2 Забазпечення комп'ютерної безпеки в інформаційних системах

УДК 681.3

МЕТОДИКИ ВИЗНАЧЕННЯ ЗАЛИШКОВИХ РИЗИКІВ У ЛОМ

Вячеслав Василенко
Національний авіаційний університет

Анотація: **Для оцінки захищеності інформації автоматизованих систем запропоновано моделі відповідних систем захисту інформації та застосування ймовірностей подолання порушником засобів захисту тих чи інших властивостей захищеності – величин залишкового ризику; наведені вирази для їх розрахунків.**
Summary: **For estimation of protected of information of the automated systems the models of the proper systems of defenses of information and application of probabilities of overcoming by the violator of facilities of defense of those or other properties of protected are offered – sizes of remaining risk, resulted expressions for their calculations.**
Ключові слова: **Інформація, конфіденційність, доступність, цілісність, оцінка ризиків.**

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.

Для визначення вимог та оцінки захищеності інформації використовуються [1] критерії оцінки захищеності. Відомо також, що досягнуті результати із забезпечення ефективності захисту можна оцінювати або величиною можливих збитків по кожному з класів порушень, або за допомогою залишкового ризику чи інших показників ефективності захищених систем, застосування яких рекомендується в [1]. 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 оптимізації параметрів систем захисту).

На відміну від цього в даній статті пропонуються методики визначення кількісних показників захищеності інформації в ЛОМ – величин залишкових ризиків [2].

Як величини залишкового ризику в методиках пропонується використання ймовірностей: *порушення цілісності* – $q_{пц}$, *порушення конфіденційності* – $q_{пк}$, *порушення доступності* – $q_{пд}$ та *подолання, злому комплексної системи захисту* – q.

Для визначення залишкового ризику за допомогою відповідних методик необхідно:

1) визначити (побудувати) моделі порушників та загроз відповідним ресурсам ЛОМ, визначити для кожної із функціональних властивостей захищеності (конфіденційності, цілісності, доступності) найбільш суттєві із цих загроз; визначити сукупність засобів та побудувати модель системи захисту від цих загроз;

2) детально проаналізувати взаємодію загроз (засобів реалізації атак), спрямованих на подолання механізмів забезпечення захищеності інформації ЛОМ, із засобами протидії цим загрозам; визначити вирази для обрахування величин залишкового ризику.

У даних методиках припускається, що службою захисту інформації відповідного підприємства моделі порушників та загроз побудовані, найбільш суттєві загрози відповідним ресурсам ЛОМ визначені. У цій статті до найбільш суттєвих загроз віднесено: 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.

Виходячи з цього, методики оцінки по кожній із функціональних властивостей захищеності інформаційних ресурсів ЛОМ складаються із наступних типових етапів:

1) побудова графічних моделей взаємодії загроз відповідній функціональній властивості захищеності інформаційних ресурсів ЛОМ із відповідними засобами захисту;

2) оцінка величин залишкових ризиків у ЛОМ;

3) визначення вихідних даних для оцінки залишкових ризиків у ЛОМ.

І Графічні моделі взаємодії засобів захисту із загрозами функціональним властивостям захищеності інформаційних ресурсів ЛОМ

Для побудови графічних моделей взаємодії засобів захисту із відповідними загрозами функціональним властивостям захищеності інформаційних ресурсів ЛОМ слід виконати наступні етапи :

1) сформулювати моделі порушників та загроз (здійснюється службою захисту інформації підприємства);

2) визначити, хоча б у загальному вигляді, засоби протидії загрозам як елементи моделі захисту інформаційного об'єкту;

3) розробити графічні моделі (часткові моделі та узагальнену) взаємодії загроз із засобами протидії цим загрозам.

На другому етапі (визначення часткових моделей захисту інформаційного об'єкту) будемо вважати, що об'єктом захисту є інформаційні ресурси певної ЛОМ. Побудову графічних моделей доцільно розпочати із визначення узагальненої графічної моделі загроз ресурсам локальних обчислювальних мереж (ЛОМ). Найчастіше таку модель можна представити у вигляді, який наведено на рис. 1.

