УДК 65.012.8 **Архипов О.Є. (НТУУ "КПІ")**

ЩОДО МЕТОДИКИ ІДЕНТИФІКАЦІЇ ТА ОЦІНЮВАННЯ АКТИВІВ СИСТЕМИ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Розглянуто теоретико-практичні аспекти реалізації процедури ідентифікації та оцінювання активів інформаційних систем відповідно до рекомендацій стандарту ISO/IEC 13335-3. Запропоновано деякі способи підвищення ефективності реалізації цієї процедури.

Згідно міжнародному стандарту ISO/IEC TR 13335-3, якому відповідає український національний стандарт ДСТУ ISO/IEC TR 13335-3 : 2003, стратегічним моментом керування інформаційною безпекою організації є правильний вибір прийнятного для даної організації рівня ризику. Цей вибір напряму залежить від цілей, що ставить перед собою організація при створенні системи забезпечення інформаційної безпеки. Для того, щоб оцінити та сформулювати такі цілі, необхідно вивчити активи організації та визначити їх цінність для цієї організації ([1], розділ 7.1). Таким чином, вибрана організацією стратегія інформаційної безпеки повинна відповідати цінності активів, що захищаються, у зв'язку з чим визначення цінності активів стає однією з ключових задач побудови системи безпеки. На жаль, деталізація процедури оцінювання активів в стандартах [1,2] відсутня, її зміст обмежено рекомендаціями загального характеру та рядом прикладів, методичний бік проблеми оцінювання активів практично недосліджений.

Метою даної статті є аналіз теоретико-методичних аспектів оцінювання активів організації та застосування результатів цього аналізу для формування технології оцінювання активів.

За стандартом [1], активи організації – це усе, що має цінність для організації, причому цінність кожного активу визначається його важливістю щодо ділової (функціональної) складової діяльності організації. Зокрема. якщо мова йде про безпеку системи ІТ, що застосовуються в межах певної організації, оцінюванню підлягають насамперед активи цієї системи, причому при визначенні їх цінності має враховуватися те, наскільки може постраждати ця діяльність через виток, спотворення, недоступність та/або руйнування інформації, тобто внаслідок реалізації загроз по відношенню до ресурсів інформаційно-телекомунікаційної системи (ІТС)організації . Таким чином, ідентифікація та оцінювання активів, які були проведені на основі обліку ділових інтересів організації, є основним фактором у визначенні ризику.

Однак зазвичай оцінюванню активів передує кілька допоміжних етапів, один з яких – це етап інвентаризації (ідентифікації) активів. За результатами інвентаризації активів складається перелік важливих для організації активів, в якому можна виділити дві групи активів: активи системи ІТ (за вітчизняною термінологію – ресурси інформаційно-телекомунікаційної системи (ІТС)) та другу групу активів, куди увійшли всі інші активи організації, цінність яких залежить від стану активів першої групи.

До активів системи ІТ звичайно відносять

- інформаційні активи: бази даних, файли даних, системну документацію, настанови користувачеві, архівірована інформацію тощо;
- активи програмного забезпечення (ПЗ): системне ПЗ, прикладне ПЗ, інструментальні засоби, утиліти;
- фізичні активи: комп'ютерне устаткування (процесори, монітори, модеми й т.п.), апаратура зв'язку (АТС, маршрутизатори, телефони тощо), інше технічне обладнання, споруди та приміщення ІТС;
- персонал та співробітники ІТС.

Склад активів другої групи (інші активи організації) суттєво залежить від сфери, в якій функціонує організація, її фінансового становища, підпорядкованості тощо. Зокрема це

нематеріальні активи: репутація, імідж організації, рівень її ділової активності. Сюди ж слід віднести комунальні активи: освітлення, кондиціювання, обігрів, електроживлення. Нарешті, це можуть бути переліки робіт, заказів, організацій-суміжників, постачальників, списки продукції, що виробляється організацією, та інше. Загалом перелік активів другої групи можуть бути досить об'ємним. Щоб його раціонально звузити й одночасно не втратити чогось важливого, оцінюванню активів передує ще один додатковий етап – визначення меж огляду [1]. Його задача – виділити ті аспекти ділової діяльності організації, які залежать від інформаційно-телекомунікаційних технологій (ІТТ), що використовуються організацією. З метою виявлення цих аспектів діяльність організації треба проаналізувати за двома групами критеріїв. Критерії першої групи дозволяють виявити межи залежності організації від ІТТ й спираються на наслідки аналізу наступних положень:

- наскільки важлива частина бізнесової діяльності, яка вимагає обов'язкового залучення ІТТ;
- які профільні (виробничі) задачі організації можуть бути реалізовані тільки за допомогою ІТТ.

