unusual program behavior using the statistical component of the next generation intrusion detection system (NIDES)". // Technical Report SRI-CSL-95-06, Computer Science Laboratory, SRI International, Menlo Park, USA, May 1995.

[9] Y. Frank Jou, Fengmin Gong, Chandru Sargor, Shyhtsun FelixWu, and CleavelandW Rance, "Architecture design of a scalable intrusion detection system for the emerging network infrastructure." // Technical Report CDRL A005, Dept. of Computer Science, North Carolina State University, Releigh, N.C, USA, April 1997.

[10] Sebring, M., Shellhouse, E., Hanna, M. & Whitehurst, R. Expert Systems in Intrusion Detection: A Case Study. // Proceedings of the 11th National Computer Security Conference, 1988

[11] Herve Debar, Monique Becker, and Didier Siboni, "A neural networkcomponent for an intrusion detection system." // Proceedings of the 1992 IEEE Computer Sociecty Symposium on Research in Security and Privacy,pages 240–250, Oakland, CA, USA, May 1992.

[12] M.P.Zielinski, "Applying Mobile Agents in an Immune-system-based intrusion detection system." // University of South Africa, 2004.

[13] Sheyner, Oleg "Scenario Graphs and Attack Graphs." // PhD thesis, SCS,Carnegie Mellon University, 2004.

УДК 004.056.53 (045)

Чунарева А.В., Чунарев А.В. Методы и системы обнаружения несанкционированного доступа в современных информационно-коммуникационных системах и сетях

Аннотация. *В данной статье проведен анализ современных методов и систем обнаружения несанкционированного доступа в современных информационно-коммуникационных системах и сетях. В результате проведения анализа выделены преимущества и недостатки применения существующих методов и систем. Выделены наиболее эффективные с точки зрения повышения защиты информации и обеспечения противодействия угрозам, как преднамеренным и случайным.*

Ключевые слова: *защита информации, несанкционированный доступ, атака, информационно-коммуникационная система и сеть, уязвимость.*

Chunariova A.V., Chunariov A.V. Methods and systems for the detection of unauthorized access to modern information and communication systems and networks

Abstract. *In this paper, an analysis of modern methods and systems to detect unauthorized access to modern information and communication systems and networks. As a result, the analysis highlighted the advantages and disadvantages of existing methods and systems. Select the most efficient in terms of improving data protection and security to counter threats such as deliberate and accidental.*

Keywords: *information security, unauthorized access, attacks, information and communication system and network, vulnerabilities.*

Отримано *15 березня 2012 року,* затверджено редколегією *04 червня 2012 року*
(рецензент д.т.н., професор О.К. Юдін)

МЕТОДИКА ОЦІНКИ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ В ЛОМ. ГРАФІЧНІ МОДЕЛІ ВЗАЄМОДІЇ ЗАГРОЗ ФУНКЦІОНАЛЬНИМ ВЛАСТИВОСТЯМ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ РЕСУРСІВ ЛОМ ІЗ ЕЛЕМЕНТАМИ СИСТЕМИ ЗАХИСТУ

Вячеслав Василенко, Олена Дубчак, Микола Василенко

Національний авіаційний університет

ВАСИЛЕНКО Вячеслав Сергійович, к.т.н., доцент

Рік та місце народження: 1941 рік, с. Євстратівка, Россошанський р-н, Воронізька обл., Росія.
Освіта: Київське вище інженерне радіотехнічне училище ППО, 1971 рік, Харківська інженерна радіотехнічна академія ППО, 1978 рік.
Посада: доцент кафедри комп'ютеризованих систем захисту інформації з 2005 року.
Наукові інтереси: технічний захист інформації.
Публікації: більше 200 наукових публікацій, серед яких навчальні посібники, наукові статті свідотства та патенти на винаходи.
E-mail: bbc1@voliacable.com

ДУБЧАК Олена Вікторівна

Рік та місце народження: 1959 рік, м. Київ, Україна.
Освіта: Київський інститут інженерів цивільної авіації (з 2000 року – Національний авіаційний університет), 1981 рік.
Посада: старший викладач кафедри комп'ютеризованих систем захисту інформації з 2009 року.
Наукові інтереси: інформаційна безпека.
Публікації: більше 70 наукових публікацій, серед яких навчально-методичні видання, наукові статті, тези доповідей.
E-mail: edubchak@yandex.ru