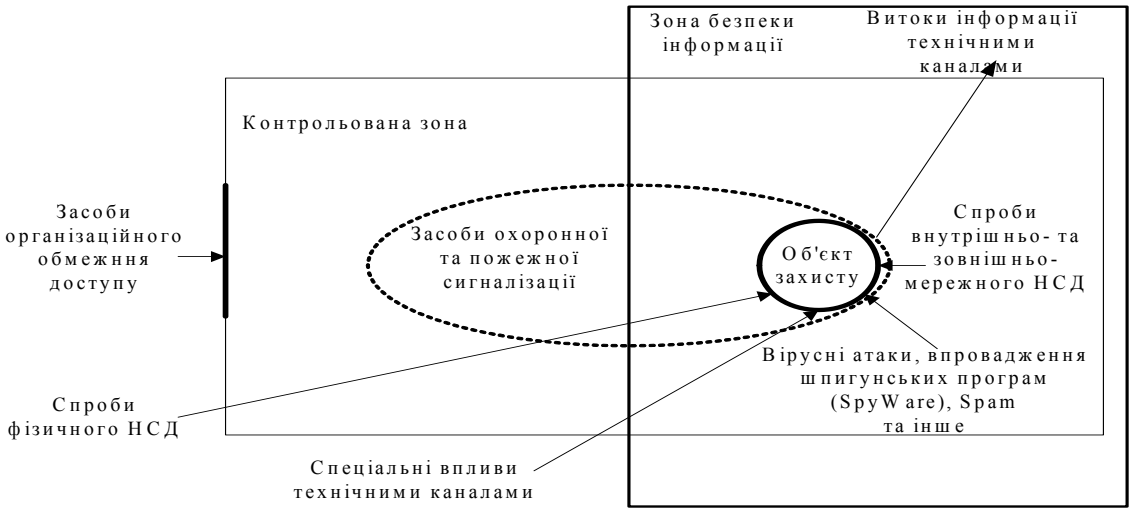

Рисунок 1 – Узагальнена графічна модель загроз інформаційному об'єкту ЛОМ

З цієї узагальненої моделі випливає, що загрози об'єкту захисту (інформаційним ресурсам певної ЛОМ) можуть здійснюватися шляхом несанкціонованого доступу (НСД), тобто шляхом подолання порушником засобів:

1) організаційного обмеження доступу;

2) управління фізичним доступом;

3) охоронної сигналізації;

4) внутрішньомережних управління доступом – засобів адміністрування доступу (проблемно – орієнтованих засобів захисту базового програмного забезпечення – операційних систем та систем керування базами даних (при їх наявності);

5) захисту в телекомунікаційних мережах (в разі підключення ЛОМ до розподілених чи глобальних інформаційно – телекомунікаційних мереж);

6) захисту від впровадження комп'ютерних вірусів, шпигунських програм (SpyWare), спамів, засобів неконтрольованого завантаження вірусів, троянських і шпигунських програм Trojan-Downloader тощо – **в подальшому засобів антивірусного захисту**.

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 уже можна розробити часткові графічні моделі взаємодії загроз із засобами протидії цим загрозам по відношенню до кожної з властивостей захищеності інформації ЛОМ.

Третій етап методики також слід розглядати відносно кожної з функціональних властивостей захищеності інформації ЛОМ.

1.1. Часткова графічна модель взаємодії засобів реалізації атак із засобами протидії цим загрозам - засобами забезпечення конфіденційності інформації

Графічна модель взаємодії засобів реалізації атак із засобами протидії цим загрозам - засобами **забезпечення конфіденційності інформації,** представлена на рис. 2. На цьому рисунку ЗК - загрози конфіденційності, ЗЗК – засоби забезпечення конфіденційності, ТКМ – телекомунікаційна мережа.

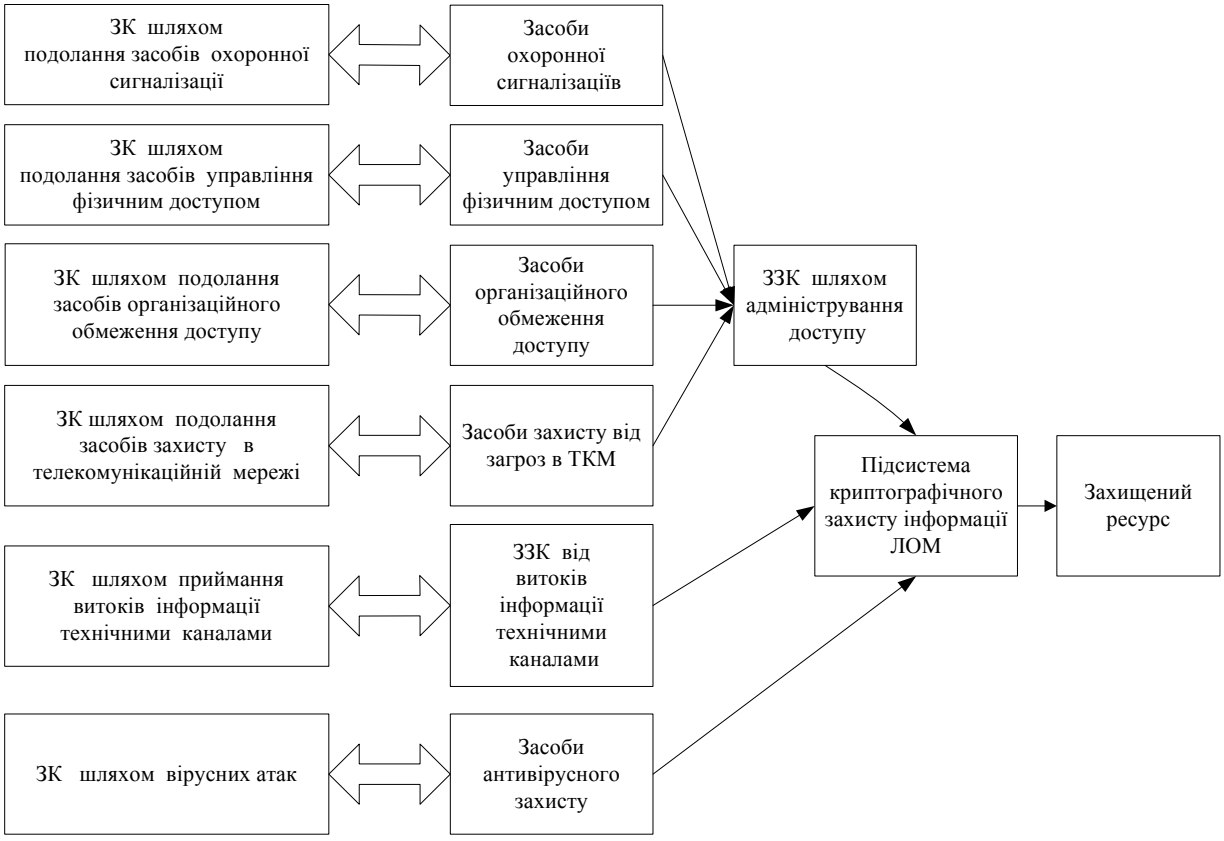

Рисунок 2 – Графічна модель процесу взаємодії засобів реалізації атак із засобами забезпечення конфіденційності інформації в ЛОМ

