існуючій системі технічної експлуатації ЦСК.

Додаткові заходи і механізми забезпечення інформаційної безпеки, як правило, необхідні для досягнення високого рівня захищеності інформаційних ресурсів ЦСК. Для базового рівня захишеності доля витрат на додаткові засоби і механізми захисту може бути незначною. Найбільша доля витрат припадає на ділянки систему захисту від впливів позаштатними програмними і (або) програмно-технічними засобами на програми, дані і процеси на АТС, які установлені в процесі її експлуатації (14%) та на систему ліквідації наслідків реалізованих загроз інформації на АТС (14%). Доцільність їх визначається на етапах оцінки захищеності інформаційних ресурсів та атестації КЗМЗ на відповідність вимогам системи технічного захисту інформації.

*Література: **1.** Тардаскін М. Ф. Особливості стратегії інформаційної безпеки цифрових автоматичних телефонних станцій // Зв'язок. – 2005. - № 1. – С. 31-33. **2.** ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення. **3.** ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт. **4.** ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. **5.** ДБН А.2.2-2-96. Проектування. Технічний захист інформації. Загальні вимоги до організації проектування та проектної документації для будівництва. Введено в дію 01.01.97 р. **6.** НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. **7.** НД ТЗІ 1.1-001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення. **8.** НД ТЗІ 2.5-001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації функціональних послуг захисту. 9. НД ТЗІ 2.5-002-99. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації гарантій захисту. 10. НД ТЗІ 2.5-003-99. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації довірчих оцінок коректності реалізації захисту. **11.** НД ТЗІ 2.7-001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Порядок виконання робіт. **12.** НД ТЗІ 3.7-002-99. Технічний захист інформації на програмно-керованих АТС загального користування. Методика оцінювання захищеності інформації (базова). **13.** НД ТЗІ 2.1-001-2001. Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення. **14.** НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі. **15.** КНД 45-164-2001 Типова модель загроз для формування ресурсів цифрових АТС, що використовуються в мережах електрозв'язку загального користування України. **16.** Воробиенко П.П., Нечипорук О. Л., Щербина Ю. В. Модели угроз информационным ресурсам систем и сетей связи // Зв'язок. – 2003. - № 6. – С. 39-41. **17.** Воробиенко П., Нечипорук О., Щербина Ю. Принципы построения моделей угроз информационным ресурсам систем и сетей связи // Правове нормативне та метрологічне забезпечення системи захисту інформації в Україні. К.: 2001, вип. 7. – С. 11-13. **18.** НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. **19.** НД ТЗІ 3.6-001-2000. Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супровадження і модернізації засобів технічного захисту інформації від несанкціонованого доступу. **20.** НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу (Критерії базуються на аналізі Федеральних критеріїв США і критеріїв оцінки безпеки Канади). **21.** Князєва Н. О., Баландін І. О. Методика розрахунку собівартості послуг місцевого телефонного зв'язку // Зв'язок. – 2005. - № 1. – С. 9-15. **22.** КНД 45-076-98 Система автоматизованого телефонного зв'язку для мереж загального користування. Основні положення. Книга 1, книга 2. Київ. 2002. **23.** Демина Е. В., Иодко Е. К., Майофис Л. И., Резникова Н. П. Организация планирование и управление предприятиями связи.-М.: „Радио и связь", 1990.*

УДК 681.3

МЕТОДИКА ОЦІНКИ ЗАГРОЗ ДЛЯ ІНФОРМАЦІЇ АВТОМАТИЗОВАНИХ СИСТЕМ

Микола Будько
Відкрите акціонерне товариство "КП ОТІ"

Анотація: **Пропонується методика оцінки загроз для інформації автоматизованих систем на основі аналізу моделей порушника, можливих каналів і видів загроз ресурсам автоматизованих систем, моделі загроз та методика аналізу можливих контрзаходів для забезпечення припустимої захищеності та залишкового ризику.**

Summary: **The method of estimation of threats for information of the automated systems on the basis of analysis of models of violator, possible channels and types of threats to the resources of the automated systems, models of threats and method of analysis of possible counter-measures, for providing of possible protected and remaining risk is offered.**
Ключові слова: **Загроза, порушник, ресурси, модель.**

Відомо [1, 2], що в основу методики оцінки загроз для інформації в автоматизованих системах (АС) доцільно покласти методики побудови моделей порушника та загроз для інформації АС. Такі моделі створюються на підставі детального аналізу можливих загроз, способів та каналів їх реалізації. В свою чергу, моделі порушника та моделі загроз для інформації АС є основою для подальшого проведення аналізу ризиків і формування вимог до системи захисту інформації [3 – 5].

І Методика побудови моделі порушника

У кожному конкретному випадку, виходячи з технології обробки інформації, необхідно розробити модель порушника, яка має бути адекватна реальному порушнику для даної АС. Модель порушника – абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час та місце дії і т. ін. Для побудови цієї моделі рекомендується виконати аналіз та упорядкування наступної інформації.

Як порушника слід розглядати особу, яка прагне чи може одержати несанкціонований доступ до роботи з включеними до складу АС засобами. При побудові моделі порушника слід врахувати, що особливістю ресурсів АС, в першу чергу інформаційних, є їх принадливість для окремих осіб чи певних груп осіб, які з метою використання цих ресурсів прагнуть бути чи є користувачами АС. Ця принадливість найчастіше є обумовленою характером та об'ємом інформації, яка вводиться, обробляється, зберігається та циркулює в системах АС. Якщо та чи інша особа – користувач ресурсами АС здійснює спробу *несанкціонованого доступу* (тут і надалі виділення та підкреслення авторів) до об'єктів захисту (ознайомлення, модифікація, знищення, зміна режимів використання чи функціонування та т. п.), то *такий користувач є порушником*.

По відношенню до АС порушники можуть бути внутрішніми (з числа співробітників, користувачів системи) або зовнішніми (сторонні особи, або будь-які особи, що знаходяться за межами контрольованої зони).