ВАСИЛЕНКО Микола Юрійович

Рік та місце народження: 1992 рік, м. Київ, Україна.
Освіта: Авіакосмічний ліцей Національного авіаційного університету, 2009 рік.
Посада: студент кафедри комп'ютеризованих систем захисту інформації з 2009 року.
Наукові інтереси: інформаційна безпека.
Публікації: більше 20 наукових публікацій, серед яких наукові статті, тези доповідей та патенти на винаходи.
E-mail: nikolaj92@bigmir.net

Анотація. *У статті запропоновано використання графічних моделей взаємодії загроз функціональним властивостям захищеності інформаційних ресурсів ЛОМ із елементами системи захисту, які дозволяють визначити склад таких систем та, в подальшому, оцінити можливі залишкові ризики при забезпеченні конфіденційності, доступності та цілісності інформаційних об'єктів в телекомунікаційних системах.*

Ключові слова: *конфіденційність, цілісність, доступність інформації, залишкові ризики, локальні обчислювальні мереж.*

Вступ

Загально відомо, що на сучасному етапі розвитку локальних обчислювальних мереж (ЛОМ) захист їх ресурсів, насамперед інформації, є дуже важливою й актуальною проблемою. Для цього розробляються чи використовуються системи захисту, які забезпечують той чи інший рівень захищеності інформації ЛОМ. Нормативними документами Системи технічного захисту України [1-3] властивості захищеності інформації визначені наступним чином:

1. Конфіденційність інформації – властивість інформації, яка полягає в тому, що інформація не може бути отриманою неавторизованим користувачем або процесом;
2. Цілісність інформації – властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем або процесом;
3. Доступність – властивість інформації, яка полягає в тому, що користувач або процес, який володіє відповідними повноваженнями, може використати її відповідно до правил, установлених політикою безпеки, не очікуючи довше заданого (малого) проміжку часу, тобто коли інформація знаходиться у вигляді, необхідному користувачеві, і в той час, коли вона йому необхідна.

Постановка задачі

Для визначення вимог та оцінки захищеності інформації використовуються критерії оцінки захищеності. Відомо також, що досягнуті результати із забезпечення ефективності захисту можна оцінювати або величиною можливих збитків по кожному з класів порушень, або з допомогою залишкового ризику [4] чи інших показників ефективності захищених систем, застосування яких рекомендується в [1 – 4]. Їх основний недолік полягає в тому, що вони є якісними а не кількісними, що на етапах проектування чи вибору засобів системи технічного захисту інформації потрібної якості звужує можливості оцінки рівня та ефективності захищеності ресурсів, насамперед, захищеності інформації, наприклад з погляду оптимального співвідношення витрат на засоби захисту та досягнутих при цьому результатів (можливості з оптимізації параметрів систем захисту).

На відміну від цього автори ставлять завдання ввести та використати кількісні показників захищеності інформації в ЛОМ у вигляді величин залишкових ризиків. Як **величини залишкового ризику** пропонується використовувати ймовірності порушення: конфіденційності – $q_{пк}$, цілісності – $q_{пц}$, доступності – $q_{пд}$ та подолання, злому комплексної системи захисту – q.

Для визначення того чи іншого залишкового ризику за допомогою відповідних методик необхідно:

1. Визначити (побудувати) моделі порушників та загроз відповідним ресурсам ЛОМ, визначити найбільш суттєві з цих загроз;
2. Детально проаналізувати взаємодію загроз (засобів реалізації атак), спрямованих на подолання механізмів забезпечення захищеності інформації ЛОМ, із засобами протидії цим загрозам.

У цій статті будемо виходити з того, що моделі порушників та загроз побудовані, найбільш суттєві загрози відповідним ресурсам ЛОМ визначені, наприклад так, як в роботах [5 – 7]. До найбільш суттєвих загроз віднесемо: різноманітні спроби несанкціонованого, у тому числі фізичного, доступу (з подоланням засобів організаційного обмеження доступу, засобів охоронної сигналізації, засобів адміністрування доступу операційних систем, систем керування базами даних, використання витоків інформації за рахунок побічних електромагнітних випромінювань та спеціальних впливів на інформаційні ресурси ЛОМ тощо), загрози з боку впроваджених тим чи іншим чином вірусів.