Примітка 1. У даній графічній моделі передбачено наявність загроз та відповідних засобів захисту конфіденційності шляхом подолання засобів захисту в телекомунікаційній мережі, що не завжди є притаманним ЛОМ підприємств, оскільки в деяких із них можуть використовуватися лише відокремлені ЛОМ підрозділів чи, навіть відокремлені ПЕОМ. Але з урахуванням можливого об'єднання окремих ЛОМ у розподілену обчислювальну мережу підприємства, чи приєднання окремих ЛОМ до інших обчислювальних мереж (наприклад, деяких глобальних обчислювальних мереж) цей підхід може бути корисним і для цих підприємств.

Як витікає із даної графічної моделі, несанкціоноване отримання користувачем інформації чи ознайомлення з нею тим чи іншим чином є можливим за умови:

1) подолання неавторизованим користувачем засобів криптографічного захисту;
2) несанкціонованого доступу до інформаційних ресурсів з подоланням, в свою чергу, засобів:

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

- 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 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.;
- засобів захисту в телекомунікаційній мережі (в разі використання ЛОМ, яка є підключеною до інших ЛОМ підприємства чи є елементом розподіленої мережі більш високого рівня);
- засобів захисту від витоків інформації технічними каналами;
- засобів захисту від вірусних атак (засобів антивірусного захисту), спроможних перевести захищений інформаційний ресурс із розряду конфіденційного до розряду відкритого.

1.2. Графічна модель взаємодії засобів реалізації атак із засобами протидії цим загрозам – засобами забезпечення цілісності та доступності інформації

Графічна модель взаємодії засобів реалізації атак із засобами протидії цим загрозам – засобами забезпечення цілісності та доступності інформації з урахуванням наведеної вище примітки 1 щодо загроз із телекомунікаційних мереж та відповідних засобів захисту, представлена на рис. 3 (на цьому рис. ЗЦ – загрози цілісності).

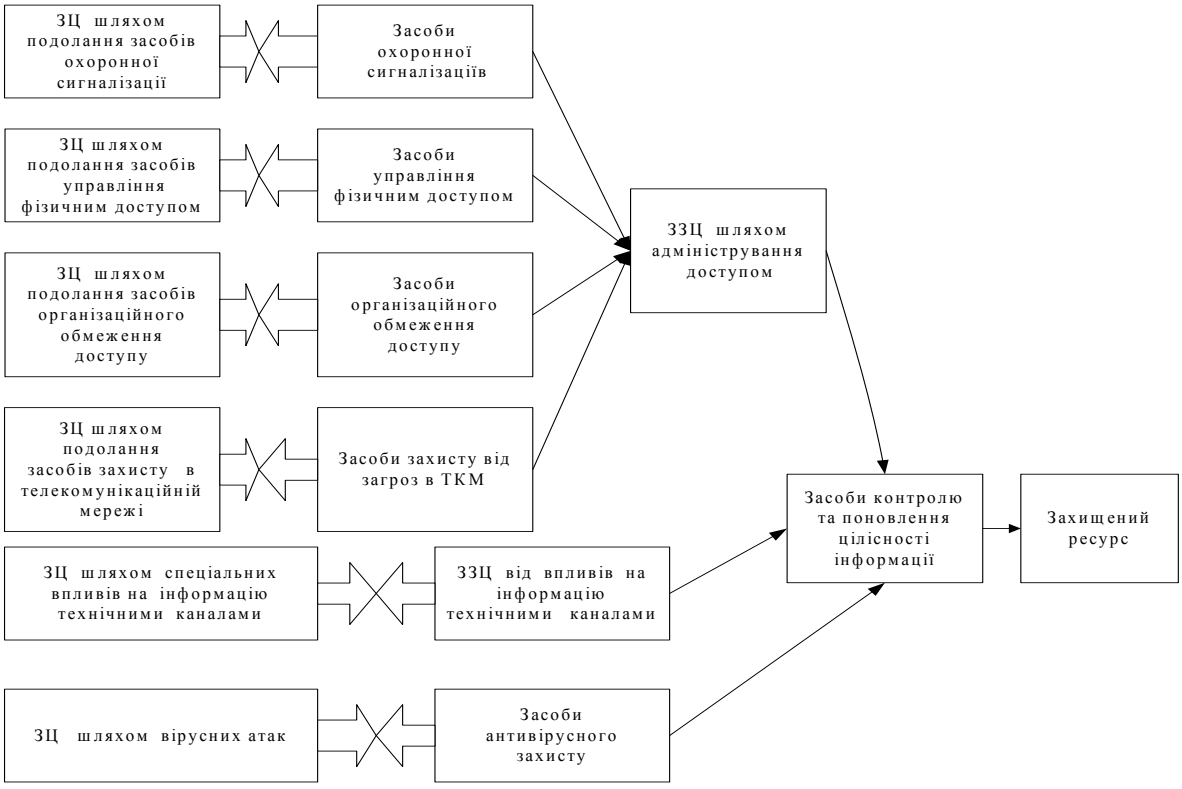

Рисунок 3 – Графічна модель процесу взаємодії засобів реалізації атак із засобами забезпечення цілісності та доступності інформації в ЛОМ

Використати для оцінки цілісності і доступності інформації єдину графічну модель дозволяє наведене вище трактування Нормативними документами Системи технічного захисту України 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 і 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:

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, спроможних 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:

- з імовірністю $q_{пц}$ порушено цілісність інформаційного об'єкту;
- 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).

