мережі.

Аналіз останніх досліджень та публікацій

Консолідована інформація – це одержані з кількох джерел та системно інтегровані різнотипні інформаційні ресурси, які в сукупності наділені ознаками повноти, цілісності, несуперечливості та становлять адекватну інформаційну модель проблемної області з метою її аналізу, опрацювання та ефективного використання в процесах підтримки прийняття рішень [8].

Для системи менеджменту корпоративної мережі зв'язку повинні проводитись процедури спостереження та дослідження якості її роботи. Цими процедурами визначається відповідність корпоративної мережі зв'язку складеному стратегічному плану діяльності корпорації та проведення аналізу впливу специфічних ризиків на загальну її діяльність. Зокрема, до них належать перевірка функцій електронних каналів доставляння інформації, їх відповідність стратегічному плану діяльності; здатність електронних засобів опрацьовувати запланований обсяг інформації [9, 10].

Процедури системи менеджменту визначають, чи керівництво корпорації та відповідальні підрозділи отримують необхідну їм інформацію та досліджують функціонування кожної впровадженої електронної системи, здійснюють її аналіз, зокрема:

- встановлення, чи враховуються різні аспекти функціонування електронних систем, включаючи аналіз критичних випадків, збоїв;
- визначення для кожної електронної системи, яка співпрацює з головною операційною системою корпорації, базами даних, їх сумісність і захищеність;
- перевірка на точність та інтелектуальність програмного забезпечення з планування, розрахунків тощо, яке доступне через мережу зв'язку;
- визначення, чи встановлена система дублювання для користувачів на випадок, коли системи електронних послуг не працюють тривалий період часу;
- перевірка на наявність розроблених процедур повідомлення керівного складу системи менеджменту у разі виникнення технічних проблем мережі;
- перевірка на наявність розподілу фізичного доступу до комп'ютерного обладнання, програмного забезпечення, комунікаційного обладнання і ліній комунікацій з чітко визначеними особами персоналу залежно від їх функцій і посад в корпорації [6].

Організація діяльності корпорації повинна бути пристосована до умов використання електронних засобів, тому некомпетентність керівництва чи недосконаліть технологій, які використовуються, можуть вплинути на економічний стан установи. Також вже існуюча організація діяльності може недостатньо забезпечувати захист конфіденційної електронної інформації. Існуючі порядки і процедури можуть не враховувати швидкість здійснення трансакцій і розширену географію досяжності електронних каналів, якими передається корпоративна інформація.

Тому система менеджменту включає:

1. Спостереження операційних порядків і процедур, що полягає у визначенні їх придатності в умовах використання електронних каналів передачі інформації. Визначається, чи застосовувані порядки організації праці персоналу, що застосовуються, відповідають вимогам впровадження у нових корпоративних продуктах та послугах; як впливають електронні технології на канали передачі інформації. Корпорація повинна мати належну систему безпеки, що включає такі елементи:

- контроль доступу та захисту конфіденційної інформації клієнтів;
- методи визначення права запиту кожного учасника електронних систем передачі даних;
- виділення інформації, яка може бути доступною для третіх осіб.

2. Визначення здатності вдосконалення порядків і процедур відповідно до застосування електронних технологій забезпечення доступу і зміни конфіденційної інформації:

- яку інформацію та як можна передавати третім особам;
- чи порядок використання конфіденційної інформації є частиною контрактів і угод з найманими корпорацією третіми особами.

3. Визначення наявності в процедурах обов’язкового засвідчення авторизації. Підтверджується наявність захисту відстеження і запобігання подвійним трансакціям в кожній електронній системі. Перевіряється якість проведення навчання клієнтів стосовно захисту і безпеки під час використання електронних корпоративних систем. Періодично за встановленим графіком перевіряється увесь спектр трансакційних корпоративних можливостей, здійснюється консолідація ресурсів діяльності кожного сегмента захищеної корпоративної мережі зв’язку, операційні порядки і процедури здійснення трансакцій та відповідність вимогам захисту та безпеки корпоративної інформації [11].

Ефективне управління інформаційною безпекою вимагає розуміння мережевих атак. Як правило, атаки проводяться у кілька кроків.