Тоді для оцінки захищеності інформаційних ресурсів ЛОМ слід виконати наступні етапи:

1. Побудова графічних моделей взаємодії загроз функціональним властивостям захищеності інформаційних ресурсів ЛОМ із засобами їх захисту.
2. Розроблення методик оцінки величин залишкових ризиків у ЛОМ.
3. Розроблення методик визначення вихідних даних для оцінки залишкових ризиків у ЛОМ.

Результати їх виконання наведено нижче.

Зауваження. Наведені результати стосуються лише інформації, яка циркулює суто в ЛОМ (та їх елементах) і не стосуються інших видів інформації (різних видів акустичної, візуальної та т. інш.), яка циркулює в приміщеннях, в яких функціонують елементи ЛОМ.

Результати дослідження щодо графічних моделей взаємодії загроз функціональним властивостям захищеності із засобами захисту інформаційних ресурсів ЛОМ**.** Побудова графічних моделей взаємодії загроз функціональним властивостям захищеності інформаційних ресурсів ЛОМ передбачає виконання наступних етапів:

1. Формулювання моделі порушників (здійснюється службою захисту інформації підприємства і в цій статті не розглядається) та загроз.
2. Визначення, хоча б у загальному вигляді, засобів протидії загрозам – моделі захисту інформаційного об'єкту.
3. Розроблення графічних моделей взаємодії загроз із засобами протидії цим загрозам.

За наслідками першого етапу та з урахуванням [5 – 7] доцільно здійснити додаткову класифікацію порушників на:

"Випадкових порушників" – авторизованих користувачів, які порушили політику безпеки тієї чи іншої послуги ненавмисно, а помилково шляхом виконання непередбачених дій з об'єктом захисту шляхом випадкового подолання засобів управління (адміністрування) доступом до нього та т.п.

"Терплячих зловмисників" – авторизованих користувачів, які порушили політику безпеки тієї чи іншої послуги навмисно, але без рішучих дій, маскуючись, шляхом підбору атрибутів доступу інших користувачів з метою прихованого подолання засобів управління (адміністрування) доступом до нього та т.п.

"Рішучих зловмисників", які мають на меті будь-що порушити ту чи іншу властивість захищеної інформації. Для цього такі зловмисники прагнуть подолати засоби організаційного обмеження доступу, охоронної сигналізації, управління доступом до фізичних ресурсів, елементи будівельних конструкцій тощо й отримати змогу фізичного доступу до засобів оброблення, зберігання чи передавання інформаційних об'єктів з метою виведення їх з ладу, зміни режимів функціонування, крадіжки носіїв, наприклад, накопичувачів на жорстких чи гнучких магнітних дисках тощо.

Зловмисників, які використовують засоби віддаленого доступу до інформаційних об'єктів: витоки інформації технічними каналами, спеціальні впливи на інформацію технічними каналами, мережеве обладнання локальних чи розподілених мереж, у тому числі й засоби телекомунікаційних мереж. Ця класифікація дозволяє більш чітко визначати способи унеможливлення несанкціонованих дій порушників та засоби, які потрібні для побудови моделей взаємодії засобів реалізації атак із засобами захисту відповідних властивостей захищеності інформації (чи взагалі ресурсів ЛОМ). Такий підхід дозволяє визначити деяку узагальнену графічну модель загроз ресурсам локальних обчислювальних мереж (ЛОМ), у вигляді, який наведено на рис. 1.