Остання ситуація в методиці розглядається як штучна відмова в обслуговуванні, а порядок розрахунку відповідної ймовірності викладено нижче.

II Методики оцінки залишкових ризиків

2.1. Оцінка залишкового ризику при забезпеченні конфіденційності

Для оцінки залишкового ризику при забезпеченні конфіденційності (ймовірність отримання інформації порушником з розкриттям змісту) із врахуванням висновків, отриманих при розгляді **графічної моделі** взаємодії засобів реалізації атак із засобами протидії цим загрозам – засобами **забезпечення конфіденційності інформації** (рис. 2), подію, пов'язану з порушенням конфіденційності, слід розглядати як складну та таку, що складається з подій [4]:

1) несанкціонованого отримання користувачем інформації тим чи іншим чином (несанкціонований доступ) з метою ознайомлення з нею чи будь-якого подальшого використання;

2) розкриття змісту інформації з обмеженим доступом (ІзОД) після отримання її тим чи іншим; останнє слід трактувати як можливість подолання порушником відповідних засобів криптозахисту.

При цьому ймовірність несанкціонованого доступу q_1 можна визначити з виразу:

$$q_1 = q_{ад}\cdot[1-(1-q_{ос})\cdot(1-q_{уфд})\cdot(1-q_{оод})\cdot(1-q_{кткм})], \qquad (1)$$

де: $q_{ад}$ – ймовірність подолання засобів адміністрування доступом;

$q_{ос}$ – ймовірність подолання засобів охоронної сигналізації;

$q_{уфд}$ – ймовірність подолання засобів управління фізичним доступом;

$q_{оод}$ – ймовірність подолання засобів організаційного обмеження доступу;

$q_{кткм}$ – ймовірність порушення конфіденційності в засобах телекомунікаційної мережі (в разі використання ЛОМ, яка є підключеною до інших ЛОМ підприємства чи є елементом розподіленої мережі більш високого рівня).

Примітка 2. Тут і надалі ймовірність подолання відповідного захисту за відсутності певних загроз того чи іншого виду вважається такою, що дорівнює нулю, а за відсутності засобів захисту від таких загроз – такою, що дорівнює одиниці.

Примітка 3. Звернемо увагу на можливість трансформації частини виразу (1) для обчислення ймовірності несанкціонованого доступу q_1. З цією метою розглянемо добуток у квадратних дужках:

$$(1-q_{ос})\cdot(1-q_{уфд})\cdot(1-q_{оод})\cdot(1-q_{кткм}) = \prod_{i=1}^{n}(1-q_i),$$

який через розклад у ряд Маклорена із обмеженням першими двома членами такого ряду можна представити у вигляді

$$\prod_{i=1}^{n}(1-q_i) = (1-q_{ос})\cdot(1-q_{уфд})\cdot(1-q_{оод})\cdot(1-q_{кткм}) \approx 1 - \sum_{i=1}^{n} q_i \ .$$

Це є можливим через те, що величини ймовірностей p_i є суттєво меншими за одиницю і тому іншими членами ряду, які є сумами різних добутків цих же величин p_i (третій член ряду – сума подвійних добутків, четвертий – сума потрійних добутків та т. інш.) можна знехтувати. У свою чергу, в останній сумі також можна обмежитися її найбільшим членом, знехтувавши іншими, меншими, членами. Тобто вираз (1) може набути вигляду

$$q_1 = q_{ад}\cdot[1-(1-q_{ос})\cdot(1-q_{уфд})\cdot(1-q_{оод})\cdot(1-q_{кткм})] = q_{ад}\cdot q_2, \qquad (2)$$

де $q_2 = \max(q_{ос}, q_{уфд}, q_{оод}, q_{кткм})$.

Окрім того, несанкціоноване отримання користувачем інформації є можливим і через засоби віддаленого доступу до інформаційних об'єктів, використовуючи витоки інформації технічними каналами, вірусні атаки та засоби телекомунікаційної мережі за умови подолання неавторизованим користувачем відповідних засобів захисту. Нехай імовірність подолання засобів захисту від витоків інформації технічними каналами дорівнює $q_{зв}$, а ймовірність подолання засобів антивірусного захисту – $q_{ав}$.

Після отримання ІзОД тим чи іншим шляхом порушнику необхідно здійснити розкриття її змісту. Подія, яка полягає в тому, що порушник може розкрити зміст ІзОД (за умови подолання системи захисту даного інформаційного об'єкту) є також складною і складається з трьох подій: першої – порушник знає мову, якою інформація представляється; другої – порушник знає і може застосувати програмні засоби або апаратуру для криптографічного перетворення (для дешифрування закритої інформації); третьої – має необхідні ключі (ключові набори) для такого перетворення. Імовірності цих подій $P_{зм}$, $P_{зкп}$, $P_{кн}$ відповідно.