Модель порушника має визначати:

- категорії осіб, з числа яких може бути порушник;
- рівень можливостей порушника;
- припущення про кваліфікацію та можливий рівень знань порушника;
- методи і способи, що використовуються при здійсненні порушень;
- можливу мету порушника та її градацію за ступенями небезпечності для АС;
- можливі місця здійснення порушень;
- можливі способи для здійснення загроз в АС;
- припущення про характер його дій.

До ***категорій осіб, які можуть бути порушниками*****,** слід відносити:

суб'єктів інформаційної діяльності – працівників організації – власника АС (близько 81,7 % порушень) – *внутрішні порушники*; для їх визначення слід детально розглянути можливості несанкціонованого доступу до ресурсів АС ***кожного*** із працівників організації;

сторонніх осіб, що отримують тим чи іншим шляхом доступ до ресурсів АС (близько 17,3 % порушень) – зовнішні порушники; для їх визначення слід детально розглянути можливості відвідувачів організації щодо несанкціонованого доступу до ресурсів АС з урахуванням наявної системи організаційного обмеження їх доступу.

За рівнем можливостей, що надаються їм штатними засобами АС, порушників доцільно класифікувати за чотирма рівнями можливостей. Класифікація є ієрархічною, тобто кожний наступний рівень включає в себе функціональні можливості попереднього:

- перший рівень визначає найнижчий рівень можливостей проведення діалогу з АС – можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;
- другий рівень визначається можливістю створення і запуску власних програм з новими функціями обробки інформації;
- третій рівень визначається можливістю управління функціонуванням АС, тобто впливом на базове програмне забезпечення системи і на склад і конфігурацію її устаткування;

- четвертий рівень визначається всім обсягом можливостей осіб, що здійснюють проектування, реалізацію і ремонт апаратних компонентів АС, аж до включення до складу АС власних засобів з новими функціями обробки інформації.

Слід припускати, що в своєму рівні порушники можуть бути **фахівцями вищої кваліфікації** (наприклад, адміністратори безпеки, баз даних, мереж), які мають повну інформацію про АС і комплекс засобів захисту (КЗЗ). Тому за рівнем знань усіх порушників слід класифікувати як таких, що:

- володіють інформацією про функціональні особливості АС, основні закономірності формування в ній масивів даних та потоків запитів до них, вміють користуватися штатними засобами;
- володіють високим рівнем знань та досвідом роботи з технічними засобами системи та їхнього обслуговування;
- володіють високим рівнем знань у галузі обчислювальної техніки та програмування, проектування та експлуатації АС;
- володіють інформацією про функції та механізм дії засобів захисту.

Зрозуміло, що найбільш небезпечні порушники можуть знати:

1. склад, розміщення, функціональні особливості, умови та режими функціонування елементів АС, включаючи траси прокладених чи можливих ліній зв'язку комунікаційних мереж та трафіки відповідних каналів передачі даних;
2. порядок, засоби та режими здійснення охорони елементів АС, місць їх розташування (включаючи пункти підсилення, як такі, що обслуговуються, так і ті, що не обслуговуються) та прилеглої території;
3. порядок, засоби та режими здійснення організаційно – правових та технічних заходів захисту ресурсів ЄДАПС;
4. основні закономірності формування в АС баз даних та потоків запитів до них.

За використовуваними методами і способами порушників можна класифікувати як таких, що використовують:

- виключно агентурні методи одержання відомостей;
- пасивні технічні засоби перехоплення інформаційних сигналів;
- виключно штатні засоби АС або недоліки проектування КСЗІ для реалізації спроб НСД;
- способи і засоби активного впливу на АС, що змінюють конфігурацію системи (підключення додаткових або модифікація штатних технічних засобів, підключення до каналів передачі даних, впровадження і використання спеціального ПЗ тощо).

Така класифікація порушників є корисною для використання в процесі оцінки ризиків, аналізу вразливості системи, ефективності існуючих і планових заходів захисту.

Можливою метою порушника – зловмисника може бути:

1. особиста авторизація, тобто отримати особисті легальні атрибути доступу, бажано з найширшими правами, до ресурсів АС з метою їх використання, отримання необхідної інформації у потрібному обсязі та асортименті, ознайомлення з конфіденційною інформацією, її модифікації чи знищення відповідно до своїх намірів (інтересів, планів);
2. авторизація своїх прихильників чи довірених осіб, які б мали змогу отримати легальні атрибути доступу, бажано з найширшими правами, до ресурсів АС з метою їх використання, отримання необхідної інформації у потрібному обсязі та асортименті, ознайомлення з конфіденційною інформацією, її модифікації чи знищення згідно з своїми намірами (інтересами, планами);
3. пошук прихильників чи довірених осіб серед персоналу чи користувачів АС, які мають змогу отримувати легальні атрибути доступу, бажано з найширшими правами, до ресурсів АС і можуть їх використовувати, отримувати бажано конфіденційну інформацію, її модифікувати чи знищувати; при відсутності змоги чи безуспішності реалізації пунктів 1 – 3 метою порушника – зловмисника може бути реалізація спроб щодо:
4. здобуття атрибутів доступу авторизованих користувачів шляхом використання технічних засобів, крадіжок, купівлі, чи отримання іншим шляхом;
5. проникнення на місця розміщення тих чи інших компонентів, елементів чи ресурсів АС (обчислювальних ресурсів, інформаційних ресурсів, базового, прикладного програмного забезпечення та програмного забезпечення системи ТЗІ, включаючи носії резервних копії, ресурсів вводу/ виводу, телекомунікаційного обладнання, включаючи мережу передачі даних) шляхом подолання перешкод (огорожі, елементів будівельних конструкцій, охорони чи охоронної сигналізації та ін.) та нанесення збитків шляхом знищення матеріальних та інформаційних цінностей;
6. зміна режимів функціонування чи виводу з ладу фізичних ресурсів АС;
7. установка фізичних засобів (апаратурних закладок) чи інших засобів технічної розвідки в місцях розміщення елементів АС (в тому числі і віддалених, наприклад в елементах комунікаційної мережі