Друга група критеріїв спрямована на виявлення інформації, що потребує захисту, й на аналіз можливих наслідків реалізації загроз щодо цієї інформації:

- які важливі рішення, що приймаються в організації, залежать від точності, цілісності, доступності та конфіденційності інформації, оброблюваної в ІТТ;
- яка оброблювана інформація потребує захисту;
- які наслідки можуть виникнути після інциденту, пов'язаного з порушенням безпеки критичної інформації.

Закінчивши інвентаризацію активів, можна переходити безпосередньо до встановлення цінності активів. Основою для визначення цінності може бути:

1) вартість створення та обслуговування активу;
2) вартість модернізації та відновлення активу;
3) збиток, що наноситься організації у випадку порушення конфіденційності, цілісності або доступності інформаційних активів;
4) комбінація трьох попередніх варіантів, що дає змогу отримати певну інтегральну оцінку загальної цінності активу.

Найбільш поширеним в практичних застосуваннях є спосіб обчислення цінності активів, в основі якого лежить третій з вищенаведених варіантів. Зокрема, рекомендації щодо його застосування приведені в обов'язкових додатках В, Е до стандарті [1]. При аналізі цього способу обчислення цінності активів треба приймати до уваги два наступних моменти. По-перше, точкою введення загроз в ІТС є вразливість активів системи ІТ, тоді як наслідки реалізації цих загроз треба оцінювати на повній множині активів організації: активи системи ІТ + активи другої групи. По-друге, на певному кроці реалізації будь-якої загрози інформації цю загрозу можна звести до однієї із трьох: конфіденційності, доступності та цілісності, що дозволяє спростити і скоротити аналіз наслідків успішної реалізації загроз, зокрема, обрахунок відповідних збитків. В [1] відмічається, що при розгляді інформаційних загроз слід аналізувати їх можливі наслідки, що призводять (серед іншого) до:

- зниження рівня ділової активності організації;
- втрати/погіршення репутації організації;
- фінансових втрат;
- перебоїв у виконанні ділових операцій;
- погіршенню інвестиційного клімату;
- виникненню загроз особистої безпеки і т.п.

Формально оцінювання збитку можна представити у вигляді триетапної процедури. При її формуванні будемо виходити з того факту, що в організації об'єктом прикладання загроз є інформаційні ресурси та елементи інформаційної інфраструктури (обладнання,

програмне забезпечення, персонал), які разом складають деяку підмножину активів системи ІТ: $AS^{\inf} \subset AS$, тоді як наслідки реалізації загроз (збитки організації) визначаються на всій множині AS активів організації.

На першому етапі процедури оцінювання збитків виконується інвентаризація активів організації, результат якої – список активів, що визначає повну множину активів організації: $AS = \{as_i\}$, $i = \overline{1, n_A}$. Встановлюється перелік можливих загроз інформації $T = \{t_k\}$, $k = \overline{1, n_t}$. Формується підмножина $AS^{\inf 1} \subset AS^{\inf}$, що включає лише ті активи системи ІТ організації, до яких в принципі можливе застосування будь-яких загроз зі складу множини T.

В ході другого етапу виконується аналіз всіх можливих пар виду $\left\langle as_l^{\inf 1}, as_i \right\rangle$, за результатами якого визначаються групи активів, що асоціюються з кожним з інформаційних активів $as_l^{\inf 1}$, відносно якого може бути реалізована загроза. На третьому етапі, в ході аналізу всіх можливих трійок $\left\langle t_k, as_l^{\inf 1}, as_i \right\rangle$, $i = \overline{1, n_A}$, виявляються збитки q_{ik}, що завдаються активам as_i, $i = \overline{1, n_A}$ організації у випадку реалізації загрози t_k відносно інформаційного активу $as_l^{\inf 1}$, і за сукупним значенням всіх цих збитків, обрахованим за всією множиною активів $AS = \{as_i\}$, визначають часткову цінність відповідного інформаційного активу $as_l^{\inf 1}$ (так звану «надану» цінність [1]).