При цьому $q_{кзі}$ – ймовірність подолання неавторизованим користувачем засобів криптозахисту (можливість розкрити зміст ІзОД) інформації можна визначити з виразу:

$$q_{кзі} = P_{зм}\cdot P_{зкп}\cdot P_{кн}.$$

Тоді вираз для розрахунку ймовірності $q_{пк}$ порушення конфіденційності інформації з подоланням розглянутих засобів захисту із врахуванням результатів примітки 3 можна записати у вигляді

$$q_{пк} = q_{кзі}\cdot[1-(1-q_1)\cdot(1-q_{зв})\cdot(1-q_{ав})] \approx q_{кзі}\cdot q_3, \qquad (3)$$

де $q_3 = \max(q_1, q_{зв}, q_{ав})$.

Розглянута модель дозволяє зробити висновок про те, що для забезпечення конфіденційності шляхом унеможливлення доступу неавторизованих користувачів до інформації та розкриття її змісту необхідно застосовувати засоби (апаратурні чи програмні) для адміністрування доступу, для криптографічного перетворення (для шифрування та дешифрування закритої інформації, а також засоби генерації та розповсюдження ключів), засоби управління фізичним доступом, засоби охоронної сигналізації, організаційного обмеження доступом та засоби антивірусного захисту.

Аналіз отриманих виразів дозволяє зробити наступні висновки. По-перше, із виразів (2), (3) із врахуванням примітки 3 витікає, що слабкість системи захисту (як і в теорії "слабкості ланцюга") визначається найбільш слабкою ланкою цієї системи, а отже має сенс застосування в системі захисту елементів із приблизно рівними ймовірностями їх подолання. По-друге, у цих виразах можна виділити домінуючі ймовірності, наприклад, у виразі (2) домінуючою є величина ймовірності подолання засобів адміністрування доступом $q_{ад}$, тобто ця величина найбільш суттєво впливає на загальну ймовірність несанкціонованого доступу q_1. Нарешті, подія, яка полягає в подоланні системи захисту конфіденційності, може бути зведеною до двох подій – подолання засобів адміністрування доступу та подолання засобів криптографічного захисту, а за відсутності останніх – лише до подолання засобів адміністрування доступу.

2.2. Оцінка залишкового ризику при забезпеченні цілісності

Для оцінки залишкового ризику при забезпеченні цілісності подію, пов'язану з її порушенням, слід розглядати як складну та таку, що складається з подій[5]:

- виведення з ладу, зміни режимів функціонування або несанкціонованого використання засобів зберігання носіїв інформації і порушення, таким чином, її цілісності;
- несанкціонованої модифікації (зміни, підміни, знищення та т. п.) ІзОД у середовищах її оброблення, зберігання чи передавання з метою унеможливлення подальшого її використання чи нанесення іншої шкоди власнику даного ресурсу.

Тоді, з використанням застосованих вище підходів, імовірність порушення цілісності $q_{пц}$ можна знайти з виразу

$$q_{пц} = q_{кц}\,[1-(1-q_1)\cdot(1-q_{св})\cdot(1-q_{ав})].$$

Виходячи із отриманих вище результатів, можна записати

$$q_{пц} \approx q_{кц} \cdot q_4,$$

де, як і раніше, $q_4 = \max (q_1, q_{св}, q_{ав})$.

Розглянута модель дозволяє зробити, по-перше, висновок про те, що для забезпечення цілісності шляхом унеможливлення доступу до інформації та модифікації неавторизованим користувачем змісту інформаційного об'єкту необхідно застосовувати засоби (апаратурні чи програмні) для контролю цілісності, адміністрування доступу, управління фізичним доступом, засоби охоронної сигналізації та організаційного обмеження доступом.

По-друге, з останнього витікає необхідність, на відміну від моделі взаємодії засобів реалізації загроз та засобів забезпечення конфіденційності, застосування для забезпечення цілісності інформаційних об'єктів засобів з відповідними механізмами контролю цілісності та замість засобів захисту від витоків – засобів захисту від спеціального впливу. Окрім того, для унеможливлення порушення цілісності за рахунок отримання неавторизованим користувачем доступу до інформації з обмеженим доступом слід застосовувати такі ж засоби управління доступом (апаратурні чи програмні), як і для забезпечення конфіденційності.

Примітка 4. Звернемо увагу на те, що із наведеного вище визначення цілісності, як функціональної властивості захищеності інформації, не витікає ніяких часових обмежень щодо тривалості процесу поновлення цілісності, у разі виявлення засобами контролю наявності її порушення. Це дає змогу для забезпеченні цілісності використовувати і ручні методи, наприклад, поновлення із застосуванням резервних копій інформаційних об'єктів чи шляхом забезпечення відкоту процесів у разі виявлення порушення цілісності.

2.3. Оцінка залишкового ризику при забезпеченні доступності

Виходячи із наведеного вище визначення функціональної властивості доступності інформації та **графічної моделі** взаємодії засобів реалізації атак із засобами протидії цим загрозам – засобами **забезпечення цілісності та доступності інформації** (рис. 3), **для оцінки залишкового ризику при забезпеченні доступності** подію, пов'язану з її порушенням, слід розглядати як наслідок впливу на інформаційний об'єкт загроз, найбільш суттєвими з яких є [4, 5]:

1) несанкціонована модифікація інформаційного ресурсу (порушення цілісності – вигляду ресурсу, необхідного користувачеві), включаючи зміни режимів його функціонування, місця зберігання, необхідного чи заданого користувачем, що потребує поновлення цілісності ресурсу шляхом, наприклад, використання його резервної копії; така подія передбачає можливість фізичного доступу до джерел чи носіїв інформаційних ресурсів, наявність реалізованої спроби несанкціонованого доступу до інформаційного ресурсу, в тому числі каналами ТКМ та каналами спеціального впливу (порушник зумів здійснити маскування під авторизованого користувача чи модифікація не виявлена засобами контролю цілісності);

