

УДК 681.3

О. Я. Матов¹, В. С. Василенко², М. М. Бурдюк²

¹Інститут проблем реєстрації інформації НАН України

вул. М. Шпака, 2, 03113 Київ, Україна

²НВО «Електронмаш»

Визначення залишкового ризику при оцінці захищеності інформації в інформаційно-телекомунікаційних системах

Для аналізу захищеності інформації автоматизованих систем запропоновано застосування кількісних характеристик у вигляді величин залишкового ризику чи ймовірностей подолання порушником засобів захисту тих або інших властивостей захищеності; наведено вирази для їх розрахунків та моделі відповідних систем захисту інформації.

Ключові слова: загроза, захищеність інформації, конфіденційність інформації, цілісність інформації, доступність інформації, засоби захисту, залишковий ризик, ймовірність подолання засобів захисту, модель засобу захисту, порушник.

Загальновідомо, що на сучасному етапі розвитку інформаційно-телекомунікаційних систем (ІТС) захист їх ресурсів, насамперед інформації, є дуже важливою і актуальною проблемою. Для цього розробляються або використовуються системи захисту, які забезпечують той чи інший рівень захищеності інформації ІТС. Нормативними документами [1–3] властивості захищеності інформації в ІТС визначені наступним чином:

1) конфіденційність інформації — властивість інформації, яка полягає в тому, що інформація не може бути отримана 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 потрібна.

Для визначення вимог та оцінки захищеності інформації в ІТС 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 за допомогою залишкового ризику [4] чи інших показників ефективності захищених систем. Але ці критерії чи показники 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).

Тому в статті пропонується введення кількісних показників захищеності інформації в ІТС, які можна використовувати як для визначення залишкового ризику, так і в якості параметрів управління при оптимізації шкоди, яка запобігається при застосуванні засобів захисту і розглянута в [5]. Окрім того, корисні і ті моделі систем захисту (забезпечення відповідних функціональних властивостей), які застосовані для оцінки запропонованих у статті кількісних показників захищеності інформації в ІТС. Такі моделі можна застосовувати при проектуванні ефективних систем технічного захисту інформації.

В якості кількісних **показників залишкового ризику** пропонується використовувати ймовірності порушення конфіденційності $q_{нк}$, цілісності $q_{цн}$, доступності $q_{нд}$.

Визначення величин означених кількісних характеристик дозволяє оцінити рівень забезпечення захищеності інформації застосованими засобами захисту, чи ступінь забезпечення захищеності інформації засобами, які проектуються для впровадження. В обох випадках необхідно мати методику для їх визначення та фактичний склад застосованих засобів чи моделі засобів системи захисту, які розробляються для впровадження. Нижче пропонується варіант такої методики для випадку оцінки захищеності проектуємих систем.

Методика передбачає, що для визначення показників захищеності інформації (залишкового ризику) необхідно детально проаналізувати взаємодію засобів реалізації атак, спрямованих на подолання механізмів забезпечення кожного з цих показників захищеності інформації ІТС, із засобами протидії цим загрозам. У методиці для визначеного об'єкта захисту необхідно передбачити наступні три етапи:

- 1) формулювання моделі порушника та загроз;
- 2) визначення, хоча б у загальному вигляді, засобів протидії загрозам — моделі захисту інформаційного об'єкта;
- 3) розробка моделі взаємодії засобів реалізації атак із засобами протидії цим загрозам та формульних співвідношень для визначення показників захищеності інформації, у відповідності з якими можна розрахувати величини залишкового ризику. Врахуємо при цьому, що узагальнені моделі такої взаємодії значною мірою уже розглянуто і представлено в [5–7]. Нижче розглядаються більш детальні моделі, які дозволяють, на погляд авторів, досягти тих цілей, які поставлено перед статтею.