Перший – дослідження або мережева розвідка. Зловмисник збирає інформацію про використання цільової бази даних і документів, наявність засобів моніторингу корпоративної мережі. Тоді зловмисник намагається виявити уразливості в апаратному, програмному або організаційному забезпеченні інформаційної безпеки, продовжує додаткові дослідження та шукає інструмент, який здатний порушити налагоджену роботу. Системи виявлення атак класифікують таке сканування, як низький рівень загрози, тому що вони не завдають шкоди серверам або діяльності корпорації.

Сканування є попереднім кроком для здійснення атак. Якщо порт виявили відкритим або не захищеним, тоді, зазвичай, зловмисник переходить до фази підготовлення атак. Деякі сервіси і додатки є цілями для нападу. Незважаючи на використання технології безпеки, мережеві адміністратори повинні виконати завдання захисту систем від атак зловмисників і від випадкових невдач. Один метод, що називається розвідувальним, використовується хакерами для вибору мереж і доменів для пошуку цілей. Розвідка дає змогу хакерові визначити цілі для нападу або використовувати їх для нападу [12].

Виділення проблеми

Оцінка ризиків, пов'язаних з порушенням захисту, повинна виявити, кількісно визначити і прийняти рішення для їх запобігання. Результати повинні спрямовувати та визначати відповідну дію з управління та пріоритети управління ризиками, які пов'язані з порушенням захисту

інформації, а також пріоритети реалізації вибраних засобів управління, з метою захисту від цих ризиків. Процес оцінювання ризиків і вибору засобу управління може здійснюватися кілька разів, щоб охопити різні частини організації чи окремі інформаційні системи.

Оцінка ризиків повинна включати систематичний метод оцінки величини ризиків (аналіз ризиків) і процес порівняння передбачуваних ризиків стосовно критеріїв ризиків з метою визначення значущості ризиків. Також оцінки ризиків повинні виконуватися періодично, щоб врахувати зміни у вимогах захисту і в ризикованих ситуаціях, наприклад, в активах, в загрозах, в слабких місцях, негативних впливах, оцінці значущості ризиків, а також, коли відбуваються значні зміни. Ці оцінки ризиків повинні виконуватись методичним способом, що здатний дати порівняння та відтворювані результати. Оцінка ризиків, які пов'язані з порушенням захисту інформації, повинна мати чітко визначену область дії для того, щоб бути результативною, і повинна включати взаємозв'язок з оцінками ризиків в інших областях, якщо це доречно.

Відповідно до вимог стандарту ISO / IEC 27002:2007, який визначає основні напрями і загальні принципи розроблення, здійснення, підтримки і вдосконалення управління інформаційної безпеки організації, наведемо діаграму аналізу загроз щодо мережі корпорації (рис. 2) для їх консолідації та визначення стратегії менеджменту інформаційної безпеки (рис. 3).

Моніторинг використання корпоративних електронних інформаційних систем, зокрема їх технічних складових, є надзвичайно важливим чинником у забезпеченні надійності і ефективності здійснення діяльності сучасної корпорації. Дані моніторингу електронних систем, консолідація первинних даних за визначеними нами напрямами є одним з основних джерел інформації для прийняття управлінських рішень і складання програм управління ризиками в корпоративній діяльності. У [13] подано етапи аналізу та прогнозування ризиків:

Загалом середній за певний проміжок часу комбінований ризик від небезпечної події А може бути обчислений за формулою

$$R(A) = P(A)Y(A), \tag{1}$$

де *P(A)* – статистична ймовірність події А (або подієвий ризик); *Y(A)* – можливий одномоментний збиток (або, якщо *P(A)=1*, вартісний ризик).

Своєю чергою, подієвий ризик дорівнює

$$P(A) = \frac{\nu(t)}{T}, \tag{2}$$

де $\nu(t)$ – кількість проявів подій A за час t; T – період спостереження.

Тобто фізичний зміст показника *R(A)* – кількість або вартість підданих ризику протягом періоду дослідження елементів.