зв'язку) для знімання інформації;

8. установка фізичних чи інших засобів (апаратурних закладок) в місцях розміщення елементів АС (в тому числі і віддалених, наприклад, в елементах комунікаційної мережі зв'язку) для генерації несправжніх сигналів, інформаційних символів чи повідомлень;

9. установка програмних засобів (програмних закладок) знімання інформації з метою її того чи іншого використання;

10. установка програмних засобів (програмних закладок чи вірусів) для модифікації як програмних засобів, так і інформації АС шляхом генерації (впровадження) програмних вірусів, несправжніх сигналів, інформаційних символів чи повідомлень з метою перевантаження систем АС і порушення, таким чином, доступності компонентів АС чи АС в цілому;

11. здійснення спроб несанкціонованого доступу до обчислювальних ресурсів, інформаційних ресурсів, базового та прикладного програмного забезпечення та програмного забезпечення системи ТЗІ як власне АС, так і її телекомунікаційної підсистеми шляхом подолання системи управління доступом.

За місцем здійснення порушення дії зловмисника можна класифікувати на:

1. без одержання доступу на контрольовану територію (центрального рівня АС, регіональних рівнів АС чи робочих місць місцевих рівнів АС, пунктів підсилення з обслуговуванням) з використанням технічних засобів дистанційної розвідки (наприклад, оптичними, акустичними каналами, каналами побічних електромагнітних випромінювань та ін.) або з використанням засобів здобуття інформації з мережі передачі даних (наприклад, шляхом підключення чи "врізання" в лінії зв'язку) – дистанційний вплив;

2. з одержанням доступу на контрольовану територію (центрального рівня АС, регіональних рівнів АС чи робочих місць кінцевих, в тому числі, віддалених користувачів АС, пунктів підсилення з обслуговуванням, але без доступу до технічних засобів АС) – також з використанням технічних засобів дистанційної розвідки (наприклад, оптичними, акустичними каналами, каналами побічних електромагнітних випромінювань та ін.) з подальшим несанкціонованим доступом до будівель, споруд чи приміщень, в яких розміщено елементи АС (безпосередній вплив);

3. з одержанням доступу до робочих місць кінцевих (в тому числі віддалених кінцевих робочих місць та пунктів підсилення без обслуговування) користувачів АС з подальшим несанкціонованим доступом до пристроїв вводу/виводу, копіювання, канального чи каналоутворюючого обладнання та інших елементів АС – безпосередній, як і в наступних пунктах 4 – 5 вплив;

4. з одержанням доступу до місць накопичення і зберігання даних (баз даних, архівів) з подальшим несанкціонованим копіюванням власне носіїв даних, їх копій чи інформації з цих накопичувачів та баз даних (наприклад, шляхом крадіжки, купівлі та ін.);

5. з одержанням доступу до засобів адміністрування АС і засобів управління комплексною системою ТЗІ з подальшими, практично необмеженими можливостями доступу до ресурсів АС, їх використання, модифікації чи знищення (за виключенням, можливо, того, що його дії будуть зафіксованими компонентом спостереженості системи ТЗІ).

Необхідно визначити, якими з можливих способів можуть здійснюватися загрози в АС:

- технічними каналами, що включають канали побічних електромагнітних випромінювань і наводок, акустичні, віброакустичні, акусто-електричні, оптичні, радіо- та радіотехнічні, хімічні та інші канали;
- каналами спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації;
- несанкціонованим доступом шляхом підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм та вкорінення комп'ютерних вірусів.

За характером дій зловмисник може здійснювати активні чи пасивні загрози ресурсам АС. Під активною загрозою розуміється спроба навмисної несанкціонованої зміни стану АС, а під пасивною загрозою – спроба несанкціонованого проникнення в систему без зміни її стану. При цьому за характером дій порушників можна класифікувати на:

- "випадкових порушників" – авторизованих користувачів, які порушили політику безпеки тієї чи іншої послуги не навмисно, а помилково – шляхом випадкового подолання засобів управління (адміністрування) доступом до об'єкту захисту, виконання непередбачених дій відносно цього об'єкту 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 і отримати змогу фізичного доступу до засобів оброблення, зберігання чи передавання інформаційних об'єктів з метою виведення їх з ладу, зміни режимів функціонування, крадіжки чи пошкодження 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 по технічним каналам, мережне обладнання локальних чи розподілених мереж, в тому числі і засоби телекомунікаційних мереж.

Слід врахувати також, що *порушення* з боку цих осіб *можуть бути як ненавмисними, так і зловмисними*. Особливу небезпеку слід очікувати від зловмисних порушників. ***Ненавмисний порушник*** може здійснювати випадкові загрози (див. нижче) ресурсам АС під час виконання своїх функціональних обов'язків внаслідок помилкових дій, за рахунок неуважності чи недбалості.

Така класифікація дозволяє більш чітко визначати способи несанкціонованих дій порушників – перелік загроз ресурсам АС та засоби, які потрібні для їх унеможливлення.

II Методика аналізу загроз ресурсам АС

Для аналізу загроз ресурсам АС необхідним є, перш за все, визначення можливих каналів та видів загроз ресурсам АС чи інформації, що можуть бути реалізовані відносно комп'ютерних систем слід здійснити аналіз основних джерел їх походження. Як відомо [1 – 3], основними видами джерел загроз є:

1. зміна умов фізичного середовища (стихійні лиха й аварії, як землетрус, пожежа чи інші випадкові події);
2. наслідки помилок під час проектування і розробки компонентів ЛОМ (технічних засобів, технології обробки інформації, програмних засобів, засобів захисту, структур даних і т.п.);
3. збої і відмовлення в роботі устаткування і технічних засобів ЛОМ;
4. помилки персоналу (користувачів) комп'ютерних систем під час експлуатації;
5. навмисні дії (спроби) потенційних порушників – спроби несанкціонованого доступу до інформаційних ресурсів АС.

Загрози, джерела яких мають природу 1 – го та 2 – го видів, розглядати не доцільно, оскільки засобів технічного захисту інформації від них не існує.