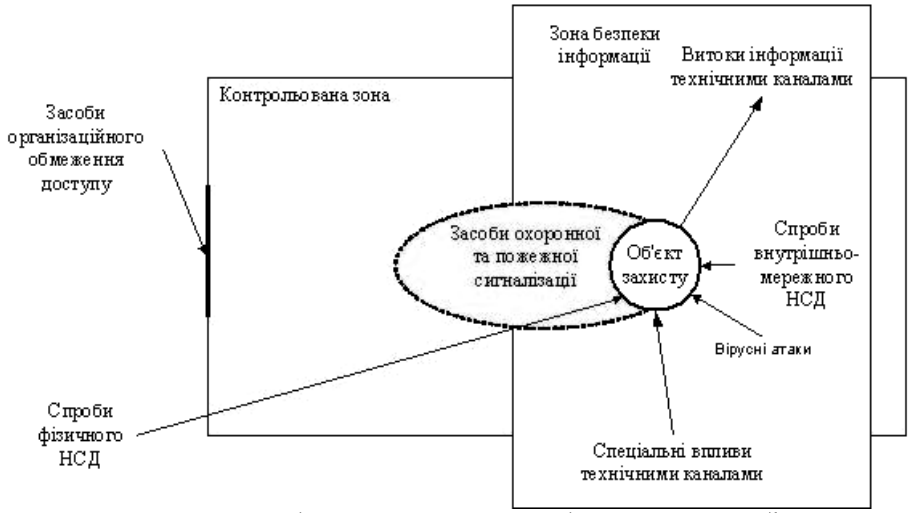

Рис. 1. Узагальнена графічна модель загроз інформаційному об'єкту ЛОМ

На другому етапі побудови моделей взаємодії загроз функціональним властивостям із засобами захисту інформаційних ресурсів ЛОМ (визначення засобів протидії загрозам – моделей захисту інформаційного об'єкту) будемо вважати, що об'єктом захисту є інформаційні ресурси певної ЛОМ, а засоби технічного захисту ресурсів такої ЛОМ, виходячи із наданої на рис. 1 узагальненої моделі загроз інформаційному об'єкту ЛОМ, складаються із засобів організаційного обмеження доступу, охоронної сигналізації, адміністрування доступу – внутрішньомережевих засобів управління доступом до ресурсів ЛОМ, засобів захисту від витоків інформації технічними каналами, засобів захисту від спеціальних впливів на інформацію технічними каналами та засобів антивірусного захисту і забезпечують реалізацію певного набору функцій щодо обслуговування множини запитів.

З розглянутого витікає, що загрози об'єкту захисту (інформаційним ресурсам певної ЛОМ) можуть здійснюватися шляхом несанкціонованого доступу (НСД), тобто шляхом подолання порушником:

1. Засобів організаційного обмеження доступу.
2. Засобів управління фізичним доступом.
3. Засобів охоронної сигналізації.
4. Внутрішньомережевих засобів управління доступом – засобів адміністрування доступу (проблемно – орієнтованих засобів захисту базового програмного забезпечення – операційних систем та систем керування базами даних (при їх наявності).
5. Засобів захисту в телекомунікаційних мережах (в разі підключення ЛОМ до розподілених чи глобальних інформаційно – телекомунікаційних мереж).
6. Засобів антивірусного захисту (засобів захисту від впровадження комп'ютерних вірусів).

Окрім того, впливи на інформаційні об'єкти можливі за рахунок використання: технічних каналів побічних електромагнітних випромінювань і наведень; каналів спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту чи порушення цілісності інформації.

Після розгляду такої узагальненої графічної моделі загроз інформаційному об'єкту ЛОМ можна виконати **третій етап** – розробити графічні моделі взаємодії загроз із засобами протидії цим загрозам по відношенню до кожної з властивостей захищеності інформації ЛОМ. На цьому етапі оцінку захищеності інформаційних ресурсів ЛОМ пропонується розглядати по відношенню **до кожної з функціональних властивостей захищеності інформації ЛОМ**.

Графічна модель взаємодії засобів реалізації атак із засобами протидії цим загрозам - засобами **забезпечення конфіденційності інформації** представляється авторам так, як це подано на рис. 2. На цьому рисунку ЗК - загрози конфіденційності.