Введемо нову характеристику $C_y(A)$ – ступінь уразливості від впливу події A:

$$C_y(A) = \frac{M_{ve}}{M_z}. \tag{3}$$

де M_{ve} – кількість уражених елементів; M_z – загальна кількість елементів, які опинилися в зоні ураження. Тоді можливий одномоментний збиток *Y(A)* може бути визначений за такою формулою:

$$Y(A) = C_y(A)Y_n(A), \tag{4}$$

де $Y_n(A)$ – умовний повний збиток, який чисельно дорівнює кількості або вартості усіх елементів обчислювальної техніки (або усіх елементів, які опинилися в зоні ураження). Отже, з урахуванням виразів (2) і (4), формула (1) набуває вигляду:

$$R(A) = \frac{\nu(t)}{T}\Big|_A C_y(A)Y_n(A). \tag{5}$$

Це загальна формула обчислення ризику. Розглядаючи частинні ризики, притаманні саме певному типу елементів загроз мережі (віруси, шкідливі програми, трояни, хробаки), слід вводити необхідні модифікації. Тоді ця формула набуває такого вигляду:

$$R_c(A) = \frac{v(t)}{T}\Big|_A P(H)C_{yc}(A)H\,, \qquad (6)$$

де $R_c(A)$ – частинний ризик; *P(H)* – ймовірність перебування елементів певного типу у зоні ураження; *H* – їх кількість; $C_{yc}(A)$ – ступінь ураженості цієї групи елементів.

