УДК 004.056

ВИЗНАЧЕННЯ УМОВИ НЕЕФЕКТИВНОСТІ ПРОДАЖУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

В.З.ТАБАКОВ, кандидат технічних наук

Інститут підготовки кадрів державної служби зайнятості України

Обгрунтовано актуальність урахування людського чинника при моделюванні систем захисту інформації в автоматизованих системах. Побудовано математичну модель для дослідження процесів його впливу на витік конфіденційної інформації. Визначено умову, що виключає формування мотиву продажу конфіденційної інформації секретоносієм.

Ключові слова: людський чинник, захист інформації, конфіденційна інформація.

Проблемна ситуація пов'язана з аналізом ризику просочування конфіденційної інформації до галузевих конкурентів [1]. Такий витік може призвести до значних збитків як в бізнесі, так і в політиці, а недбайливий або недобросовісний менеджер здатен перетворити контрольований ним чинник на ресурс суперника.

Сучасні системи захисту інформації в автоматизованих системах конфіденційного діловодства на базі ПЕОМ, як правило, засновані на шифруванні і застосуванні електронних ідентифікаторів. Основним напрямом нейтралізації прихованих загроз і атак, пов'язаних з неправомірними діями санкціонованих користувачів автоматизованих систем – осіб, які мають доступ на територію контрольованої зони і до інформації, що захищається, є розробка і впровадження спеціальних програмно-апаратних комплексів її захисту [2].

Проте основною причиною витікання конфіденційної інформації залишається людський чинник, урахування якого вимагає розв’язання таких задач: дослідження мотивів, що штовхають людей на порушення

корпоративних угод і правопорушення; розробка механізмів управління секретоносіями, способів інформаційного впливу на санкціонованих користувачів автоматизованих систем та ін.

Метою дослідження є забезпечення ефективного розв'язання цих задач шляхом створення математичної моделі витікання конфіденційної інформації з урахуванням людського чинника та визначення умови, що виключає формування мотиву продажу конфіденційної інформації секретоносієм.

Матеріал та методика. Об'єктом дослідження слугували підприємства, організації та установи, що володіють інформацією, якій надано статус конфіденційності. Методикою дослідження є декомпозиція конфіденційної інформації на блоки за рівнями підлеглості секретоносіїв з наступним визначенням вартості і продажної ціни відповідного блоку конфіденційної інформації та виведенням умови неефективності продажу конфіденційної інформації.

Результатом дослідження є математичний вираз, що дозволяє визначити умову, за якою продаж конфіденційної інформації секретоносіями підприємств, організацій та установ є економічно недоцільним.

Розглянемо модель проблемної ситуації. Позначимо через i номер оператора-секретоносія, $i = \overline{1, N}$, де N - загальне число операторів; q_i - об'єм блоку конфіденційної інформації, що знаходиться в користуванні i-го оператора; Q - повний об'єм конфіденційної інформації $Q = \sum_{i=1}^{N} q_i$; $C(q_i)$ - вартість блоку q_i, що складається з вартості його розробки, впровадження і експлуатації, $k(q_i)C(q_i)$ - «продажна ціна» блоку q_i для конкурента, де $k(q_i)$ - коефіцієнт корисності блоку q_i для конкурента, $k(q_i) > 0$.

Фрагмент q_i конфіденційної інформації тим цінніший для конкурента, чим докладніше він інформує про її повний об'єм Q. Чим більший об'єм фрагмента q_i, тим вищий коефіцієнт його корисності для конкурента $k(q_i)$ і його ціна $k(q_i)C(q_i)$. Передбачається, що $k(q_i)$ монотонно зростає із збільшенням q_i, причому $k(q_i) = 1$, якщо $q_i = Q$. Тому $0 < k(q_i) \leq 1$. Типова

залежність $k(q_i)$ показана на *рис1*.

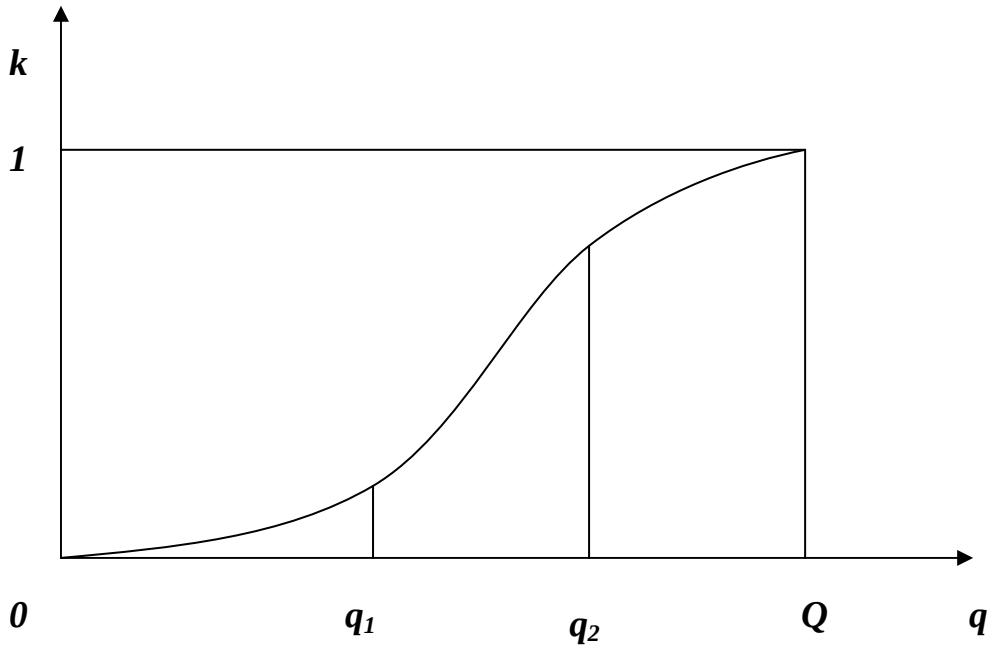

Рис. 1. Графік залежності коефіцієнта корисності інформації $\mathbf{k(q_i)}$ від її об'єму $\mathbf{q_i}$