2) переведення ресурсу в режим штучної відмови шляхом:

- несанкціонованого використання інформаційного ресурсу в той час, коли ресурс є необхідним користувачеві, та протягом часу довше заданого (малого) проміжку – шляхом захоплення ресурсів (неконтрольованого використання, утримання, занадто тривалого використання) і створенню, таким чином перешкод іншим користувачам в використання цих ресурсів;
- постійного використання ресурсу, наприклад, шляхом генерації потоку заважаючих запитів (несправжніх запитів на обслуговування, несправжніх пакетів вхідної інформації, спроб підбору паролів, спамів (Spam) та т. п. – завад процесу обслуговування справжніх запитів) з такою інтенсивністю, коли їх період (середня тривалість проміжку часу між двома сусідніми запитами) не перевищує тривалості обслуговування кожного з таких запитів, тобто такого потоку, коли захищений ресурс призначається для обслуговування лише заважаючих запитів;
- постійного порушення цілісності з періодичністю, меншою ніж час відновлення інформаційного ресурсу. Така подія передбачає наявність порушень цілісності шляхом впливу природних факторів (збої, відмови), а також наявність реалізованих спроб несанкціонованого доступу до інформаційного ресурсу каналами спеціального впливу (без спроб маскування).

Імовірність першої із цих подій визначено вище (з використанням моделі, представленої на рис. 3) і вона дорівнює $q_{пц}$.

Для оцінки ймовірності порушення доступності шляхом переводу ресурсу в режим штучної відмови необхідно визначити інтенсивність потоку впливів на доступність ресурсу. Для цього скористаємося відомими з [6] підходами для розрахунку результуючої інтенсивності як природних, так і штучних впливів на інформаційні ресурси технічними каналами. *Під природними впливами* будемо розуміти потоки будь-яких подій, які здатні вивести ЛОМ з ладу тимчасово (збої, для яких є характерним самоусунення), чи на тривалий термін (відмови, усунення яких вимагає втручання персоналу), тобто *потоки відмов*. Причинами таких

впливів може бути недостатня спроможність уже згаданих первинних технічних засобів запобігти дії таких впливів, недостатня надійність засобів ЛОМ, виходи за межі допустимих значень температури, вологості, радіаційного чи електромагнітного випромінювання, яке впливає на елементи ЛОМ, та т. п. Такі події впливають як безпосередньо на інформаційні ресурси ЛОМ, так і на засоби технічного захисту цієї системи. При цьому стійкість ЛОМ до природних загроз визначається в основному такою її властивістю як надійність і забезпечується відповідними заходами (резервування – гаряче та холодне, застосування елементів підвищеної надійності та т. інш.). Для боротьби зі збоями, які призводять до порушення цілісності програмних засобів та оброблюваної інформації, можна застосовувати засоби контролю та поновлення цілісності чи інші засоби поновлення після збоїв.

Під штучними впливами розуміються ті події, які є наслідком діяльності користувачів, як авторизованих, так і неавторизованих стосовно ресурсів ЛОМ, що є з якихось причин забороненими для даних користувачів. Такі впливи – спроби НСД можуть бути випадковими (внаслідок помилки користувача), або зловмисними, тобто спеціальними, з метою використання чи то ресурсів, чи то інформації ЛОМ.

Таким чином, на інформаційні ресурси ЛОМ можуть впливати як спроби несанкціонованого доступу, за умови подолання систем управління доступом та фільтрації, так і безпосередньо природні впливи.

Будемо вважати потік загроз найпростішим з інтенсивністю $\lambda_з$. Зрозуміло, що цей потік складається зі штучних загроз з інтенсивністю $\lambda_ш$ та природних з інтенсивністю λ, так що $\lambda_з = \lambda_ш + \lambda$. У свою чергу, штучні загрози можуть бути внутрішніми з інтенсивністю $\lambda_{шв}$ (з боку авторизованих чи неавторизованих користувачів ЛОМ чи її елементів) та зовнішніми з інтенсивністю $\lambda_{шз}$. Виявлення і подальша протидія загрозі (ймовірність захисту ЛОМ від загроз) залежить від того, чи запобігла (не допустила) система ТЗІ впливу цієї загрози, чи встановила факт її впливу і ліквідувала відповідні наслідки.

Ця задача вирішується, по-перше, шляхом управління доступом до інформаційних ресурсів ЛОМ (ідентифікація, автентифікація, надання певних повноважень чи привілеїв з наступною їх перевіркою під час кожної зі спроб доступу до ресурсів). Для цього в системі ТЗІ повинен виділятись адміністратор (адміністратор безпеки), який і вирішує усі ці питання, зрозуміло з використанням засобів системи захисту, можливо через спеціальним чином обладнане автоматизоване робоче місце (АРМ) адміністратора безпеки. Зауважимо, що оскільки адміністратор безпеки має, як правило, найширші права щодо управління доступом до ресурсів ЛОМ, то захопивши його повноваження можна порушити процес надання цією ЛОМ будь–якої функціональної послуги.

Тому слід уважати, що стійкість (в розумінні ймовірності не подолання) системи управління доступом $p_д = 1 - q_1$ визначається стійкістю процесів ідентифікації та автентифікації самого адміністратора безпеки, як користувача з найширшими повноваженнями. Останнє визначається можливостями системи ідентифікації та автентифікації (наприклад, кількістю можливих варіантів ідентифікаторів та кількістю можливих варіантів паролів і надійністю їх конфіденційного зберігання). Унаслідок відсіву (фільтрації) внутрішніх впливів системою управління доступом на її виході інтенсивність завад буде дорівнювати $\lambda_{шв} \cdot q_1$.