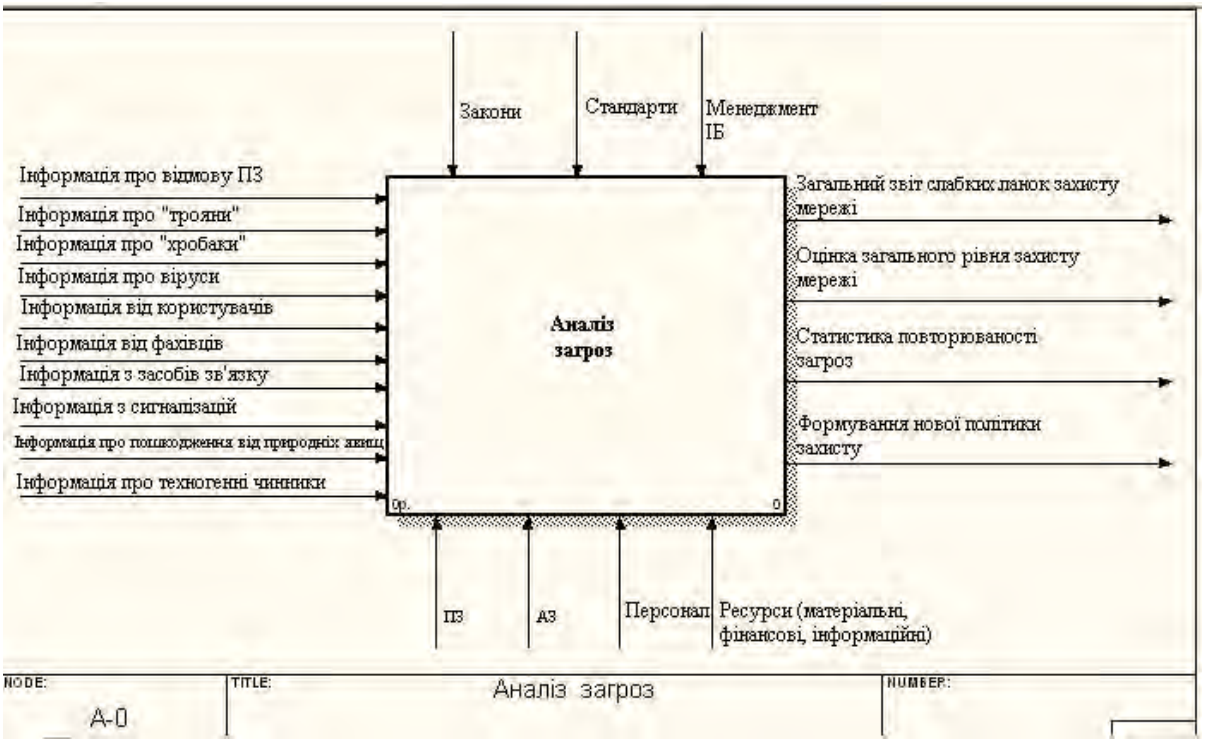

Рис. 2. Діаграма аналізу загроз мережі

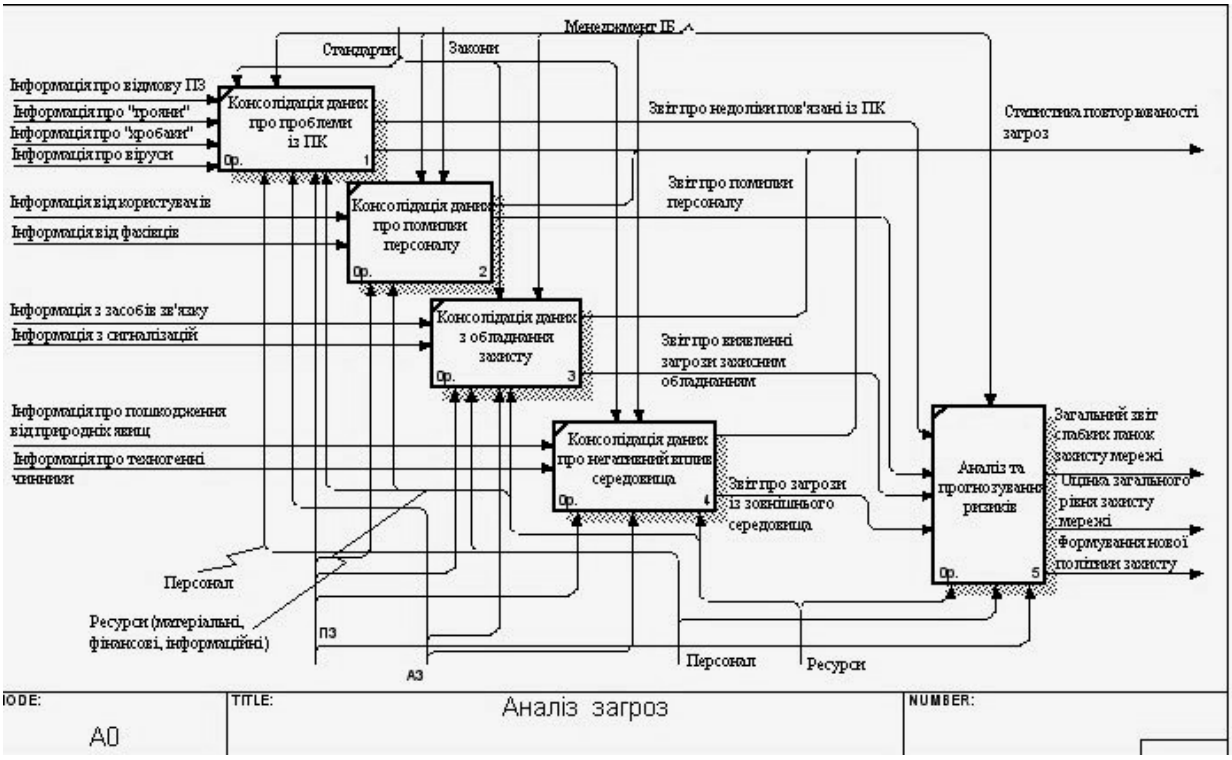

Рис. 3. Керуючі елементи процессу аналізу загроз

Аналіз отриманих результатів

Консолідація загроз мережі проводилась на кафедрі ІТПК. Період дослідження охоплює 18 днів. Мережа складається з 3 ПК, на яких встановлено п’ять програмних продуктів. За час дослідження були виявлені загрози:

із комп’ютерів мережі – 18 (рис. 5);

несанкціонованого доступу до інформації – 3;

злий задум або помилки персоналу – 5;

зовнішні загрози – 2.

Написана програма для оцінення ризиків від загроз (рис. 4) з використанням формул (1)–(6).

Досліджено чотири події (проблеми):

Подія I (техніка) – відмова, неполадки, збої в ЕОТ;

Подія II (перехоплення / НСД до інформації) – перехоплення інформації або отримано соціотехнічним способом;

Подія III (злий задум персоналу) – навмисне або не правильне поводження з інформацією;

Подія IV (техногенна загроза) – негативний вплив середовища.

