УДК 004.056

АНАЛІЗ І ОЦІНЮВАННЯ РІВНЯ НЕБЕЗПЕКИ ІНСАЙДЕРСЬКИХ ЗАГРОЗ

Д.І. Каленюк[1], О.Є. Архіпов[1]

[1] *Національний технічний університет України «Київський політехнічний інститут»*

Анотація

В роботі представлений метод оцінки ризиків, який є підґрунтям для дослідження інсайдерських загроз.

Ключові слова: інсайдер, інсайдерська загроза, ризик, коефіцієнт мотивації, акцентуація

Вступ

Метою аналізу ризиків, пов'язаних з експлуатацією інформаційних систем (ІС), є оцінка загроз, тобто умов і факторів, які можуть стати причиною порушення цілісності системи, її конфіденційності, а також полегшити несанкціонований доступ до неї і вразливостей – слабких місць в захисті, які роблять можливою реалізацію загрози. При оцінюванні ризиків враховуються багато факторів: цінність ресурсів, значимість загроз, вразливостей, ефективність наявних і запланованих засобів захисту та багато іншого [1]. Існують різні способи вимірювання інформаційних ризиків. На практиці найчастіше застосовують так звані табличні методи знаходження ризиків, що використовують якісні шкали для оцінювання імовірнісних характеристик загроз і ступеня тяжкості наслідків, що наступають в разі реалізації цих загроз. Табличні методи зручні і досить адекватні для завдань, що вирішуються на ранніх стадіях проектування СЗІ, зокрема, на етапі передпроектних досліджень [2]. Однак у міру конкретизації структури СЗІ, деталізації механізмів захисту, засобів та елементів, що реалізують ці механізми, з'являється необхідність у більш точному вимірі ризиків, що вимагає застосування кількісних шкал для оцінювання імовірнісних параметрів загроз і вразливостей ІС, визначення збитку, зокрема, вартості втрат, зумовлених успішною реалізацією загроз. Але майже завжди забувають про оцінку вмотивованості конкретної особи, яка потенційно може використати певну вразливість системи для завдання їй шкоди. Це досить важливий аспект і тому виникає необхідність категорювати порушників за чіткою схемою.

1. Мотиваційно-вартісна модель дій атакуючої сторони та оцінка коєфіцієнта мотивації

Розглянемо ситуацію, що виникає при реалізації атакуючою стороною (зловмисниками) загрози T щодо деякого інформаційного ресурсу I. Вважаємо, що D – загальна вартість витрат атакуючої сторони на реалізацію загрози , g – отриманий при цьому «виграш», який визначається цінністю ресурсу I для зловмисників. Загальновживане математичне співвідношення, за яким обчислюються ризик, обумовлений можливою реалізацією загрози , має вигляд:

$$r_T = P_T q = P_t P_V q \tag{1}$$

де P_T – ймовірність реалізації загрози , q – збитки, що виникають за умов реалізації загрози , P_t – ймовірність виникнення (активації) загрози , P_V – ймовірність вдалого використання зловмисником вразливостей інформаційної системи, що призводить до реалізації загрози . Тобто обчислення ризику потребує знання двох(P_T, q) або трьох (P_t, P_V, q)параметрів ризику r_T, які звичайно визначаються експертним шляхом , що може вельми суттєво погіршити якість оцінок ризиків, а відтак – абсолютно непрогнозовано вплинути на кінцеві результати менеджменту ризиків. Чистий прибуток зловмисника в разі успішної реалізації загрози складає:

$$Q = g - D \tag{2}$$

Якщо цінність ресурсу I для атакуючої сторони А значна, інтенсивність потоку спроб доступу зловмисника до ресурсу I буде дуже високою. Зокрема, якщо $g \gg D$, можна припустити, що ймовірність P_t активації (виникнення) загрози буде практично дорівнювати 1, тобто зловмисник спробує використати будь-які шанси для реалізації цієї загрози. Навпаки, для малих значень g економічні мотиви виникнення загрози практично відсутні: при $Q = 0$ (або ж $g = D$) атака ресурсу I стає недоцільною, в цьому випадку $P_t = 0$. Для $g < D$ спроба реалізації загрози втрачає будь-який економічний сенс. Виходячи з цих міркувань, для оцінювання значень ймовірності активації (виникнення) загрози запропоновано співвідношення:

$$P_t = \frac{Q}{g} = 1 - \frac{D}{g} \tag{3}$$

Однак в виразі (2) ніяк не враховується рівень індивідуальних мотиваційних характеристик зловмисника. Тому більш гнучким є варіант оцінювання