Аналіз загроз, які створюються навмисними діями потенційних порушників, доцільно розглядати з використанням моделі захищеного об'єкта, приклад якої наведено на рис. 1.

Для моделі об'єкта, що підлягає захисту, слід визначити механізми впливів загроз на об'єкт захисту. Для визначеності в подальшому будемо вважати, що об'єктом захисту є ресурси локальної обчислювальної мережі, яка, в свою чергу, є елементом розподіленої обчислювальної мережі. Для таких умов слід вважати, що загрози об'єкту захисту (інформаційним ресурсам ЛОМ) можуть здійснюватися шляхом несанкціонованого доступу (НСД) при безпосередніх чи дистанційних впливах на об'єкти захисту наступними можливими способами:

1.безпосередній вплив (з безпосереднім доступом до об'єкту захисту) є можливим при умові подолання порушником:

- засобів організаційного обмеження доступу;
- засобів охоронної сигналізації;
- засобів адміністрування доступу (проблемно – орієнтованих засобів захисту базового програмного забезпечення – операційних систем та систем управління базами даних (при їх наявності), включаючи маскування під зареєстрованого користувача з метою використання інформації чи нав'язування помилкової інформації, застосування заставних пристроїв чи програм і впровадженням комп'ютерних вірусів).

2. дистанційний вплив можливий за рахунок:

- 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.

Модель загроз визначає перелік можливих загроз і класифікацію їх за результатами впливу на інформацію, тобто на порушення яких властивостей вони спрямовані (конфіденційності, цілісності і доступності інформації), а також порушення спостереженості і керованості комп'ютерних систем.

Випадковими загрозами суб'єктивної природи (дії, що здійснюються персоналом чи користувачами через неуважність, недбалість, незнання і т. п., але без навмисного наміру) є:

- дії, що приводять до відмовлення комп'ютерних систем (окремих компонентів), руйнування апаратних, програмних, інформаційних ресурсів (устаткування, видаленню даних, програм і ін.);

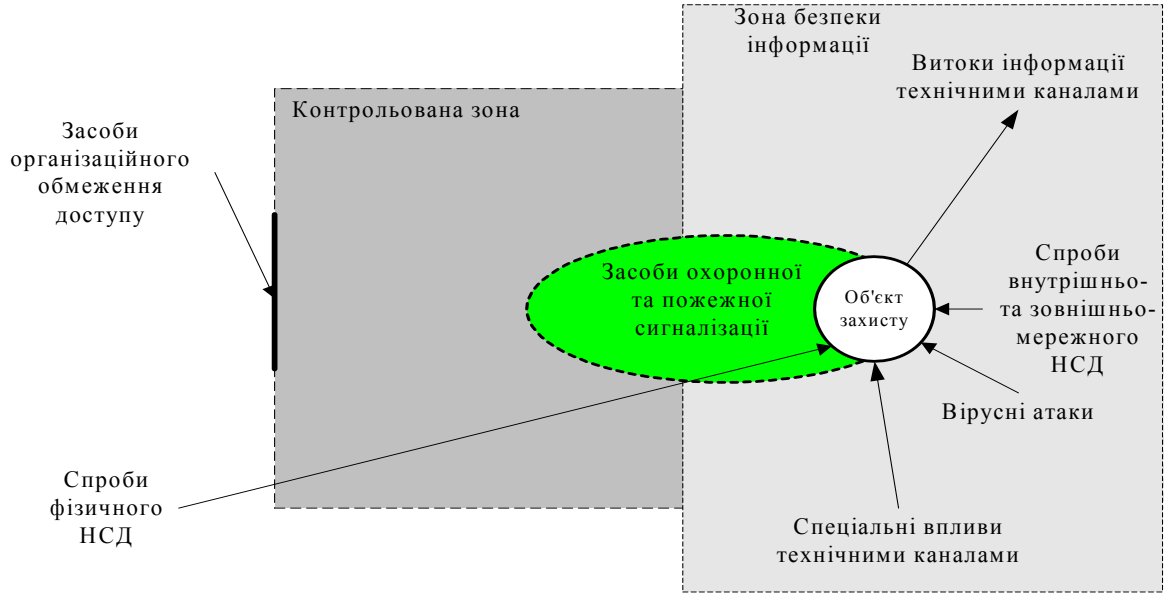

Рисунок 1 – Приклад моделі захищеного об'єкта

- ненавмисне ушкодження носіїв інформації;
- неправомірна зміна режимів роботи комп'ютерних систем (окремих компонентів, устаткування, програмного забезпечення (ПЗ) і т.п.), ініціювання тестуючих чи технологічних процесів, здатних привести до необоротних змін у системі (наприклад, форматування носіїв інформації);
- ненавмисне зараження ПЗ комп'ютерними вірусами;
- невиконання вимог до організаційних заходів захисту діючих ЛОМ розпорядницьких документів;
- помилки при введенні даних у систему, видача даних за невірними адресами пристроїв, внутрішніх абонентів і т. п.;
- будь-які дії, що можуть привести до розголошення конфіденційних відомостей, атрибутів розмежування доступу, втрати атрибутів і т. п.;
- неправомірне впровадження і використання забороненого політикою безпеки ПЗ (наприклад, навчальні й ігрові програми, системне і прикладне забезпечення й ін.);
- наслідки некомпетентного застосування засобів захисту.