Результати занесені в таблицю (рис. 4), де R – середній ризик від події; C – ступінь ураженості елементів мережі; R_o – одномоментні збитки; C_a – частковий ступінь ураженості апаратури; C_p – частковий ступінь ураженості програмного забезпечення; R_a – частковий ризик від події для апаратного забезпечення (АЗ); R_p – частковий ризик від події для програмного забезпечення (ПЗ).

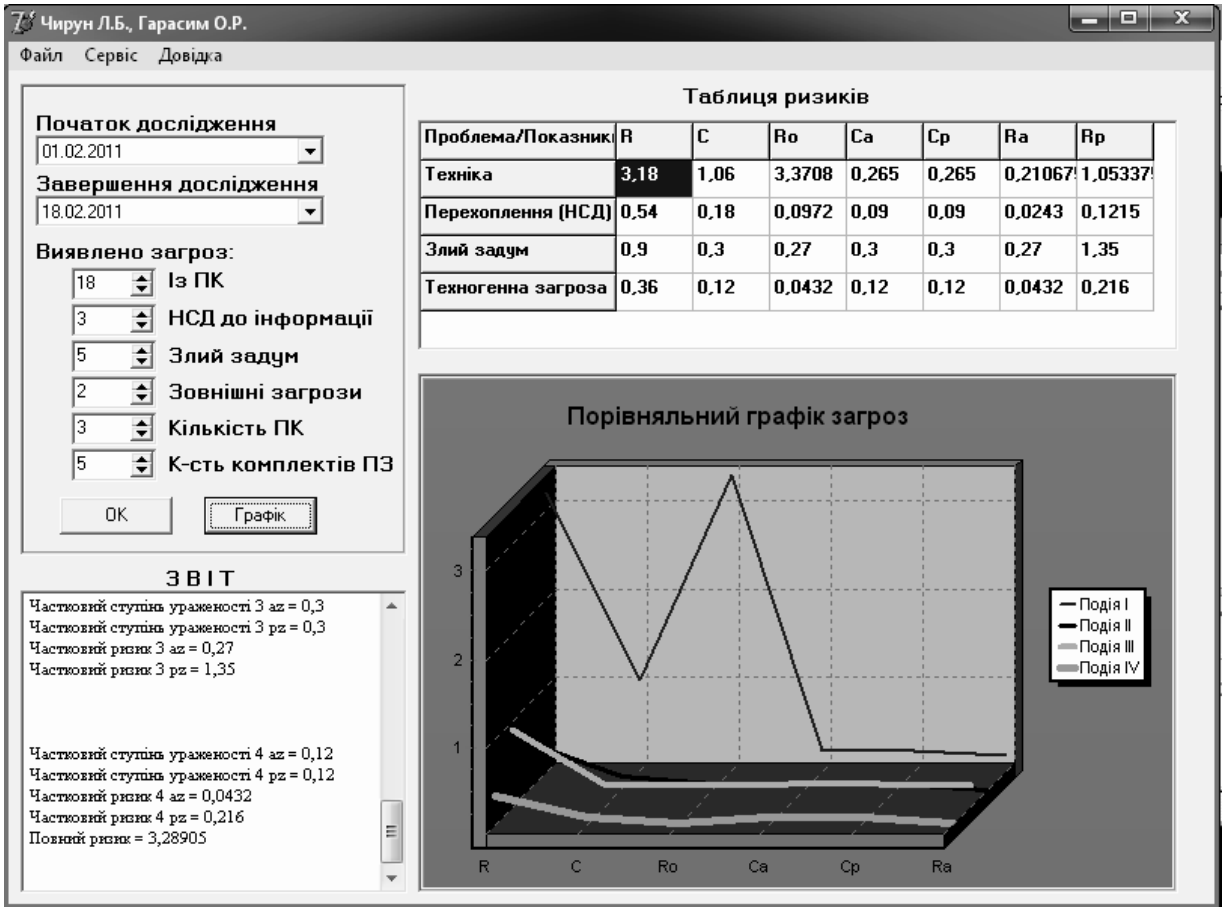

Рис. 4. Програма оцінки загроз

У результаті обчислень за формулами (1)–(6) отримано такі результати:
Середні ризики:
I подія = 3,18
II подія = 0,54
III подія = 0,9
IV подія = 0,36