ймовірності P_t за формулою (4):

$$P_t = \frac{\gamma g - D}{\gamma g} = 1 - \frac{D}{\gamma g} \quad (4)$$

де введено коефіцієнт мотивації γ , що відображає ступінь впливу величини «виграшу» g на дії сторони А з активації загрози . Залежно від індивідуальних властивостей зловмисника коефіцієнт мотивації γ може бути як більше 1 (атакуючій стороні А властивий азарт, авантюризм, впевненість у своєму успіху), так і менший за 1 (зловмисник обережний, не гарячкує, воліє «мати синицю в руці, ніж журавля в небі»). Враховуючи, що значення ймовірності обмежуються діапазоном $[0; 1]$, на область існування значень коефіцієнта мотивації γ накладається умова:

$$\gamma \geq (\frac{D}{g})$$

Особливістю наведених вище формул є те, що вони отримані для гіпотетичного зловмисника, який діє за принципом виключно економічної доцільності. Ситуацію, коли при великій економічній вигоді людина забажає перейти закон можна проаналізувати за допомогою акцентуації характеру [4].

2. Типи акцентуації

Акцентуації характеру – це крайні варіанти норми, при яких окремі риси характеру надмірно посилені, унаслідок чого виявляється виборча уразливість відносно певного роду психогенних впливів при добрій і навіть підвищеній стійкості до інших. Акцентуація характеру дає можливість розділити зловмисників за типами, так як кожна людина має свої індивідуальні властивості. За характеристикою типу і його особливостями нормується коефіцієнт мотивації. На думку Личко, акцентуації особистості насамперед проявляються у спілкуванні з іншими людьми. Тому, оцінюючи стилі спілкування, можна виділити певні типи акцентуацій. У класифікації, запропонованій Личко, поділ йде на 10 типів з такими визначеними мінімальними діагностичними числами (МДЧ):

- гіпертимний — 10;
- циклоїдний — 8;
- лабільний тип — 9;
- астено-невротичний тип — 8;
- сенситивний тип — 8;
- тривожно-педантичний — 9;
- інтровертований тип — 9;
- збудливий — 9;
- демонстративний тип — 9;
- нестійкий тип — 10;
- контрольна шкала — 4.

Показник за контрольною шкалою, що становить 4 бали, розглядається як критичний. Високий показник свідчить про тенденцію обстежуваних давати «хороші» відповіді. Високі бали за цією шкалою можуть служити свідченням демонстративності в поведінці обстежуваного. Тому при отриманні більше 4 балів слід додати до шкали демонстративності 1 бал. Якщо показник за шкалою брехні перевищує 7 балів, то до шкали демонстративності додаються 2 бали. Якщо при цьому демонстративний тип не діагностується, то результати тестування слід визнати недостовірними. Наприклад, розглянемо гіпертимний тип акцентуації. Основна риса цього типу – постійне перебування в доброму настрої, яке лише зрідка затьмарюється спалахами агресії у відповідь на протидію оточуючих. Цьому типу характерна контактність, говіркість, жвава жестикуляція. Гіпертимам властива жадоба діяльності, спілкування, вражень і розваг. Вони часто проявляють тенденцію до лідерства, що підкріплюється наявністю лідерських здібностей. Досить ініціативні й оптимістичні. У конфліктні стосунки вступають лише в умовах жорсткої дисципліни, монотонної діяльності, вимушеної самотності. Вони є потенційними інсайдерами с досить високим коефіцієнтом мотивації γ . Напротивагу їм розберемо нестійкий тип. Основна риса представників цього типу — патологічна слабкість волі. їхнє безвілля, перш за все, проявляється тоді, коли справа стосується навчання, праці, виконання обов'язків, досягнення мети, яку ставлять перед ними рідні, старші, суспільство. Окрім безвілля, відмічаються підвищена навіюваність нестійких особистостей, їхня не цілеспрямована кримінальність. Психічна нестійкість стає підгрунтям, на якому формуються різні варіанти невротичних розладів, алкоголізм, наркоманія. Такі люди не вміють досягати поставленої цілі, боягузливі та слабкі духом, тому цілком очевидно, що їх коефіцієнтом мотивації γ буде значно нижчим. Було проведено тестування випадкових людей на їх тип акцентуації. У переважній більшості випадків діагностується змішаний тип. Частина даних по тестуванню наведена в таблиці 1.