Навмисними загрозами суб'єктивної природи, спрямованими на дезорганізацію роботи комп'ютерних систем (окремих компонентів) чи виводу її з ладу, проникнення в систему й одержання можливості несанкціонованого доступу до її ресурсів, є:

- порушення фізичної цілісності комп'ютерних систем (окремих компонентів, пристроїв, устаткування, носіїв інформації);
- порушення режимів функціонування (вивід з ладу) систем життєзабезпечення комп'ютерних систем (електроживлення, заземлення, охоронної сигналізації, вентиляції й ін.);
- порушення режимів функціонування комп'ютерних систем (устаткування і ПО);
- впровадження і використання комп'ютерних вірусів, заставних (апаратних і програмних) пристроїв, що підслуховують, інших засобів розвідки;
- використання засобів перехоплення побічних електромагнітних випромінювань і наведень, акусто-електричних перетворень інформаційних сигналів;
- використання (шантаж, підкуп і т. п.) з корисливою метою персоналу комп'ютерних систем;
- крадіжки носіїв інформації, виробничих відходів (роздруківок, записів, і т. п.);
- несанкціоноване копіювання носіїв інформації;
- читання залишкової інформації з оперативної пам'яті ЕОМ, зовнішніх накопичувачів;
- одержання атрибутів доступу з наступним їхнім використанням для маскування під зареєстрованого користувача ("маскарад");
- впровадження і використання забороненого політикою безпеки ПЗ чи несанкціоноване використання ПЗ, за допомогою якого можна одержати доступ до критичної інформації (наприклад, аналізаторів безпеки мереж).

Зрозуміло, що кожна з загроз здійснюються з деякою ймовірністю, може порушувати ту чи іншу

функціональну властивість захищеної системи, має своїм наслідком (особливо навмисні загрози) певні втрати (шкоду) та джерело виникнення чи активізації.

Загрози, пов'язані з діяльністю зареєстрованих користувачів, в свою чергу, можуть розподілятися на випадкові чи навмисні. Випадковими загрозами є загрози, які здійснюються персоналом або користувачами по неуважності, недбалості, незнанню тощо, але без спеціального наміру. Зрозуміло, що кожна з загроз здійснюються з деякою ймовірністю, може порушувати ту чи іншу функціональну властивість захищеної системи, має своїм наслідком (особливо навмисні загрози) певні втрати (шкоду) та джерело виникнення чи активізації. Врахування цього надає можливість подальшої розробки ефективних засобів системи технічного захисту інформації, які в першу чергу забезпечують захист від найбільш імовірних та шкідливих загроз.

З цією метою слід визначити найбільш імовірні властивості захищеності інформації, які порушуються внаслідок впливу загроз кожного з їх типів, тобто здійснити їх ідентифікацію у вигляді переліку загроз з констатацією відповідності властивостям захищеності ресурсів АС, на порушення яких вони спрямовані (конфіденційності (к), цілісності (ц), доступності (д), спостереженості та керованості (с) АС). Приклад такої ідентифікації наведено нижче в таблиці.

В цій таблиці показано також оцінку ризиків, тобто ймовірності здійснення загроз та рівень збитків (шкоди) від порушень по кожному з видів порушень, і джерела (чи джерело) виникнення загроз, – які внутрішні чи зовнішні суб'єкти можуть ініціювати загрозу. Оцінка ризиків здійснена згідно з рекомендаціями нормативних документів у вигляді якісної оцінки ймовірностей реалізації загроз (незначна, низька, висока, неприпустимо висока) при допущенні, що закон розподілу ймовірностей кожної з них є найгіршим для реалізації захисту – рівномірним. Оцінка рівня шкоди внаслідок реалізації загроз розглядається як очікувані збитки від втрати об'єктами захисту кожної з властивостей захищеності (к, ц, д) або втрати спостереженості та керованості (с). Ця оцінка здійснена також за якісною шкалою (відсутня, низька, середня, висока, неприпустимо висока).

Аналіз найпоширеніших загроз – методів несанкціонованого доступу

Серед найбільш розповсюджених загроз шляхом несанкціонованого доступу (НСД) до інформаційних ресурсів АС – методів подолання ("зламу") засобів управління доступом – слід відзначити:

1. комплексний пошук можливих методів НСД; зловмисники винятково ретельно вивчають системи безпеки перед проникненням у неї; дуже часто вони знаходять очевидні й дуже прості методи подолання системи, які розробники просто "прогледіли", створюючи можливо дуже гарну систему ідентифікації або шифрування;

2. НСД через термінали захищеної інформаційної системи – точки входу користувача в інформаційну мережу; у тому випадку, коли до них мають доступ кілька людей або взагалі будь-який бажаючий, при їхньому проектуванні й експлуатації необхідно ретельно дотримуватися комплексу заходів безпеки, в тому числі, а можливо і насамперед, організаційних;

3. НСД шляхом спроб входу в систему зовсім без знання пароля, ґрунтуючись на викривленнях у реалізації програмного або апаратурного забезпечення, тобто шляхом підбору пароля;

4. НСД шляхом маскування під авторизованого користувача передбачає попереднє отримання паролю тим чи іншим чином, наприклад, на основі помилок адміністратора та користувачів.

III Методика розроблення моделі загроз. Аналіз загроз та складу можливих контрзаходів

Модель загроз ресурсам АС – максимально повний і деталізований перелік загроз ресурсам АС, розробляється для аналізу цих загроз та їх наслідків. Для побудови такої моделі слід здійснити аналіз моделі порушника і визначити несанкціоновані дії (навмисні чи випадкові), які може здійснити кожен із таких порушників відносно ресурсів АС (перш за все – інформаційних). Окрім того, слід проаналізувати також впливи природних факторів. Такі несанкціоновані дії, а також інші обставини, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків АС, прийнято називати загрозами. Перелік таких можливих загроз є основою для розроблення моделі загроз. Нижче пропонується приклад методики розроблення моделі загроз у вигляді таблиці. Методика розроблення такої моделі полягає в тому, що: в один із стовпчиків таблиці заноситься по можливості повний перелік видів загроз; в наведеному прикладі такий перелік (на погляд автора, повний) наведено в стовпчику 2.

Надалі для кожної із можливих загроз шляхом їх аналізу (можливо і методом експертних оцінок) необхідно визначити:

- ймовірність виникнення таких загроз. В таблиці наведена якісна оцінка їх ймовірності – неприпустимо висока, дуже висока, висока, значна, середня, низька, знехтувано низька (стовпчик 3);

- на порушення яких властивостей інформації або АС вона спрямована (рекомендується користуватись чотирма основними градаціями – порушення конфіденційності – к, цілісності – ц, доступності – д інформації, а також порушення спостереженості та керованості – с АС) (стовпчик 4);
- можливий (такий, що очікується) рівень шкоди (стовпчик 5);
- джерела виникнення (які суб'єкти АС, зовнішні чи внутрішні відносно неї, можуть ініціювати загрозу) (стовпчик 6).