Наведеній схемі знаходження цінності активу притаманний ряд недоліків.

По-перше, це множинність отримуваних по кожному активу оцінок q_{ik}, кількість яких визначається кількістю тих загроз, наслідки реалізації яких ведуть до потенційних збитків, що вимагають свого обліку. Фактично кожна окрема оцінка q_{ik} відображує лише частковий збиток, що наноситься *i*-му активу as_i реалізацією загрози t_k. При реалізації різних загроз ураженими можуть опинитися як різні елементи, що входять до складу активу, так і частково або повністю співпадаючі. Очевидно, що формування підсумкової цінності активу в цих випадках буде відбуватися по-різному, виходячи з інформації про механізми утворення окремих збитків, яка носить частковий характер та може бути отримана лише під час обстеження конкретної організації. Тому в стандарті [1] відмічається наявність проблеми множинності оцінок активів, але відсутні будь-які загальні рекомендації щодо її вирішення.

По-друге, в цьому ж стандарті [1], п.9.3.3, підкреслюється необхідність обліку наявності взаємозв'язків між різними активами при визначенні рівня цінності кожного з них, що пояснюється існуванням взаємозв'язків певних вразливостей інформаційної системи організації та, відповідно, наявністю взаємозв'язків при реалізації окремих загроз інформації. Також як і у випадку множинності оцінок активів, облік взаємозв'язків активів можливий лише при наявності цілком конкретної інформації про часткові особливості та характеристики функціонування окремих підсистем організації.

По-третє, при великих значеннях n_A та n_t (порядку декількох десятків та більше) кількість аналізованих пар $\left\langle as^{\inf 1}{}_l, as_i \right\rangle$, стає достатньо великою, трійок $\left\langle t_k, as_l^{\inf 1}, as_i \right\rangle$ – ще більшою, а процедура оцінювання значень q_{ik} – надмірно громіздкою та трудомісткою. Знаходження збитку q_{ik} у цьому випадку можливе лише шляхом прямого експертного оцінювання, бо застосування процедур експертно-аналітичного характеру стає нереальним через множину альтернатив, що зіставляються $<as_i, t_k>$, $i = \overline{1, n_A}$, $k = \overline{1, n_t}$, та перевищують рекомендований граничний об'єм 7±2 (число Ингве-Миллера). Безумовно, пряме експертне оцінювання значно спрощує та прискорює процедуру знаходження часткових збитків q_{ik},

проте при цьому експерт навряд чи в дійсності зможе свідомо виділити частковий збиток. В будь-якому випадку рівень суб'єктивних похибок експертизи істотно зростає.

Прикладом одного з найекстремальніших варіантів, що можуть виникати при оцінювані активів, слід вважати ситуацію, в якій організацією, чиї активи оцінюються, є ціла країна. В цьому випадку множина пар <актив-загроза>, які підлягають експертуванню, є фактично незліченною, а відтак застосування до неї наведеної вище процедури оцінювання активів – безглуздою витратою часу. Для отримання працездатної процедури оцінювання активів в цьому прикладі необхідно ввести механізми скорочення кількості співставляємих експертом варіантів пар <актив-загроза> до розумно прийнятної кількості.

Одним з таких механізмів, детально розглянутим в [3], є метод сценарного аналізу збитку, обумовленого реалізацією загроз щодо певного інформаційного ресурсу. За цим методом експерт до кожного ймовірного випадку реалізації загрози визначає скінченну множину можливих сценаріїв розвитку подій-наслідків (3-5 варіантів). Розгортання кожного з сценаріїв асоціюється з деякою конкретною множиною активів, яка за своїм обсягом незрівнянно вужче гіпотетичної повної групи активів. Тому експерт здатний достатньо об'єктивно оцінити наслідки розвитку кожного сценарія, які фактично становитимуть часткові інтегровані оцінки збитків (втрат), обумовлених реалізацією вихідної загрози. За остаточну оцінку збитків в разі реалізації відповідної загрози можна взяти найбільшу з часткових оцінок, отриманих за кожним з сценаріїв, або збитки за найбільш ймовірним сценарієм, або, нарешті, середньозважений інтегрований збиток, де вагами являються ймовірності реалізацій кожного з сценаріїв.