На першому етапі методики виконується класифікація 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 тощо;

— «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 тощо;

— «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 та ін. й отримати змогу фізичного доступу до засобів обробки, 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: витіки інформації технічними каналами, спеціальні впливи на інформацію технічними каналами, мережне обладнання локальних чи розподілених мереж, у тому числі й засоби телекомунікаційних мереж.

Така 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 ІТС).

Окрім того будемо вважати, що загрози захищеності інформації відомі, хоча б на рівні, викладеному в [6], а найбільш суттєві загрози визначені. Такий підхід дозволяє визначити деяку узагальнену модель загроз ресурсам локальних обчислювальних мереж (ЛОМ), наприклад, таку, яка наведена на рис. 1.

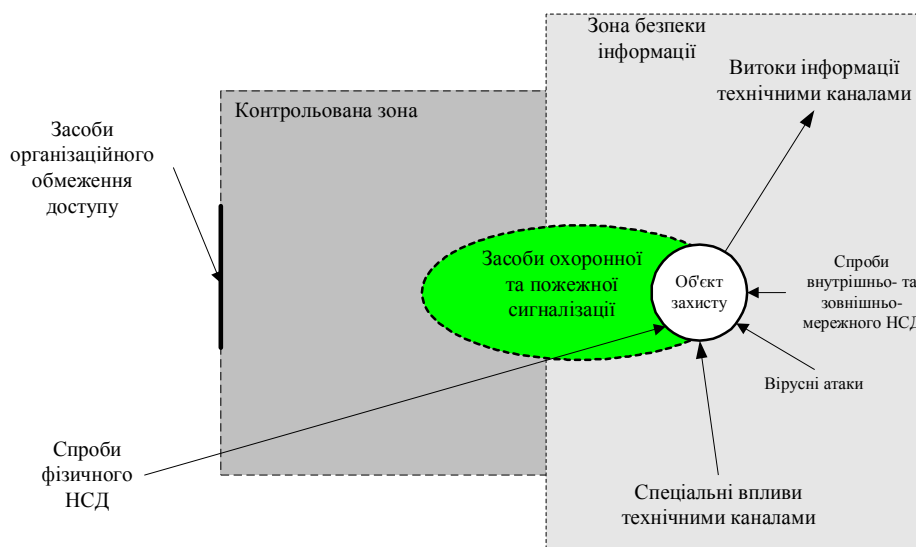


Рис. 1. Узагальнена модель загроз інформаційному об'єкту ЛОМ

На другому етапі (визначення моделі захисту інформаційного об'єкта) будемо вважати ІТС складною, ієрархічною, розподіленою інформаційно-обчислювальною системою, елементами якої є ЛОМ. Нехай елементи різних рівнів ієрархічної структури ІТС при цьому пов'язані елементами телекомунікаційної мережі (ТКМ). Нехай також об'єктом захисту є інформаційні ресурси ЛОМ, а засоби технічного захисту ресурсів певної ЛОМ складаються із засобів організаційного обмеження доступу, охоронної сигналізації, адміністрування доступу — внутрішньомережних засобів управління доступом до ресурсів ЛОМ, зовнішньомережних засобів управління доступом до ресурсів даної ЛОМ (із ТКМ), 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 з обслуговування множини запитів.

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

- засобів організаційного обмеження доступу;
 - засобів охоронної сигналізації;
 - внутрішньомережних засобів управління доступом — засобів адміністрування доступу (проблемно-орієнтованих засобів захисту базового програмного забезпечення — операційних систем та систем керування базами даних (за їх наявності));
 - засобів захисту інформації у ТКМ (від несанкціонованого доступу до ресурсів даної ЛОМ із телекомунікаційної мережі);
 - засобів антивірусного захисту (від впровадження комп'ютерних вірусів).
- Окрім того, впливи на інформаційні об'єкти можливі за рахунок використання:
- технічних каналів побічних електромагнітних випромінювань і наведень, акустичних каналів;
 - каналів спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту чи порушення цілісності інформації.