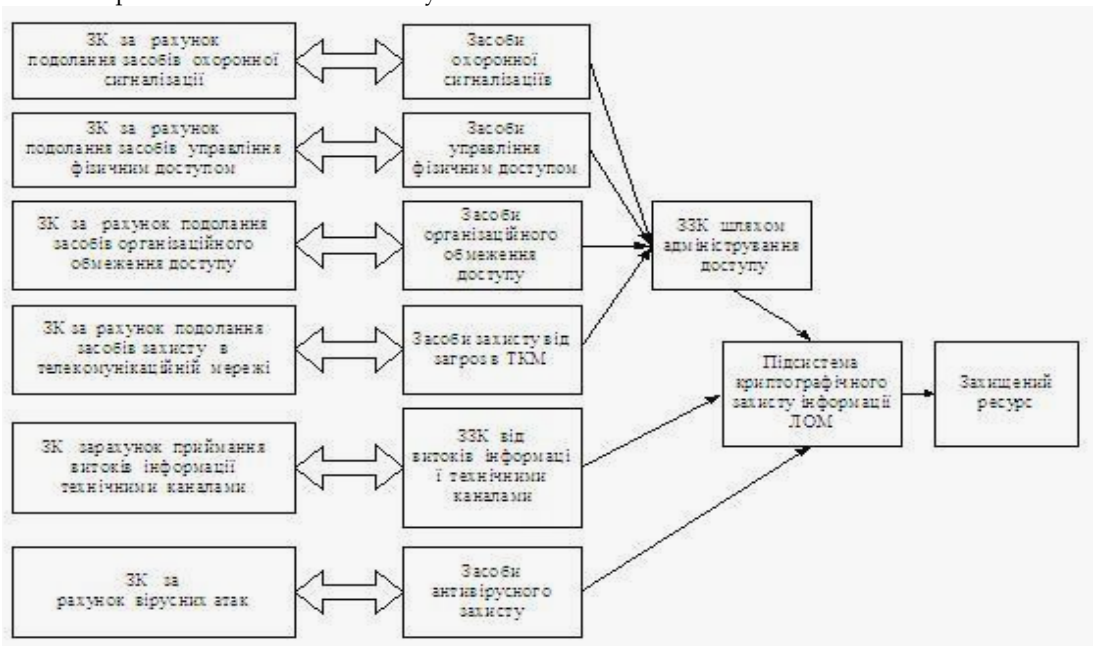

Рис. 2. Графічна модель процесу взаємодії засобів реалізації атак із засобами забезпечення конфіденційності інформації в ЛОМ

Як витікає із цієї графічної моделі, несанкціоноване отримання користувачем інформації чи ознайомлення з нею тим чи іншим чином є можливим з імовірністю $q_{пк}$ при умові:

1. Подолання неавторизованим користувачем із ймовірністю подолання $q_{кзі}$ засобів криптозахисту (одержання можливості розкрити зміст інформації з обмеженим доступом) інформації засобів підсистеми криптографічного захисту.
2. Несанкціонованого доступу до інформаційних ресурсів з імовірністю такої події q_1 з подоланням, в свою чергу, засобів:

а. охоронної сигналізації, тобто шляхом "обходу" засобів організаційного обмеження доступом. Такі дії слід очікувати, скоріше за все, від "рішучих зловмисників", які мають на меті будь-що порушити ту чи іншу властивість захищеної інформації;

b. організаційного обмеження доступу – недотримання порушниками, у тому числі персоналом підрозділів, у яких використовуються ЛОМ, посадових інструкцій, наказів та розпоряджень керівництва щодо забезпечення безпеки інформації тощо;

c. управління доступом, включаючи засоби управління фізичним доступом (дозвіл чи блокування доступу до приміщень, терміналів, системних блоків, клавіатури та інших фізичних засобів) та адміністрування доступу (адміністрування суб'єктів, об'єктів, побудови і реалізації моделі захищеної системи, розмежування доступу тощо). Такі дії слід очікувати, скоріше за все, від "терплячих зловмисників", які порушують політику безпеки даної послуги навмисно, але без рішучих дій, маскуючись, шляхом підбору атрибутів доступу інших користувачів з метою прихованого подолання засобів управління (адміністрування) доступом до інформації, або від "випадкових порушників" - авторизованих користувачів, які порушують конфіденційність не навмисно, а помилково – шляхом випадкового подолання засобів управління (адміністрування) доступом до об'єкту захисту, виконання непередбачених дій відносно цього інформаційного об'єкту та т.п.;

d. засобів захисту в телекомунікаційній мережі (в разі використання ЛОМ, яка є підключеною до інших ЛОМ ВАТ чи є елементом розподіленої мережі більш високого рівня.

3. Подолання із ймовірністю $q_{св}$ засобів захисту інформації від витоків технічними каналами.

4. Подолання із ймовірністю $q_{ав}$ засобів антивірусного захисту – засобів захисту від вірусних атак, спроможних перевести захищений інформаційний ресурс із розряду конфіденційного до розряду відкритого.

Графічна модель взаємодії засобів реалізації атак із засобами протидії цим загрозам – засобами **забезпечення цілісності та доступності інформації** з урахуванням загроз із телекомунікаційних мереж та відповідних засобів захисту представлена на рис. 3 (на цьому рис. ЗЦ – загрози цілісності). Використати для оцінки цілісності і доступності інформації єдину графічну модель дозволяє наведене вище трактування Нормативними документами Системи технічного захисту України [1-3] цих функціональних властивостей захищеності, коли доступність розглядається, зокрема, як властивість інформації, що полягає в тому, що інформація знаходиться у вигляді, необхідному користувачеві (тобто є не модифікованою), і в той час, коли вона йому необхідна. Тобто порушення цілісності є, одночасно, і порушенням доступності.