Для створення цього прикладу моделі автор намагався проаналізувати якомога більшу кількість доступних інформаційних джерел та спирається на власний досвід розроблення політики безпеки інформації для досить складних АС у вигляді розподілених обчислювальних мереж (за класифікацією НД ТЗІ – АС класу 3.КЦД).

Слід врахувати, що наведені оцінки ймовірностей та величини можливої шкоди кожної із загроз в даному прикладі моделі загроз носять ілюстративний характер. Для випадків конкретних АС ці величини повинні бути визначеними фахівцями служби захисту відповідного підприємства.

Таблиця. Характеристика загроз ресурсам АС та їх наслідків

№	Вид загрози	Ймовір-ність	Що пору-шує	Рівень шкоди	Джерело
1	2	3	4	5	6
Навмисні загрози (з боку зловмисників)					
1.	Порушення фізичної цілісності АС (її окремих компонентів), пристроїв, обладнання, носіїв інформації	висока	к, ц, д, с	непри–пустимо високий	внут. зовн.
2.	Доступ до даних з порушенням встановлених правил розмежування доступу з метою ознайомлення, модифікації, копіювання, знищення даних тощо	низька	к, ц, д, с	непри–пустимо високий	внут. зовн.
3.	Модифікація інформаційних ресурсів, в тому числі програмного забезпечення	низька	ц, д, с	непри–пустимо високий	внут. зовн.
4.	Несанкціоноване змінювання повноваження інших користувачів	низька	к, ц, д, с	непри–пустимо високий	внут. зовн.
5.	Порушення режимів функціонування (виведення з ладу) систем життєзабезпечення АС (електроживлення, заземлення, охоронної чи пожежної сигналізації, вентиляції та ін.)	висока	ц, д, с	непри–пустимо високий	внут. зовн.
6.	Порушення режимів функціонування АС (обладнання та ПЗ)	висока	к, ц, д, с	непри–пустимо високий	внут. зовн.
7.	Впровадження і використання комп'ютерних вірусів, закладних (апаратурних і програмних) і пристроїв для підслуховування, інших засобів технічної розвідки, навмисно включати до складу програмного забезпечення спеціальні блоки для порушення безпеки даних	висока	к, ц, д, с	середній	внут. зовн.
8.	Використання персоналу АС (шантаж, підкуп тощо) з корисливою метою	висока	к, ц, д, с	високий	внут. зовн.
9.	Видавання власних несанкціонованих запитів за запити операційної системи	середня	к, ц, д, с	середній	внут.
10.	Отримання захищених даних за допомогою спеціально організованої серії санкціонованих запитів	середня	к, ц, д, с	середній	внут. зовн.
11.	Читання залишкової інформації з оперативної	низька	к	високий	внут.

№	Вид загрози	Ймовір-ність	Що пору-шує	Рівень шкоди	Джерело
	та зовнішньої пам'яті ЕОМ				
12.	Одержання атрибутів доступу з наступним їх використанням для маскування під зареєстрованого користувача, незаконне розширювання своїх повноважень, видавання себе за зареєстрованого користувача, вивчання права доступу інших користувачів	низька	к, ц, д, с	непри–пустимо високий	внут. зовн.
13.	Неправомірне підключення (в тому числі, наприклад, "врізання" в канал пар типу "модем – модем") до каналів зв'язку, перехоплення даних, що передаються, зміна (модифікація) інформації повідомлень (в тому числі службової, наприклад, адрес передавача та отримувача повідомлень	непри–пусти–мо висока	к, ц, д, с	непри–пустимо високий	зовн.
14.	Маскування захищених даних під незахищені	Дуже висока	к	високий	внут.
15.	Впровадження і використання забороненого політикою безпеки ПЗ або несанкціоноване використання ПЗ, за допомогою якого можна одержати доступ до критичної інформації (наприклад, аналізаторів безпеки мереж) та ін.	висока	к, ц, д, с	високий	внут. зовн.
16.	Несанкціоноване копіювання носіїв інформації	висока	к	висока	внут.
17.	Крадіжки носіїв інформації, виробничих відходів (роздруківок, записів тощо)	низька	к	середній	внут.
18.	Фальсифікація фактів формування та видачі даних	висока	ц	високий	внут.
19.	Підтвердження отримання від деякого користувача даних, сформованих самим порушником	висока	ц	високий	внут.
20.	Підтвердження передачі якому–небудь користувачеві даних, які не передавалися	висока	ц	середній	внут.
21.	Фальсифікація фактів отримання даних	висока	ц	середній	внут.
22.	Розкриття змісту даних у каналах зв'язку	висока	к	високий	внут.
23.	Виконання аналізу потоку даних (трафіку)	висока	д, с	низький	внут. зовн.
24.	Змінювання потоку даних, наприклад шляхом генерації несправжніх повідомлень для перевантаження системи	висока	ц, д, с	високий	внут. зовн.
25.	Переривання передачі потоку даних	дуже висока	ц, д	Непри-пустимо високий	внут. зовн.
26.	Виконання ініціації фіктивного з'єднання	середня	ц, д	високий	внут.
Випадкові загрози					
27.	Дії, що призводять до відмови АС чи окремих її елементів, руйнування апаратурних ресурсів (в тому числі обчислювальних ресурсів – процесорів та носіїв даних) та обладнання, в тому числі телекомунікаційного, засобів вводу/ виводу, програмних та інформаційних ресурсів (як базових так і прикладних, файлів, наборів даних тощо)	низька	к, ц, д, с	непри–пустимо високий	внут.