Третій етап методики розглядається по відношенню до кожної з властивостей захищеності інформації ІТС.

Для оцінки залишкового ризику при забезпеченні конфіденційності (ймовірність отримання інформації порушником з розкриттям змісту) подію, пов'язану з порушенням конфіденційності, слід розглядати як складну та таку, що складається з подій:

- несанкціонованого отримання користувачем інформації тим чи іншим чином з метою ознайомлення з нею чи будь-якого подальшого використання;
- розкриття змісту інформації з обмеженим доступом (ІЗОД) після отримання її тим чи іншим чином. Останнє слід трактувати як можливість подолання порушником відповідних засобів криптозахисту.

Модель взаємодії засобів реалізації атак з засобами протидії цим загрозам — засобами забезпечення конфіденційності інформації представлена на рис. 2 (на цьому рисунку ЗК — загрози конфіденційності, ЗЗК — засоби захисту конфіденційності).

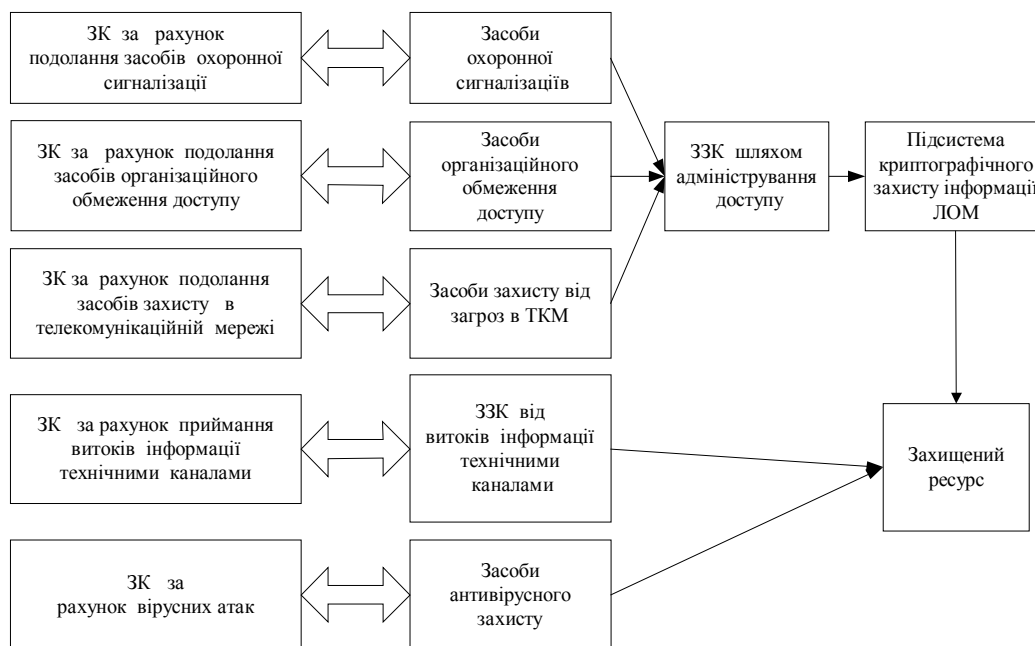


Рис. 2. Модель взаємодії засобів реалізації атак із засобами протидії загрозам — засобами забезпечення конфіденційності інформації

Як витікає з моделі, несанкціоноване отримання користувачем інформації тим чи іншим чином є можливим за умови подолання неавторизованим користувачем засобів захисту у складі:

1) організаційного обмеження доступу (контроль доступу та управління доступом до приміщень організаційними засобами, наприклад реалізацією перепускного режиму до будівель чи окремих приміщень, та т.і.). Такі дії слід очікувати, скоріше за все, від «терплячих зловмисників» — авторизованих користувачів, які мають атрибути легального доступу до певних приміщень ІТС (наприклад, перепустки чи їх еквіваленти), або від «рішучих зловмисників», які вимушено використовують підроблені атрибути легального доступу до приміщень ІТС;