Ця задача може вирішуватися, по-друге, застосуванням у ЛОМ засобів фільтрації зовнішніх штучних впливів (від елементів розподіленої обчислювальної мережі через засоби телекомунікаційної мережі в разі наявності підключення даної ЛОМ до розподілених чи глобальних інформаційно – телекомунікаційних мереж), які впливають на дану ЛОМ (засоби фільтрації типу міжмережних екранів (firewall, брандмауерів), сервісів – посередників (proxy services) та т. п.). Якщо стійкість таких засобів (в розумінні ймовірності не подолання) дорівнює $p_ф = 1 - q_ф$, то внаслідок відсіву (фільтрації) зовнішніх впливів на виході системи фільтрації інтенсивність завад буде дорівнювати $\lambda_{шз} \cdot q_{фі}$, а інтенсивність $\lambda_р$ штучних впливів, які не відфільтровані системами управління доступом та фільтрації, складе:

$$\lambda_{рш} = \lambda_{шв} \cdot q_1 + \lambda_{шз} \cdot q_ф + \lambda.$$

З урахуванням інтенсивності справжніх запитів $\lambda_{сз}$ загальна інтенсивність $\lambda_з$ впливів дорівнює

$$\lambda_з = \lambda_{сз} + \lambda_{шв} \cdot q_1 + \lambda_{шз} \cdot q_ф + \lambda.$$

При середній тривалості обслуговування в ЛОМ одного запиту (середньому значення часу використання ресурсу $t_{вр}$) і пуассонівському законі розподілу ймовірностей впливу ймовірність того, що під час звернення до ресурсу він уже використовується (ймовірність звернення до ресурсу на даному інтервалі $t_{вр}$ більше ніж однієї заявки – ймовірність порушення доступності шляхом переводу ресурсу в режим штучної відмови) дорівнює

$$q_{п3} = 1 - p_0 = 1 - \exp\{-t_{вр} \cdot \lambda_з\},$$

де p_0 – ймовірність відсутності впливів (ймовірність того, що на даному часовому інтервалі виникне рівно нуль впливів), а, **отже ймовірність порушення доступності ресурсу**

$$q_{пд} = 1 - (1 - q_{п3}) \cdot (1 - q_{пц}).$$

Розглянута модель дозволяє:

по–перше, запропонувати вирази для оцінки залишкового ризику при захисті доступності ресурсів у вигляді ймовірності порушення доступності та сформувати умову переходу захищеного ресурсу в режим штучної відмови;

по–друге, зробити висновок про те, що для забезпечення доступності шляхом унеможливлення доступу до інформації та модифікації неавторизованим користувачем змісту інформаційного об'єкту необхідно застосовувати засоби (апаратурні чи програмні) для управління доступом, для контролю та поновлення цілісності, для фільтрації пакетів, блокування засобів генерації безперервних запитів та т. п., засоби управління фізичним доступом, охоронної сигналізації та організаційного обмеження доступом;

по–третє, зробити висновок про необхідність, на відміну від захисту від порушення конфіденційності та цілісності, передбачати й можливість недопущення переводу ресурсу в режим штучної відмови – порушення доступності об'єкту за рахунок унеможливлення вчасного використання того чи іншого ресурсу авторизованим користувачем, тобто необхідно передбачати механізми запобігання постійного чи занадто тривалого використання цього ресурсу чи засобів його отримання порушником (установка квот – кількості звернень поспіль, допустимої тривалості чи допустимих часових інтервалів використання ресурсу, установка пріоритетів на використання ресурсів та інше), механізми забезпечення стійкості та відновлення процесів в умовах збоїв, механізми резервування інформаційних об'єктів, механізми аналізу потоків запитів від суб'єктів ЛОМ та ТКМ, контролю та поновленню цілісності інформаційних об'єктів (наприклад, в каналах ТКМ) та т. п.

Змінну $t_{вр}$, при цьому, слід розглядати як середній час використання захищеного ресурсу в умовах обслуговування ЛОМ усіх можливих запитів (для інформаційних об'єктів це – контроль цілісності, при необхідності її поновлення, виконання програмного засобу, читання чи запис інформації та все таке інше). Як перше, грубе, наближення можна використати значення $t_{вр} = (T_{ki} - \Delta T_{ki})/ n_{зк}$, де: $n_{зк}$ – кількість інформаційних об'єктів, що потребують використання на інтервалі часу ($T_{ki} - \Delta T_{ki}$), T_{ki}, ΔT_{ki} – періодичність та тривалість контролю відповідно [5]. При цьому, якщо середнє значення часу використання ресурсу перевищить середнє значення часового інтервалу між сусідніми запитами (інтенсивність запитів перевищує інтенсивність обслуговування), то кількість будь-яких запитів у черзі на використання ресурсу буде зростати до нескінченності, що є ознакою штучної відмови захищеного ресурсу.

Тобто умову, коли $1/\lambda_з \le t_{вр}$ слід розглядати як умову переходу захищеного ресурсу в режим штучної відмови.

2.4. Оцінка загального залишкового ризику

Розглянуті вище моделі дозволяють отримати, окрім розглянутих кількісних характеристик – ймовірностей порушення конфіденційності, цілісності та доступності – також величину загального залишкового ризику.