При цьому, як і для моделі взаємодії засобів реалізації загроз конфіденційності інформації та засобів протидії цим загрозам, подолання неавторизованим користувачем системи захисту цілісності з імовірністю $q_{пц}$ можливе, якщо:

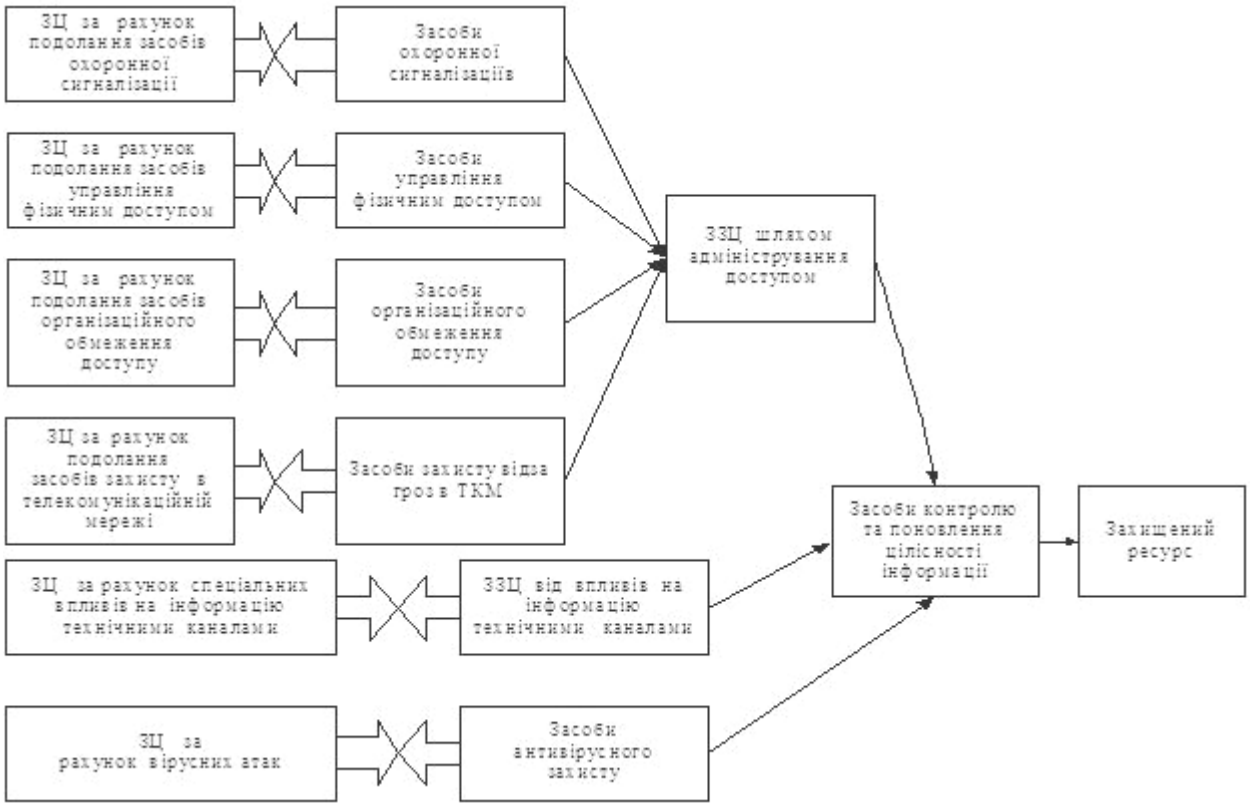

Рис. 3. Графічна модель процесу взаємодії засобів реалізації атак із засобами забезпечення цілісності та доступності інформації в ЛОМ

1. Подолано засоби захисту від несанкціонованого доступу (охоронної сигналізації, організаційного обмеження доступу, засоби управління фізичним доступом (дозвіл чи блокування доступу до приміщень, терміналів, системних блоків, клавіатури та інших фізичних засобів) та адміністрування доступу (адміністрування суб'єктів, об'єктів, побудови і реалізації моделі захищеної системи, розмежування

доступу тощо)). Імовірність такої події q_1 уже визначена раніше.