2) 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;

3) управління доступу, 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 інфор-

мації, або від «випадкових порушників» — авторизованих користувачів, які порушують конфіденційність не навмисно, а помилково — шляхом випадкового подолання засобів управління (адміністрування) доступом до об'єкта захисту, виконання непередбачених дій відносно цього інформаційного об'єкта та т.п.;

4) засобів канального захисту в ТКМ (засобів захисту від несанкціонованого доступу із телекомунікаційної мережі до ресурсів даної ЛОМ);

5) засобів захисту від вірусних атак (засобів антивірусного захисту).

При цьому ймовірність несанкціонованого доступу (ймовірність подолання засобів управління доступом) q_1 можна визначити з виразу

$$q_1 = q_{y\delta} \cdot [1 - (1 - q_{ood}) \cdot (1 - q_{oc}) \cdot (1 - q_{tkm})],$$

де $q_{y\delta}$ — ймовірність подолання засобів управління доступом; q_{ood} — ймовірність подолання засобів організаційного обмеження доступу; q_{oc} — ймовірність подолання засобів охоронної сигналізації; q_{tkm} — ймовірність подолання засобів захисту інформацій у мережах її передавання (телекомунікаційних мережах).

Примітка 1. Тут і надалі за відсутності того чи іншого виду захисту ймовірність його подолання вважається такою, що дорівнює одиниці.

У свою чергу, ймовірність $q_{y\delta}$ подолання засобів управління доступом є також ймовірністю складної події, яка полягає в подоланні порушником як засобів управління фізичним доступом, так і засобів адміністрування доступом з використанням механізмів базового та прикладного програмного забезпечення. Якщо позначити ці ймовірності через q_{yfd} і q_{ad} відповідно, то

$$q_{y\delta} = q_{yfd} \cdot q_{ad}.$$

Тоді, зрозуміло,

$$q_1 = q_{yfd} \cdot q_{ad} \cdot [1 - (1 - q_{ood}) \cdot (1 - q_{oc}) \cdot (1 - q_{tkm})].$$

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'єкта) 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. Ймовірності цих подій q_{zm} , q_{zkn} , q_{kn} відповідно.

При цьому ймовірність подолання неавторизованим користувачем засобів криптозахисту (можливість розкрити зміст ІЗОД) інформації q_{kzi} можна визначити з виразу

$$q_{kzi} = q_{zm} \cdot q_{zkn} \cdot q_{kn}.$$

Таким чином, у разі, коли для забезпечення конфіденційності при зберіганні чи передаванні інформації застосовуються засоби криптографічного захисту,

$$q_{к1} = q_{кзі} \cdot q_{уфд} \cdot q_{ад} \cdot [1 - (1 - q_{оод}) \cdot (1 - q_{ос}) \cdot (1 - q_{ткм})].$$

Окрім того, несанкціоноване отримання користувачем інформації є можливим і під час її обробки (введенні з клавіатури, відображенні на моніторі, виведенні на друк у дешифрованому вигляді тощо) шляхом використання витоків інформації технічними каналами, а також при використанні вірусних атак, за умови подолання неавторизованим користувачем відповідних засобів захисту. Нехай імовірність подолання засобів захисту від витоків інформації технічними каналами дорівнює $q_{зві}$, а ймовірність подолання засобів антивірусного захисту — $q_{ав}$.

Не розкриваючи змісту подій, пов'язаних із порушенням конфіденційності з використанням витоків інформації технічними каналами чи з використанням вірусних атак, вираз для розрахунку ймовірності $q_{нк}$ порушення конфіденційності інформації з подоланням розглянутих засобів захисту можна записати у вигляді

$$q_{нк} = 1 - (1 - q_{к1}) \cdot (1 - q_{зві}) \cdot (1 - q_{ав}).$$

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

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

— виведення з ладу, зміни режимів функціонування або несанкціонованого використання засобів зберігання носіїв інформації і порушення таким чином її цілісності;

— несанкціонованої модифікації (зміни, підміни, знищення тощо) ІзОД у середовищах її обробки, зберігання чи передавання з метою унеможливлення подальшого її використання чи нанесення іншої шкоди власнику даного ресурсу.