Ступінь ураженості:
I подія = 1,06
II подія = 0,18
III подія = 0,3
IV подія = 0,12

Одномоментні збитки:
I подія = 3,3708
II подія = 0,0972
III подія = 0,27
IV подія = 0,0432

Комбіновані збитки = 3,7812
Комбінований середній збиток = 4,98

Частковий ступінь ураженості 1 АЗ = 0,265
Частковий ступінь ураженості 1 ПЗ = 0,265
Частковий ризик 1 АЗ = 0,210675
Частковий ризик 1 ПЗ = 1,053375

Частковий ступінь ураженості 2 АЗ = 0,09
Частковий ступінь ураженості 2 ПЗ = 0,09
Частковий ризик 2 АЗ = 0,0243
Частковий ризик 2 ПЗ = 0,1215

Частковий ступінь ураженості 3 АЗ = 0,3
Частковий ступінь ураженості 3 ПЗ = 0,3
Частковий ризик 3 АЗ = 0,27
Частковий ризик 3 ПЗ = 1,35

Частковий ступінь ураженості 4 АЗ = 0,12
Частковий ступінь ураженості 4 ПЗ = 0,12
Частковий ризик 4 АЗ = 0,0432
Частковий ризик 4 ПЗ = 0,216
Повний ризик = 3,28905

За визначеними ризиками помітно, що рівень захисту мережі кафедри ІТПК є недостатнім і найбільшу загрозу мережі становить подія І. Отже, дослідимо у цьому аспекті загрози за допомогою системи пошуку логічних правил.

За допомогою системи WithWhy (Demo версії, яка має обмеження лише на кількість записів) виведемо логічні правила на основі консолідованих даних про виявлені загрози події І (рис. 4).

Virus

Cod	Name_vir	Size_kb	Dll_infect	Com_infect	Exe_infect	Resident	Polymorphi	Slowing_do	Unauthorize	streng_mes
1	Virus.Win32	20	☑	☐	☑	☑	☑	☑	☐	☐
2	Virus.Multi.I		☐	☐	☑	☐	☐	☑	☐	☐
3	Virus.Boot-I		☐	☑	☑	☑	☐	☑	☑	☐
4	Virus.Win32	36	☐	☐	☑	☐	☐	☐	☐	☑
5	Virus.Win32	18	☐	☐	☑	☐	☐	☐	☐	☐
6	Virus.Win32	41	☐	☐	☑	☑	☐	☐	☐	☐
7	Email-Worm		☑	☐	☑	☑	☑	☐	☐	☑
8	Virus.Win32	36	☐	☐	☑	☑	☐	☐	☐	☐
9	Virus.Win32		☐	☐	☑	☑	☐	☐	☐	☑
10	Virus.Win32	36	☐	☐	☑	☐	☑	☐	☐	☐
11	Virus.Win32	9	☐	☐	☑	☑	☐	☑	☐	☐
12	Virus.Win32	17	☑	☐	☑	☑	☐	☑	☑	☐
13	Virus.DOS. A	1	☐	☑	☑	☑	☐	☐	☐	☑
14	Email-Worm	53	☐	☐	☑	☑	☐	☑	☑	☐
15	Virus.Win32	31	☐	☑	☑	☑	☐	☑	☑	☐
16	Virus.Win32	16	☑	☐	☑	☑	☐	☑	☑	☐
17	Virus.Win32	8	☐	☐	☑	☐	☐	☑	☐	☐
18	Win32.Killis.	2	☐	☐	☑	☐	☐	☐	☐	☐

Рис. 5. Таблиця обліку вірусних атак

Використовуємо такі правила, які виявили недоліки в системі захисту, а саме – розподіл доступу до локальної мережі та Інтернет в програмних продуктах, що здійснювало перевантаження операційної системи та розповсюдження вірусів:

1) *If* **Unauthorized_address_to_net** *is* **No**
Then
Slowing_down_PC *is not* **Yes**
Rule's probability: **0,692**
The rule exists in **9** *records.*
Significance Level: Error probability < 0,1
Positive Examples (records' serial numbers):
4, 5, 6, 7, 8, 9, 10, 13, 18
Negative Examples (records' serial numbers):
1, 2, 11, 17