2. З імовірністю $q_{св}$ подолано засоби захисту від спеціальних впливів на інформацію технічними каналами.

3. З імовірністю $q_{ав}$ подолано засоби антивірусного захисту, спроможні здійснити ту чи іншу модифікацію (порушення цілісності) інформаційного об'єкту.

4. З імовірністю $q_{кц}$ подолано засоби контролю та поновлення цілісності інформації.

З урахуванням наведених вище зауважень, слід вважати, що ***подолання неавторизованим користувачем системи захисту доступності*** з імовірністю $q_{пд}$ можливе, якщо:

1. З імовірністю $q_{пц}$ порушено цілісність інформаційного об'єкту.

2. Порушено правила, встановлені політикою безпеки, щодо часу очікування авторизованим користувачем доступу до інформації (користувач очікує довше заданого (малого) проміжку часу або інформація не знаходиться користувачем в той час, коли вона йому необхідна). Останню ситуацію слід розглядати як штучну відмову в обслуговуванні, а порядок розрахунку відповідної ймовірності потребує окремого розгляду.

Висновки

В статті з метою оцінки захищеності інформації в ЛОМ запропоновано використання графічних моделей процесів взаємодії засобів реалізації атак із засобами забезпечення основних функціональних властивостей захищеності інформації. Такі моделі дозволяють здійснювати обгрунтований вибір сукупностей засобів захисту та здійснити, в подальшому оцінку величин залишкових ризиків – ймовірностей порушення конфіденційності, цілісності, доступності та подолання злому комплексної системи захисту.

Література

[1] Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу (НД ТЗІ 1.1 – 002 – 99);

[2] Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу (НД ТЗІ 2.5 – 004 – 99);

[3] Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу (НД ТЗІ 2.5 – 005 – 99);

[4] Типове положення про службу захисту інформації в автоматизованій системі (НД ТЗІ 1.4 – 001 – 2000);

[5] Будько М.М. Варіант формалізації процесу захисту інформації в комп'ютерних системах та оптимізації його цільової функції. / М.М. Будько, В.С. Василенко В.С. // Реєстрація, зберігання і обробка даних. - 2000. - № 2, том 2. с. 73 - 84.

[6] Будько М.М. Оцінка залишкового ризику при застосуванні засобів захисту інформації від НСД в корпоративних системах. / М.М. Будько, В.С. Василенко В.С. // К.: Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова, Матеріали науково – практичної конференції "Інформаційні технології в енергетиці", 2002, с. 29 – 39.

[7] Матов О.Я., Визначення залишкового ризику при оцінці захищеності інформації в інформаційно – телекомунікаційних системах. / Матов О.Я., Василенко В.С., Будько М.М // К.: Реєстрація, зберігання і обробка даних, 2004, Т. 6, № 2, с. 62 – 74.

УДК 004.056.2 (045)

Василенко В.С., Дубчак Е.В., Василенко Н.Ю. Методика оценки защищенности информации в ЛВС. Графические модели взаимодействия угроз функциональным свойствам защищенности информационных ресурсов ЛВС с елементами системы защиты

Аннотация. *В статье предложено использование графических моделей взаимодействия угроз функциональным свойствам защищенности информационных ресурсов ЛВС с элементами системы защиты, которые позволяют определить состав таких систем и, в дальнейшем, оценить возможные остаточные риски при обеспечении конфиденциальности, доступности и целостности информационных объектов в телекоммуникационных системах.*

Ключевые слова: *конфиденциальность, целостность, доступность информации, остаточные риски, локальные вычислительные сети.*

Vasylenko V.S., Dubchak O.V., Vasylenko M.Yu. Methods of assessment of information security in a LAN. Graphical interaction models threats functional properties of security of information resources with elements LAN security

Abstract. *The paper proposes the use of graphical interaction models threats functional properties of security of information resources of the LAN security system elements that allow the composition of such systems and, further, to evaluate possible residual risks while ensuring confidentiality, integrity and availability of information objects in telecommunication systems.*

Keywords: *confidentiality, integrity and availability of information, residual risks, local area networks.*

Отримано *29 березня 2012 року,* затверджено редколегією *07 червня 2012 року*
(рецензент д.т.н., професор О.К. Юдін)