На рис. 3 представлена модель взаємодії атак з засобами протидії цим атакам — засобами забезпечення цілісності (на цьому рисунку ЗЦ — загрози цілісності, ЗЗЦ — засоби захисту цілісності).

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

— подолано засоби охоронної сигналізації або засоби організаційного обмеження доступу та (і) засоби управління доступом, включаючи засоби управління фізичним доступом та адміністрування доступу. Ймовірність такої події q_1 уже визначена раніше;

— з імовірністю $q_{цткм}$ подолано засоби захисту цілісності від загроз у ТКМ;

- з імовірністю q_{cv} подолано засоби захисту від спеціальних впливів на інформацію технічними каналами;
- з імовірністю q_{av} подолано засоби антивірусного захисту;
- з імовірністю $q_{кц}$ подолано засоби контролю та поновлення цілісності інформації.

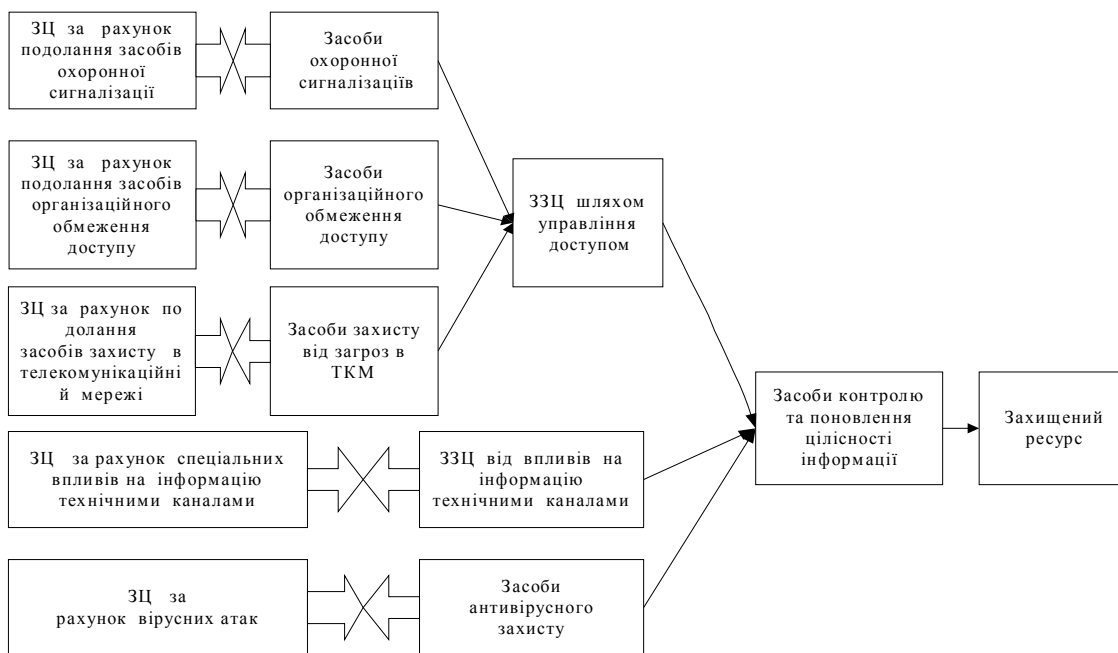


Рис. 3. Модель процесу взаємодії засобів реалізації атак із засобами забезпечення цілісності ЛОМ