Іншу технологію зменшення кількості аналізуємих та співставляємих експертом пар <актив-загроза> запропоновано в [4]. Однак наведена робота не містить детального опису механізмів реалізації самої технології. Тому нижче представлено приклад адаптації цієї технології до випадку аналізу рівня втрат, обумовлених реалізацією загрози витоку секретної інформації. Побудова цього прикладу певною мірою спирається на дані, наведені в [5], однак теоретико-методичною базою є сучасна теорія вимірювань [6, 7], застосування якої до задач класифікації інформації за рівнем її важливості розглянуто в [8].

Можливість застосування сучасної теорії вимірювань до задач оцінювання рівня втрат, обумовлених витоком секретної інформації, спирається на застосування двох базових методів прикладного аналізу інформації: методу парних порівнянь та ноніусного підходу до визначення цінності інформації.

Класичний метод парних порівнянь дозволяє розташувати елементи, що складають певну множину, у порядку збільшення або зменшення ознаки, спільної для всіх елементів даної множини [9]. Відома також методика, коли подібна класифікація (ранжування) відбувається за кількома ознаками (комплексом або вектором ознак), – метод аналітичної ієрархії [10]. На жаль, парні порівняння добре працюють за умов, коли кількість елементів множини, що аналізується, незначна. Із збільшенням обсягу цієї множини трудомісткість та складність застосування методу парних порівнянь різко зростає, що, як це вже зазначалося вище, робить його непридатним для практичного використання. Виходом в цьому випадку може бути своєрідний гіпертекстовий варіант порівняльного аналізу, в якому вихідна сукупність елементів поділяється на певні підмножини, що утворюють так звану ноніусну лінійку шкал. Кожна з цих шкал, починаючи з другої, є допоміжною для шкального фрагменту вищого рівня, яка деталізує, уточнює інформацію щодо окремих елементів шкали вищого рівня.

Наприклад, груба шкала (найвищого – першого рівня) утворюється четвіркою інформаційних блоків, що містять інформацію в сферах:

1) оборони;

2) економіки, науки, техніки;

3) зовнішніх відносин;

4) державної безпеки та охорони правопорядку.

Кожен з перелічених блоків грубої номінативної шкали може бути представлений більш деталізовано підмножиною конкретизуючих його зміст допоміжних інформаційних елементів, наприклад:

3.1) загальні відомості про дипломатичні відносини з іншими державами;

3.2) відомості про домовленості у сфері військово-технічного співробітництва з іноземними державами;

3.3) ... .

Ці інформаційні елементи припускають ранжування за рівнем втрат, обумовлених витоком відповідної інформації, тобто утворюють ноніусну ранжовану шкалу другого рівня. При необхідності можлива конкретизація окремих (чи всіх) елементів цієї шкали введенням додаткових множин деталізуючих інформаційних елементів. Приміром, за п. 3.2) можемо отримати:

3.2.1) інформація про міжнародні угоди в галузі розробки озброєнь та військової техніки;

3.2.2) інформація про міжнародні контракти в сфері постачання озброєнь та військової техніки;

3.2.3) ... .

Додатково введені інформаційні елементи після їх ранжування за рівнем можливих втрат внаслідок витоку відповідної інформації, утворюють ноніусну ранжовану шкалу третього рівня. Продовжуючи процедуру деталізації (якщо це є доцільним) інформаційних елементів шкали другого рівня, отримаємо ноніусні ранжовані шкали ще більш високих рівнів. В певній мірі прикладом подібного ноніусного підходу до класифікації інформації є структура представлення інформації в "Зводі відомостей, що становлять державну таємницю".

Впорядкована таким чином множина інформаційних елементів утворює систему рангових шкал, до якої експерт в змозі “вмонтувати” будь-який новий елемент, що підлягає оцінюванню на предмет визначення рівня можливих втрат через розголошення змісту даного елементу.

Для цього експерт визначає на ноніусній лінійці шкалу, найближчу за змістом та рівнем деталізації до об’єкту оцінювання та виконує низку парних порівнянь об’єкту з вузлами (елементами) обраної шкали. Місце, яке зайняв об’єкт оцінювання в системі рангових шкал, можна надалі сприймати як новий вузол шкали, що в подальшому буде використаний у процедурі наступних парних порівнянь при оцінюванні нових інформаційних елементів.