№	Вид загрози	Ймовір-ність	Що пору-шує	Рівень шкоди	Джерело
28.	Ненавмисне пошкодження носіїв інформації чи інформації, яка зберігається на цих носіях	низька	к, ц	низький	внут.
29.	Неправомірна зміна режимів роботи АС (її окремих компонентів, обладнання, програмних засобів тощо), ініціювання технологічних чи тестуючих процесів, які здатні призвести до незворотних змін у системі (наприклад форматування носіїв інформації)	низька	к, ц, д, с	непри–пустимо високий	внут.
30.	Невмисне зараження програмних засобів (ПЗ) комп'ютерними вірусами	значна	к, ц, д, с	непри–пустимо високий	внут.
31.	Невиконання організаційних заходів щодо порядку і правил експлуатації чи використання ресурсів АС, передбачених "Планом ТЗІ", посадовими чи іншими, в тому числі технологічними інструкціями	низька	к, ц, д, с	непри–пустимо високий	внут.
32.	Помилки при введені даних в систему, видачі даних за невірними адресами пристроїв, внутрішніх і зовнішніх абонентів тощо	низька	к, ц, д, с	високий	внут.
33.	Неправомірне впровадження і використання забороненого політикою безпеки програмного забезпечення (системне, прикладне ПЗ, навчальні та ігрові програми та ін.)	низька	к, ц, д, с	низький	внут.
34.	Некомпетентне застосування засобів захисту	висока	к, ц, д, с	високий	внут.
35.	Наслідки викривлень під час проектування та розробки компонентів АС (технічних засобів, технології обробки інформації, програмних засобів, засобів захисту, структур даних тощо);	низька	к, ц, д, с	непри–пустимо високий	внут.
Впливи природних факторів					
36.	Зміна умов фізичного середовища (стихійні лиха, як землетрус, повінь, пожежа і аварії або інші випадкові події)	низька	ц, д, с	непри–пустимо високий	зовн.
37.	Збої та відмови у роботі обладнання та технічних засобів АС, аварійне відключення живлення та т.п.	низька	ц, д, с	непри–пустимо високий	внут.
38.	Впливи природних завад (грозові розряди, іскріння в електромережах, під час електрозварювання та т.п.	низька	ц, д, с	низький	зовн.

Зрозуміло також, що для кожної конкретної АС перелік загроз можуть бути звуженим чи, навпаки, розширеним, але інформації, наведеної в таблиці, як основи для наших подальших міркувань, досить ніж достатньо.

З даної моделі загроз можна зробити висновок, що для реалізації загроз тій чи іншій властивості захищеності інформації порушник може діяти дистанційно (через засоби зв'язку, витоки інформації чи навпаки через засоби спеціального впливу технічними каналами) або безпосередньо (в тому числі і шляхом фізичного впливу) на елементи локальних обчислювальних мереж. В останньому випадку порушнику необхідно отримати фізичний доступ до згаданих елементів локальних обчислювальних мереж (тобто подолати засоби організаційного обмеження доступу та, при необхідності, охоронної сигналізації). Ці обставини можуть суттєво вплинути на склад засобів захисту відповідних властивостей захищеності інформації.

Модель загроз є також основою для аналізу можливих збитків внаслідок відсутності засобів чи заходів захисту, а відтак, і для визначення можливих контрзаходів. З моделі загроз витікає необхідність захисту від впливу загроз усім властивостям захищеності інформації, насамперед від загроз, наслідком реалізації яких може бути неприпустимо високий чи високий рівень шкоди (загрози № 1 – 10, 12, 13, 15, 27, 29 – 38), оскільки такі загрози мають комплексний, тобто одночасний вплив на декілька властивостей захищеності. Такі загрози прийнято називати найбільш суттєвими загрозами. Величину втрат, збитків, шкоди тощо, які може потерпати власник інформації (чи АС) внаслідок того, що в силу недосконалості (а, можливо, і відсутності) заходів та засобів захисту частка загроз зможе вплинути на функціональні властивості захищеності інформації, будемо називати залишковим ризиком.

Зрозуміло, що визначення найбільш суттєвих (найбільш небезпечних, найбільш імовірних) загроз є основою для визначення в подальшому потрібних засобів захисту відповідних функціональних властивостей захищеності інформаційних ресурсів, а отже визначення складу потрібних контрзаходів для забезпечення припустимої захищеності, необхідних для захисту засобів, підсистем, механізмів та функцій захисту, тобто дає змогу будувати відповідні моделі систем захисту.

В свою чергу, знання можливих чи потрібних контрзаходів, як побачимо далі, дає можливість визначення складу, характеристик та можливостей застосування тих чи інших способів, механізмів, функцій, здатних протистояти чи зменшити вплив кожної із визначеної множини загроз.

Взагалі, **до складу можливих контрзаходів** для забезпечення припустимої захищеності та зменшення залишкового ризику слід відносити:

1. ухилення від можливих загроз;
2. зміна характеру можливої загрози;
3. сприйняття допустимості реалізації певних загроз з певним рівнем залишкового ризику і, відповідно, певного рівня збитків;
4. зменшення можливості реалізації загроз шляхом застосування заходів захисту.

Для визначення можливості застосування тих чи інших контрзаходів з метою забезпечення припустимої захищеності та величин залишкового ризику на підставі побудованих моделей порушників та загроз слід здійснити їх аналіз з метою визначення початкового стану захищеності АС та, відповідно, можливої величини (рівня) шкоди від реалізації загроз, хоча б на якісному рівні. Порядок здійснення цього аналізу проілюструємо для умов введеної моделі порушника та представленої в таблиці моделі загроз.

1. Аналіз можливостей ухилення від можливих загроз ґрунтується на розумінні того, що таке ухилення є можливим шляхом:

- максимального зменшення числа користувачів, в першу чергу за рахунок найбільш небезпечних з них (з погляду можливих загроз ресурсам);
- запобігання підключенню терміналів, що є елементами АС, до інших мереж, наприклад, до Internet;
- обмеження повноважень користувачів до мінімально допустимих, коли ще забезпечується реалізація основних функцій;
- винесення всіх елементів, які можуть бути джерелом витоку інформації технічними каналами, за межі зон безпеки та таке інше.