Тоді, з використанням застосованих вище підходів, ймовірність порушення цілісності q_{nc} можна знайти з виразу

$$q_{nc} = q_{кц} \cdot [1 - (1 - q_1) \cdot (1 - q_{cv}) \cdot (1 - q_{av})].$$

Розглянута в методиці модель дозволяє зробити, по-перше, висновок про те, що для забезпечення цілісності за рахунок унеможливлення доступу до інформації та модифікації неавторизованим користувачем змісту інформаційного об'єкта необхідно застосовувати засоби (апаратні чи програмні) для адміністрування доступу, для контролю цілісності, для 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

ції з обмеженим доступом слід застосовувати такі ж засоби управління доступом (апаратні чи програмні), як і для забезпечення конфіденційності.

Примітка 2. Звернемо увагу на те, що з наведеного вище визначення цілісності, як функціональної властивості захищеності інформації, не витікає ніяких часових обмежень щодо тривалості процесу поновлення цілісності, в разі виявлення засобами контролю наявності її порушення. Це дає змогу для забезпечення цілісності використовувати і ручні методи, наприклад, поновлення з застосуванням резервних копій інформаційних об'єктів чи шляхом забезпечення відкату процесів у разі виявлення порушення цілісності.

Виходячи із наведеного вище визначення функціональної властивості захищеності інформації, 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:

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 створення таким чином перешкод іншим користувачам у використанні цих ресурсів;

— постійного використання інформаційного ресурсу, наприклад, шляхом генерації потоку заважаючих (несправжніх) запитів на використання ресурсу, обслуговування несправжніх пакетів вхідної інформації з такою інтенсивністю, коли сумарна (разом із справжніми) інтенсивність запитів стає такою, що їх період (середня тривалість проміжку часу між двома сусідніми запитами) не перевищує тривалості обслуговування кожного з таких запитів, тобто такого потоку, коли захищений ресурс навмисно призначається для обслуговування лише заважаючих запитів;

— блокування засобів адміністрування доступу, наприклад шляхом генерації такого потоку заважаючих запитів (спроб доступу тощо — завад процесу автентифікації), коли сумарна (разом із справжніми) інтенсивність запитів стає такою, що їх період (середня тривалість проміжку часу між двома сусідніми запитами) не перевищує тривалості процесів автентифікації у системах адміністрування доступу;

— переривання передачі потоку даних шляхом блокування відповідних засобів (серверів доступу, маршрутизаторів, концентраторів та т. ін.);

— постійного порушення цілісності з періодичністю меншою ніж час відновлення інформаційного ресурсу. Така подія передбачає наявність порушень ціліс-

ності за рахунок впливу природних факторів (збої, відмови), а також наявність реалізованих спроб несанкціонованого доступу до інформаційного ресурсу каналами спеціального впливу (без спроб маскування).

Ймовірність першої з цих подій визначено вище (з використанням моделі, представленій 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 ІТС 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 ІТС, 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.ін.). 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 по відношенню до ресурсів ЛОМ, що з якихось причин є забороненими для даних користувачів. Такі впливи — це спроби несанкціонованого доступу (НСД), і вони можуть бути випадковими (внаслідок помилки користувача), або зловмисними, тобто **спеціальними**, з метою використання чи то ресурсів, чи то інформації ЛОМ.

Спроби НСД можуть вплинути на ЛОМ лише після подолання засобів управління доступом та відповідних засобів забезпечення тієї чи іншої функціональної послуги.

Потоки загроз доцільно вважати найпростішими з інтенсивностями λ_3 . Зрозуміло, що ця інтенсивність дорівнює сумі інтенсивностей загроз штучних $\lambda_{ш}$ та природних λ , так, що

$$\lambda_3 = \lambda_{ш} + \lambda.$$

Причому штучні загрози можуть бути внутрішніми з інтенсивністю $\lambda_{шв}$ (з боку авторизованих чи неавторизованих користувачів ЛОМ чи її елементів) і зовнішніми з інтенсивністю $\lambda_{шз}$.