2) *If* **Unauthorized_address_to_net** *is* **Yes**
Then
Slowing_down_PC *is* **Yes**
Rule's probability: **1,000**
The rule exists in **5** *records.*
Significance Level: Error probability < 0,1
Positive Examples (records' serial numbers):
3, 12, 14, 15, 16
(див. рис. 6)

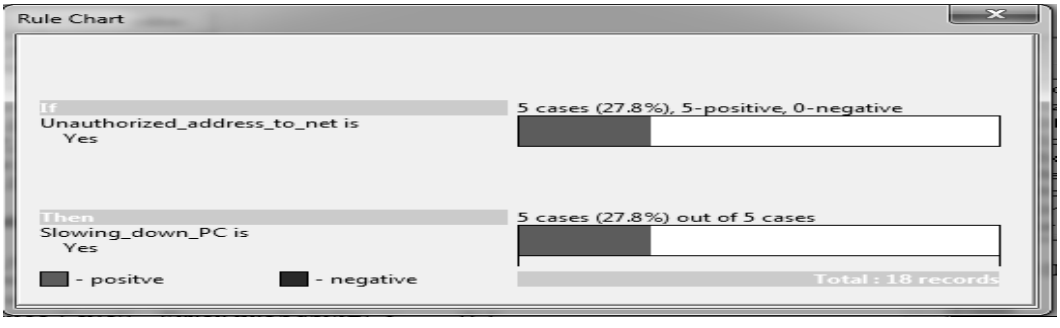

Рис. 6. Графічне відображення правила на основі аналізу консолідованих ресурсів загроз

Система менеджменту інформаційної безпеки спрямована на протистояння атакам ззовні та сприяє безпечному спілкуванню всередині організації, а також за її межами. Суть системи менеджменту полягає в необхідності консолідації інформації про стан комп'ютерної системи та ефективні способи її використання, а отже, головним завданням системи менеджменту інформаційної безпеки є здатність до вирішення проблем з врахуванням багатьох специфічних обмежень корпорації, а також швидко і правильно діагностувати і в найкращий спосіб усувати несправності системи.

Слід пам'ятати, що будь-які заходи, які вживають для забезпечення захисту інформації, не повинні коштувати більше, ніж сама інформація. Облаштування фізично ізольованих захищених каналів зв'язку для безпечного інформаційного обміну між віддаленими вузлами є надзвичайно дорогим і не завжди обґрунтованим заходом. Тому консолідовані інформаційні ресурси про стан корпоративної мережі зв'язку є основою для системи менеджменту інформаційної безпеки.

Висновки і перспективи подальших наукових розвідок

З метою координації системи менеджменту інформаційної безпеки (СМІБ) на вирішення проблем, які пов'язані зі слабкими ланками мережі зв'язку, необхідно виділити із загальної системи консолідацію загроз як складову частину інформаційної безпеки, яка є підґрунтям підготовки необхідної інформації для одержання нових знань.

Важливим напрямом покращання безпеки мережі зв'язку є оцінка ризиків загроз, які здійснюються на основі консолідованих ресурсів загроз. Використання такого підходу створює передумови для прийняття оптимальних рішень на стадії планування СМІБ та її удосконалення.

З метою упорядкування сукупності загроз згідно із завданнями СМІБ доцільно використовувати консолідовані ресурси, що становить методологічну основу СМІБ та уможливлює одержати необхідну інформацію для виконання конкретних завдань.

Доволі часто персонал системи безпеки несе відповідальність за моніторинг і аналіз даних, поданих в одній системі. Співробітники служби безпеки лише періодично аналізують дані і несвоєчасно повідомляють про результати аналізу звітів з менеджменту безпеки для усіх зацікавлених осіб. У сучасних технологіях безпеки відсутня інтеграція, прогнозування і в режимі реального часу зворотного зв'язку для користувачів, щоб вжити заходи для запобігання або зупинення атак. Крім того, технології не є ефективними для великомасштабних атак. Обмеження кожного цінного паперу технології в поєднанні зі зростанням нападів впливають на ефективність управління інформаційною безпекою та підвищення заходів, які будуть виконуватися мережевими адміністраторами. Конкретні питання включають збір даних, опрацювання даних, нормалізацію даних, кореляції подій, поведінки класифікації, звітності та реагування. Щоб забезпечити повну, точну картину подій в мережі, потрібно від системи менеджменту значну кількість опрацювання подій в режимі реального часу, консолідацію та кореляцію подій.