2. Аналіз можливостей зміни характеру можливого ризику ґрунтується на розумінні того, що така зміна може бути застосованою, якщо неможливо іншим шляхом запобігти можливим загрозам, або зменшити можливу шкоду. Прикладами такого підходу є:

- страхування обладнання чи можливих збитків від стихійних лих;
- включення до договорів з постачальниками засобів обчислювальної техніки, загальносистемного програмного забезпечення та інших комплектуючих складових умов щодо відшкодування збитків, які виникли за рахунок використань таких засобів непередбачених відповідними інструкціями.

3. Аналіз можливостей сприйняття допустимості реалізації певних загроз з певним рівнем залишкового ризику і, відповідно, певним рівнем збитків ґрунтується на розумінні того, що деякі з ризиків мають низьку ймовірність та низький рівень шкоди (наприклад, загрози № 28, 33, 38) або не можуть бути зменшеними до знехтувано малої величини. На практиці, навіть після прийняття певного набору контрзаходів, ряд ризиків зменшується, але залишається ще значним. Для таких загроз необхідно знати чи визначити залишкову величину ризику (величину залишкового ризику) та рівень витрат на його зменшення. При цьому, зрозуміло, сприйняття допустимості реалізації певних загроз є доцільним завжди, якщо:

- витрати на захист від таких загроз перевищують рівень збитків;
- усі стандартні можливості запобігання загрозам є вичерпаними.

У результаті аналізу можливостей реалізації кожного з розглянутих можливих контрзаходів для забезпечення припустимої захищеності та залишкового ризику слід визначити **стратегію управління**

ризиками без застосування заходів та засобів захисту.

4. В разі неприйнятності деяких із підходів визначеної стратегії управління ризиками, для подальшого зменшення можливості реалізації загроз необхідним є **застосування заходів та засобів захисту**. Зрозуміло, що відтепер розмову слід вести про захист лише від тих загроз, від яких не можна ухилитися, змінити їх характер чи сприйняти допустимість їх реалізації з певним рівнем залишкового ризику і, відповідно, певним рівнем збитків. Тобто слід внести відповідні зміни в модель загроз шляхом необхідної корекції таблиці.

Після вибору конфігурації можливої системи захисту та визначення параметрів її елементів (відповідних ймовірностей подолання засобів захисту певними загрозами, чи, навпаки, ймовірностей протистояти цим загрозам) слід зробити оцінку залишкового ризику (методика такої оцінки розглядається нижче), який забезпечується при застосуванні засобів забезпечення кожної з властивостей захищеності відповідних ресурсів, і повторити етапи 3 та 4 даної методики (аналіз можливостей сприйняття допустимості реалізації певних загроз з певним рівнем залишкового ризику і застосування заходів та засобів захисту). При цьому будуть виявленими загрози, для яких уже застосовані заходи та засоби не дали бажаного ефекту. Тому проти таких загроз слід розробляти (чи вибирати) більш ефективні, а отже більш витратні заходи чи засоби захисту. Ці етапи слід повторювати доти, поки не буде прийнятим рішення щодо сприйняття допустимості реалізації усіх загроз з тим рівнем залишкового ризику, який вдалося досягти при прийнятних витратах.

Таким чином, наведені методики надають змогу здійснення досить глибокого і достовірного аналізу можливих порушників, загроз ресурсам автоматизованих систем з боку цих порушників, визначення можливих контрзаходів для протидії цим загрозам, в тому числі, складу необхідних засобів захисту з метою забезпечення припустимої захищеності АС.

Література: ***1.*** *Астахов А. Актуальные вопросы выявления сетевых атак. JetInf0 № 3 (106), 2002. На сайті http://www.jetinfo.ru/2002/3/1/article1.3.2002.html;* ***2.*** *Астахов А. Анализ защищенности корпоративных систем. // Открытые системы, № 07-08/2002. На сайті http://www.osp.ru/os;* ***3.*** *Будько М. М. Визначення залишкового ризику при оцінці захищеності інформації в інформаційно – обчислювальних системах // К.: НТУ "КПІ" //Правове, нормативне та метрологічне забезпечення Системи захисту інформації в Україні. Випуск 8 // 2004, с. 20-26;* ***4.*** *Будько М. М., Василенко В. С., Проскурін В. М. Методика оцінки захищеності інформації в ЛОМ // К.: Військовий інститут інформатизації та телекомунікацій НТУУ "КПІ" Збірка доповідей на II НТК інституту "Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення";* ***5.*** *Василенко В. С., Будько М. М. Методики визначення вихідних даних для оцінки залишкових ризиків у ЛОМ // К.: НТУ "КПІ" // Правове, нормативне та метрологічне забезпечення Системи захисту інформації в Україні. Випуск 9 // 2004, с. 110-120.*

УДК 681.3.06

АНАЛІЗ СКЛАДУ ПРОФІЛІВ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ

Анатолій Антонюк, Денис Берестов, Сергій Пустовіт

Національний науково-дослідний центр оборонних технологій і воєнної безпеки України

Анотація: **Вивчається основне поняття нормативних документів системи технічного захисту інформації – стандартний функціональний профіль захищеності. Розглядаються питання його формалізації та пропонується підхід щодо оцінки рівня захищеності автоматизованих систем та вартості реалізації профілів.**

Summary: **It's studied basic conception normative system document technical protection to information - standard functional profile protectability. They are considered question to it's formalizations and is offered approach for estimations level protectability computer-based systems and cost to realization of the profiles.**

Ключові слова: **нормативні документи, автоматизована система**

Вступ

В нормативних документах із захисту інформації в автоматизованих системах (АС) [1 - 4] визначено важливе поняття стандартного функціонального профілю захищеності, причому для кожного з класів введеної в [3] класифікації АС визначена певна їх кількість. В поданому списку вони розміщені за певним ієрархічним принципом і фактично складають затверджений довідник для практичного застосування. Проте, навіть зважаючи на їх ієрархічність, виникає проблема вибору найбільш придатного профілю,