Виявлення і подальша протидія загрозі (ймовірність захисту ЛОМ від загроз) залежить від того, чи запобігла (не допустила) система захисту впливу цієї загрози, чи установила факт її впливу і ліквідувала відповідні наслідки.

Ця задача може вирішуватися застосуванням у ЛОМ засобів фільтрації зовнішніх впливів (від елементів розподіленої обчислювальної мережі через засоби телекомунікаційної мережі), які впливають на дану ЛОМ (засоби фільтрації типу міжмережних екранів (firewall, брандмауерів), сервісів — посередників (proxies) тощо). Якщо стійкість таких засобів (у розумінні ймовірності їх подолання) дорівнює q_ϕ , то внаслідок відсіву (фільтрації) зовнішніх впливів системою фільтрації на її виході інтенсивність завад буде дорівнювати $\lambda_{uz} \cdot q_\phi$.

Також ця задача вирішується шляхом управління доступом до інформаційних ресурсів ЛОМ (ідентифікація, автентифікація, надання певних повноважень чи привілеїв, з наступною їх перевіркою під час кожної із спроб доступу до ресурсів).

Слід враховувати, що ймовірності q_ϕ та q_{ad} — ймовірності подолання систем фільтрації зовнішніх впливів та управління доступом — визначаються характеристиками цих систем та коректністю виконання процедур адміністрування. Перш за все, ці ймовірності визначаються можливостями цих систем, як систем масового обслуговування (з певною продуктивністю, довжиною черг вхідних запитів, допустимим часом перебування запитів у чергах та т. ін.) обслуговувати певні потоки запитів. Окрім того, ці ймовірності визначаються, наприклад, кількістю можливих ідентифікаторів та кількістю можливих варіантів паролів і надійністю їх конфіденційного зберігання.

Враховуємо при цьому, що на вході системи управління доступом діють як внутрішні штучні впливи, так і зовнішні, не відфільтровані, впливи із загальною інтенсивністю $\lambda_{uv} + \lambda_{uz} \cdot q_\phi$.

Внаслідок відсіву (фільтрації) цієї сукупності внутрішніх та зовнішніх впливів системою управління доступом на її виході інтенсивність завад буде дорівнювати $(\lambda_{uv} + \lambda_{uz} \cdot q_\phi) \cdot q_{ad}$, а результуюча інтенсивність λ_{pi} штучних впливів, які не виявлені і не відфільтровані системами управління доступом та фільтрації, складе

$$\lambda_{pi} = (\lambda_{uv} + \lambda_{uz} \cdot q_\phi) \cdot q_{ad} + \lambda.$$

З урахуванням інтенсивності справжніх запитів λ_{cz} загальна інтенсивність λ_3 впливів дорівнює

$$\lambda_3 = \lambda_{cz} + (\lambda_{uv} + \lambda_{uz} \cdot q_\phi) \cdot q_{ad} + \lambda.$$

При середній тривалості обслуговування в ІТС одного запиту (середньому значенні часу використання ресурсу t_{ep}) 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_{ep} більше ніж однієї заявки — ймовірність порушення доступності шляхом переводу ресурсу до режиму штучної відмови) дорівнює

$$q_{n3} = 1 - p_0 = 1 - \exp\{-t_{ep} \lambda_3\},$$

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

$$q_{nd} = 1 - (1 - q_{n3}) \cdot (1 - q_{nc}).$$

Розглянута модель дозволяє:

— по-перше, запропонувати вирази для оцінки залишкового ризику при захисті доступності ресурсів у вигляді ймовірності порушення доступності та сформулювати умову переходу захищеного ресурсу до режиму штучної відмови;