Однак для визначення приналежності оцінюваної інформації до секретної необхідним є отримання кількісних оцінок можливих втрат, обумовлених розголошенням цієї інформації, які в порядковій (ранжованій) шкалі обрахувати немає змоги. Тому слід виконати метризацію ноніусної системи шкал, присвоївши її вузлам-елементам кількісні оцінки рівнів втрат.

Для цього розглядається все, що має певну цінність (іміджеву, економічну, політичну тощо) і у той чи інший спосіб може бути асоційоване з відповідним інформаційним елементом. В ДСТУ ISO/IEC 13335 це "все" визначається терміном “активи”, пов’язані з інформаційним елементом, а збитки, обумовлені витоком інформації, виступають в якості кількісної оцінки рівня цінності цих активів. В [5] перелік деяких активів (у дуже скороченому обсязі) наведено у Додатку А, де їх цінність визначається терміном „питома вага” об’єкту тієї чи іншої сфери діяльності (оборони, економіки, державної безпеки тощо). Очевидно, що ефективне застосування подібної методики оцінювання втрат можливе лише за умов існування дуже докладних переліків активів у кожній сфері діяльності, пов’язаної з

використанням секретної інформації, зокрема, при складанні таких переліків до кожної шкали ноніусної лінійки шкал.

Крім того, слід мати на увазі, що втрати інформації лише за змістом одного інформаційного елемента можуть обумовити збитки щодо різних активів, тобто слід аналізувати та розглядати різні варіанти подій, поштовхом до яких стала втрата відповідної інформації.

Висновки

В статті розглянуто процедуру експертно-аналітичної оцінки активів інформаційної системи відповідно до рекомендацій стандарту ISO/IEC TR 13335-3. Показано, що у випадку оцінювання активів достатньо складної та великої за обсягом структури ця процедура стає надмірно громіздкою та трудомісткою, що фактично виключає можливість її практичного застосування.

Запропоновано та розглянуто механізми спрощення процедури оцінювання активів, зокрема через визначення інтегрованих експертних оцінок збитків для груп активів, асоційованих з окремими сценаріями реалізації загроз інформації, та за допомогою так званого ноніусного підходу, який дозволяє скоротити до прийнятного рівня обсяг аналітичної роботи експерта.

Література

1. ДСТУ ISO/IEC TR 13335 – 3. Інформаційні технології. Настанови з керування безпекою інформаційних технологій (ІТ). Частина 3. Методи керування захистом ІТ.

2. ISO/IEC 27005, Information Technology – Security techniques – Information security risk management.

3. Архипов О.Є, Касперський І.П. Застосування методології передбачення для оцінювання шкоди, заподіяної витоком секретної інформації // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Вип.2 (15). – К.: 2007. – С.13-19.

4. Архипов А.Е. Технология построения комбинированных измерительных шкал для оценивания значимости информации / Архипов О.Є. // Адаптивные системы автоматического управления. – 2008. – № 13(33). – С.153-158

5. Методичні рекомендації державним експертам з питань таємниць щодо визначення підстав для віднесення відомостей до державної таємниці та ступеня їх секретності // Захист інформації з обмеженим доступом: збірник нормативних документів. – К.: КМУЦА, 1999. – 283 с.

6. Суппес П. Основы теории измерений / Суппес П., Зиннес Дж. // Психологическое измерение. – М.: Мир, 1976. – 220 с.

7. Пфанцагль И. Теория измерений / Пфанцагль И. – М.: Мир, 1976. – 220 с.

8. Архипов О.Є. Теоретико-методичні засади оцінювання шкоди, обумовленої розголошенням секретної інформації // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Київ-2008р, випуск 2(17).- с. 16-23.

9. Толстова Ю.Н. Измерение в социологии / Толстова Ю.Н. – М.: ИНФРА-М, 1998.– 224 с.

10. Саати Т.Л. Принятие решений. Метод анализа иерархий / Саати Т.Л.: пер. с англ. – М.: Радио и связь, 1993. – 320 с.

Надійшла: 28.02.11

Рецензент: д.т.н., проф. Кузнєцов Г.В.