Тому для підрахунку коефіцієнта мотивації γ запропоновано використовувати таку функцію.

$$\gamma = f(t) =$$
$$= (\delta t/\delta_{min} + (\delta_1/\delta_{1min} + \delta_2/\delta_{2min} + ... + \delta_n/\delta_{nmin})/n)/2$$

t=1,2... , δt < D, де δ - коефіцієнт основного типу акцентуації, δ_1,δ_2...δ_n – коефіцієнти додаткових n типів, які перевишили МДЧ, δ_{min} – мінімальне діагностичне число основного типу акцентуації, δ_{1min},δ_{2min}...δ_{nmin} – МДЧ додаткових n типів. Даний підхід дає можливість побудувати мотивоційно-вартісну оцінку зловмисника. Для конкретизації даної моделі було введено додатковий параметр інсайдера, що деталізує його як можливого порушника та вказує на втрати при реалізації загроз конкретним типом. При створенні моделі порушника та оцінці ризику втрат від дій персоналу необхідно диференціювати всіх співробітників по їх можливостях доступу до системи а, отже, по потенційному збитку від кожної категорії користувачів. Наприклад, оператор або програміст автоматизованої банківської системи може завдати незрівнянно більший збиток, ніж звичайний користувач, тим більше непрофесіонал [6].

Висновки

У даній статті розглядається методика оцінювання рівня небезпеки інсайдерських загроз, обумовленого

Табл. 1. Тестування випадкових людей

Тип акцентуації	Г	Ц	Л	А	С	Т	І	З	Д	Н	К	Сер. значення
	13	7	7	1	6	3	3	7	8	4	6	5,91
	6	6	7	5	6	5	4	6	11	4	3	5,73
	11	5	5	3	5	8	2	5	8	5	4	5,55
	6	10	10	5	8	11	3	6	6	6	6	7,00
	6	11	9	4	6	4	5	4	6	3	5	5,73
	7	11	10	5	8	9	9	9	8	4	8	8,00
	10	7	11	4	6	6	7	6	7	2	2	6,18
	11	6	5	2	6	7	6	3	7	9	10	6,55
	11	2	4	1	3	5	5	2	8	7	6	4,91
	13	4	4	1	5	2	3	2	8	6	7	5,00
	11	8	8	7	7	8	8	5	9	4	3	7,09
	11	6	6	6	6	4	7	3	8	4	4	5,91
	12	5	3	2	4	6	4	3	8	7	5	5,36
	5	8	8	8	4	7	6	4	5	9	3	6,09
	9	7	11	4	8	12	3	7	5	6	5	7,00
	9	11	8	7	8	8	12	9	6	7	2	7,91
	11	9	8	4	5	4	6	6	6	11	2	6,55
	13	4	8	6	7	7	2	9	9	8	6	7,18
Сер. значення	9,70	6,70	7,00	4,00	5,87	6,17	5,43	5,17	7,35	5,57	4,74	

можливою реалізацією вразливості ІС. Представлено шкалювання за типом акцентуації атакуючої сторони(зловмисника). Дана методика конкретизує зловмисника і дає можливість оцінити його мотивацію для реалізації певної атаки на ІС. Слід розуміти, що абсолютно точних результатів типізації можливого зловмисника отримати майже неможливо, але дуже близькі до істини – цілком реально. Тому при організації захисту інформаційної системи слід враховувати наступні обставини: ймовірність реалізації даного типу загрози і потенційний збиток, нанесений користувачам і власникам ACOI в тому випадку, якщо загроза здійсниться (що включає також витрати на захист від неї) та обов'язково коефіцієнт мотивації атакуючої сторони. Заходи, що вживаються повинні бути адекватні імовірності здійснення і ступеня загрози, тобто забезпечувати оптимальний захист від неї. Цей момент є основоположним при організації будь-якого захисту: конкретні заходи повинні визначатися в процесі аналізу впливів на систему. Тому, тільки комплексний аналіз загроз, ступеня захищеності сторони ACOI та та атакуючої сторони може забезпечити вам відносну безпеку.

Перелік використаних джерел

1. Петренко С.А., Симонов С.В. Управление информационными рисками. Экономически оправданная безопасность.М.: Компания Ай Ти; ДМК Пресс, — 2004. — 348 с.
2. Симонов С.В. Методология анализа рисков в информационных системах — 2001. — 48-53 с.
3. Петренко С.А., Петренко А.А Аудит безопасности Intranet. –М.: ДМК Пресс — 2002. — 416 с.
4. Карл Леонгард — Акцентуированные личности 1976. — 328 с.
5. Личко А. Е. — Психопатии и акцентуации характера у подростков 2009. — 256 с.
6. Гайкович В., Першин А. Безопасность электронных банковских системЪ — 1993.