— по-друге, зробити висновок про те, що для забезпечення доступності за рахунок унеможливлення доступу до інформації та модифікації неавторизованим користувачем змісту інформаційного об'єкта необхідно застосовувати засоби (апаратні чи програмні) для управління доступом, контролю та поновлення цілісності, 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 можливість недопущення переводу ресурсу до режиму штучної відмови — порушення доступності об'єкта за рахунок унеможливлення вчасного використання того чи іншого ресурсу авторизованим користувачем, тобто необхідно передбачати механізми запобігання постійного або 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 ін.), 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_{ep} при цьому, слід розглядати як середній час використання захищеного ресурсу в умовах обслуговування автоматизованою системою усіх можливих запитів (для інформаційних об'єктів це — контроль цілісності, за необхідності її поновлення, виконання програмного засобу, читання чи запис інформації тощо). Визначення величини t_{ep} виходить за рамки даної роботи, хоча в якості першого, грубого, наближення можна використати значення $t_{ep} = (T_{ki} - \Delta T_{ki})/n_{io}$, де: n_{io} — кількість інформаційних об'єктів, що потребують використання на інтервалі часу $(T_{ki} - \Delta T_{ki})$, T_{ki} , ΔT_{ki} — періодичність та тривалість контролю відповідно [6]. 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 $1/\lambda_3 \leq t_{ep}$, слід розглядати як умову переходу захищеного ресурсу до режиму штучної відмови.

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 при цьому розрахувати з виразу

$$q = 1 - (1 - q_{нк}) \cdot (1 - q_{нц}) \cdot (1 - q_{нд}),$$

що добре узгоджується з близькими за змістом виразами з [7].

Примітка 3. Усі невизначені змінні у виразах, наведених для розрахунку запропонованих показників захищеності інформації (ймовірностей порушення тієї чи іншої властивості захищеності інформації), можуть бути розрахованими, якщо відомі чи їх складові, чи закони розподілу відповідних імовірностей. У багатьох випадках можна вважати розподіл імовірностей таких подій рівномірним, принаймні, як найскладніший для функціонування систем захисту. В інших випадках для розрахунку імовірностей можна використати параметри потоків відповідних випадкових величин. Оскільки детальний розгляд цього питання виходить за межі статті, обмежимося лише прикладом визначення імовірностей, коли йдеться про необхідність прямого перебору, чи то ключових наборів (для засобів криптозахисту, контролю цілісності, та інше), чи то паролів (для засобів управління доступом тощо), коли закони розподілу можна вважати рівномірними. Якщо відома, наприклад, кількість варіантів ключів засобів криптографічного захисту інформації $N_{кл} = 2^{256}$, тоді ймовірність $P_{кзі}$ може бути прийнятою рівною $P_{кзі} = N_{кл}^{-1} = 2^{-256}$.

Таким чином, методика, що пропонується, дозволяє отримати вирази для визначення показників захищеності інформації по кожній з функціональних послуг захисту від можливих загроз у вигляді залишкового ризику — ймовірності порушення захисту від загроз відповідного типу, та побудувати загальну модель системи захисту в частині забезпечення необхідних властивостей захищеності і, за умовою оптимізації параметрів та характеристик у відповідності з [5], може бути використаною для проектування ефективних систем технічного захисту інформації взагалі та їх складових зокрема.

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., Василенко В.С., Короленко М.П. Варіант формалізації процесу захисту інформації в комп'ютерних системах та оптимізації його цільової функції // Реєстрація, зберігання і оброб. даних. — 2000. — Т 2, № 2. — С. 73–84.
6. Будько М.М., Василенко В.С., Короленко М.П. Ефективність забезпечення цілісності інформації у телекомунікаціях // Реєстрація, зберігання і оброб. даних. — 2000. — Т 2, № 3. — С. 43– 65.
7. Антонюк А.А., Волощук А.Г., Заславская Е.А., Суслов В.Ю. Об одном подходе в моделировании защиты информации // Перша міжнародна науково-практична конференція з програмування УкрПРОГ, 1998. — С. 505–510.

Надійшла до редакції 27.02.2004