Отже, в комплексні рішення необхідно включити: виявлення атак і їх фільтрацію; джерело атаки; відстеження та ідентифікація, запобігання атак. Рішення, які підтримують у реальному часі даних аналізу загроз дуже важливі, оскільки в режимі реального часу виявлення дає змогу системі менеджменту інформаційної безпеки запобігти вторгненню ще на початку циклу атаки. Це призводить до зниження шкоди, що заподіяна успішними атаками, а також зниження ризиків втрати даних.

Консолідована інформація системи менеджменту інформаційної безпеки ґрунтується на інтеграції даних про загрози з різних джерел мережевих продуктів, відкиданні помилкових тривог та кореляції подій з різних джерел. Існує необхідність ширшого використання консолідованих інформаційних ресурсів для прогнозування виникнення атак. Аудит та інтелектуальні механізми звітності повинні підтримувати оцінку безпеки та управління

погрозами в ширшому масштабі та у взаємозв'язку з минулими, поточними і майбутніми подіями. Консолідовані інформаційні ресурси скеровані на покращання якості та швидкості підтримки прийняття рішень.

1. Гарасим Ю.Р. Структура технологій функціонування систем захисту інформації корпоративних мереж зв'язку / Ю.Р. Гарасим, В.Б. Дудикевич // матер. IV Міжнар. наук.-практ. конф. "Спеціальна техніка у правоохоронній діяльності". – К., 2009. – С. 226–228. 2. Draft, E. Authentication Policy for Federal Agencies / E. Draft. – Federal Register. – 2003. – Vol. 68 (No. 133). 3. Гарасим Ю.Р. Інформаційна безпека захищених корпоративних мереж зв'язку / Ю.Р. Гарасим, В.Б. Дудикевич // Вісник Національного університету "Львівська політехніка" "Автоматика, вимірювання та керування". – 2009. – № (639). – С. 124–132. 4. Horton, Mike. Network Security – Portable Reference / Mike Horton, Clinton Mugge. – McGraw-Hill/Osborne, 2003. 5. Atkinson, R. IETF RFC 1825: Security Architecture for the Internet Protocol / R. Atkinson, 1995. 6. Грайворонський М.В. Безпека інформаційно-комунікаційних систем / М.В. Грайворонський, О.М. Новіков. – К.: Видавнича група BHV, 2009. – 608 с. 7. Saadat, Malik. Network Security Principles and Practices / Malik Saadat. – Cisco Press, 2003. 8. Кунанець Н. Е. Консолідована інформація: сучасний фах освітньо-наукового напряму інформаційних наук [Електронний ресурс]. – Режим доступу: http://www.nbuv.gov.ua/portal/natural/Vnulp/ISM/2009_653/15.pdf. 9. Пасічник В.В. Глобальні інформаційні системи та технології: моделі ефективного аналізу, опрацювання та захисту даних: монографія // В.В. Пасічник, П.І. Жежнич, Р.Б. Кравець, А.М. Пелещишин, Д.О. Тарасов. – Львів: Вид-во НУ "Львівська політехніка", 2006. – 348 с. 10. Стан і проблеми забезпечення інформаційної безпеки [Електронний ресурс]. – Режим доступу: http://old.niss.gov.ua/book/otch/roz13.htm. 11. Ткаченко М.І. Формування програми контролю ризиків при використанні банківських електронних інформаційних систем [Електронний ресурс]. – Режим доступу: http://www.economy.nayka.com.ua/index.php? operation=1&iid=359. 12. Ярочкин В.И. Информационная безопасность: учебник для студентов вузов. – 2-е изд. // В.И. Ярочкин. – М.: Академический Проект; Гаудеамус. – 2004. – 544 с. 13. Біленчук П. Концепція забезпечення безпеки інформації на об'єкті в умовах необхідної ситуації // Бизнес и безопасность. – 2008. – № 5. – С.96–98.