Неважко показати, що величину **загального залишкового ризику** у вигляді ймовірності порушення (подолання, злому) комплексної системи захисту можна розрахувати з виразу

$$q = 1 - (1 - q_{пк})\cdot(1 - q_{пц})\cdot(1 - q_{пд}).$$

Як і раніше, останній вираз може набути вигляду

$$q \approx \max (q_{пк}, q_{пц}, q_{пд}).$$

Висновок

В статті запропоновано методики оцінки кількісних значень величин залишкових ризиків і отримані відповідні вирази для їх обрахування. Аналіз отриманих виразів дозволяє зробити, перш за все, висновок про те, що слабкість елементів системи захисту визначається найбільш слабкою ланкою цієї системи. По-друге, у виразах для розрахунку відповідних ризиків можна виділити домінуючі ймовірності. І, нарешті, останнє. Усі змінні, які входять до складу виразів, що запропоновані для оцінки величин залишкових ризиків, можуть бути визначеними із застосуванням методик, викладених в [2, 6].

*Література: **1.** "Типове положення про службу захисту інформації в автоматизованій системі" (НД ТЗІ 1.4 – 001 – 2000); **2.** Матов О. Я., Василенко В. С., Будько М. М. Методика оцінки захищеності в локальних обчислювальних мережах. К. НТУ "КПІ" // Вісті Академії інженерних наук України. – 2005. – № 2 (25). – С. 59 − 78; **3.** Будько М. М. Василенко В. С. Оцінка залишкового ризику при застосуванні засобів захисту інформації від НСД в корпоративних системах. К.: Інститут проблем моделювання в енергетиці ім. Г. Є. Пухова, Матеріали науково – практичної конференції "Інформаційні технології в енергетиці", 2002, с. 29 – 39. **4.** Будько М. М. Визначення залишкового ризику при оцінці захищеності інформації в інформаційно –*

обчислювальних системах. К. НТУУ "КПІ" //Правове, нормативне та метрологічне забезпечення Системи захисту інформації в Україні. Випуск 8// 2004, с. 20-26. ***5****. Матов О. Я., Василенко В. С., Будько М. М. Визначення залишкового ризику при оцінці захищеності інформації в інформаційно – телекомунікаційних системах. // К.: Реєстрація, зберігання і обробка даних, 2004, Т. 6, № 2, с. 62 – 74.* ***6.*** *Василенко В. С., Будько М. М. Методики визначення вихідних даних для оцінки залишкових ризиків у ЛОМ. НТУУ "КПІ" //Правове, нормативне та метрологічне забезпечення Системи захисту інформації в Україні. Випуск 9// 2004, с. 110-120.*

УДК 004.056.5(045)

БЕЗОПАСНОСТЬ ПРИ ПЕРЕНОСЕ ДАННЫХ НА ДРУГУЮ ОПЕРАЦИОННУЮ СИСТЕМУ

Сергей Егоров
Национальный авиационный университет

Анотація: **Розроблено рекомендації щодо безпечного зберігання даних при електронному документообігу і безпечного переносу даних при переході на молодші операційні системи або на інший комп'ютер.**
Summary: **The recommendations for the safe storage of data in electronic document and safely moving the data in the transition to lower operating system or to another computer.**
Ключові слова: **Електронний документообіг, резервне копіювання, безпека даних, захист даних, бекап.**

Постановка проблемы

В связи с резким ростом в повседневной жизни электронного документооборота и влиянием информационных войн на электронную документацию вопрос о безопасном переходе на другую операционную систему (ОС) и безопасном резервном копировании становится актуальным. Постановка задачи: целью данной статьи является разработка рекомендаций для осуществления безопасного перехода с версии ОС Windows на другую, младшую версию.

Анализ последних научных исследований и публикаций

Большой спектр проблем защиты пользовательских ОС и рекомендации для их решения были изложены в [1 – 2]. Однако в этих источниках была обойдена стороной проблема безопасного резервного копирования, которые необходимо решить при апгрейде ОС или переходе на младшую версию. Нет чётких рекомендаций по этому вопросу и в [3 – 5], а затронуты лишь основные процедуры резервного копирования с помощью своих программных продуктов. Также следует отметить, что многие функции, которые предлагаются программными продуктами, предложенными в [3 – 5] с успехом могут быть заменены штатными средствами ОС. Пользуясь, например, штатными средствами ОС Windows Vista, которые она предлагает для резервного копирования, можно существенно сэкономить время, деньги и место на жестком диске, которое будет занимать соответствующее программное обеспечение от стороннего производителя.

Стратегия планирования резервного копирования

Резервное копирование – создание копии файла, хранящейся в другом месте отдельно от оригинала. Резервное копирование файла можно создавать многократно для отслеживания его изменений.

Резервное копирование позволяет защитить файлы в случае их потери в результате случайного удаления, атаки червя или вируса, аппаратного сбоя. Во всех этих случаях можно без проблем извлечь из архива нужную копию файла.

Следует выполнять резервное копирование тех файлов, которые трудно или невозможно заменить или если файл часто изменяется. Кандидатами на резервное копирование могут быть следующие файлы: рисунки, цифровые фотографии, видео, финансовые документы, проекты.

Не следует выполнять резервное копирование тех программ, которые обычно занимают много дискового пространства, так как их можно восстановить, воспользовавшись дисками оригинальных продуктов для повторной установки.

Частота резервного копирования зависит от количества создаваемых файлов и от того как часто они создаются или изменяются. Создавая файлы каждый день, возможно, имеет смысл делать резервные копии