Приріст коефіцієнта корисності інформації для конкурента на ділянці від 0 до q_1 незначний, оскільки після неї практично неможливо відновити необхідні відомості в повному об'ємі. На ділянці від q_2 до Q, приріст корисності інформації також невеликий, тому що різко зростає вірогідність відновлення потрібних відомостей за вже придбаною інформацією.

У моделі виділимо п'ять класів порушників. Порушники першого класу не мають доступу в контрольовану зону. Їх пряму дію на елементи автоматизованої системи, що захищаються, виключено, але можливий зйом інформації по каналах ПЕОМ. Порушники з другого до п’ятого класу мають доступ у зону. Для порушників вищого класу характерні великі можливості доступу до ресурсів автоматизованої системи, починаючи від відсутності прямого фізичного доступу до АРМ і закінчуючи необмеженими можливостями управління автоматизованою системою в особі адміністратора.

Таким чином, система доступу до конфіденційної інформації має ієрархічну структуру. Оператор, який стоїть на нижньому рівні ієрархії доступу до конфіденційної інформації, контролює певний її фрагмент. Керівники підрозділів контролюють інформацію своїх підлеглих. Так, керівник ***j****-го* підрозділу контролює об'єм інформації, що дорівнює сумі об'ємів фрагментів, контрольованих його підлеглими: $m_j = \sum_{i=1}^{M_j} q_i$, де M_j - кількість операторів в ***j***-му підрозділі, $1 < j \le K$, K - кількість підрозділів $\sum_{j=1}^{K} M_j = N$.

Отже, вартість фрагмента інформації ***m***, контрольованого керівником ***j****-го* підрозділу, дорівнює $C(m_j)$, а його «продажна ціна» - $k(m_j)C(m_j)$. Вартість конфіденційної інформації ***Q***, контрольованої адміністратором автоматизованої системи, збігається з її «продажною ціною», оскільки $k(Q)=1$.

Часто оператор продає інформацію нижче за її вартість, особливо якщо не знає останньої. Покупець інформації обізнаніший про неї і пропонує ціну ***X***. Прибуток $V(q_i,X)$ продавця конфіденційної інформації, в ролі якого виступає ***i***-й оператор, можна оцінити так:

$$V(q_i,X)=X - p_{1i}(nD(q_i)+lB(q_i)) - p_{2i} R(q_i), \quad (1)$$

де p_{1i} - вірогідність викриття продавця; n - кількість місяців, які б пропрацював на фірмі продавець без правопорушення; $D(q_i)$ - місячний оклад; l - кількість премій; $B(q_i)$ - розмір премій; p_{2i} - вірогідність збитку в разі викриття; $R(q_i)$ - розміри морального і матеріального збитку, виражені в грошах. Вираз (1) можна ускладнити, наприклад, враховуючи втрату викритим продавцем страховки, різниці в окладах після звільнення і переходу на менш оплачувану роботу. Проте ці уточнення в принципі не ускладнюють завдання.

Прибуток покупця $p_i(q_i,X)$ можна оцінити таким чином:

$$p_i(q_i,X)=k(q_i)C(q_i)-X-S(q_i)- p_{3i}U(q_i),$$

$$X<k(q_i)C(q_i), \quad (2)$$

де $S(q_i)$ - засоби, витрачені на вербування продавця; p_{3i} - вірогідність

викриття покупця; $U(q_i)$ - матеріальні і моральні втрати внаслідок викриття, виражені в грошовій формі.

З (1) витікає, що для продавця прийнятна ціна за товар, що задовольняє вимозі:

$$X > p_{1i}(nD(q_i)+lB(q_i)) + p_{2i}R(q_i). \quad (3)$$

З (2) витікає, що для покупця прийнятна ціна за товар, що задовольняє вимозі:

$$X \le k(q_i)C(q_i)-S(q_i)-p_{3i}U(q_i). \quad (4)$$

З (3) і (4) витікає, що для покупця прийнятна ціна за товар, що знаходиться в сегменті компромісу

$$[p_{1i}(nD(q_i)+lB(q_i)) + p_{2i}R(q_i),\ k(q_i)C(q_i)-S(q_i)-p_{3i}U(q_i)] \quad (5)$$

Для операції необхідно, щоб сегмент компромісу (5) не був порожнім

$$p_{1i}(nD(q_i)+lB(q_i)) + p_{2i}R(q_i) \le k(q_i)C(q_i)-S(q_i)-p_{3i}U(q_i).$$

Висновок. Щоб виключити продаж конфіденційної інформації, досить виконати умову:

$$p_{1i}(nD(q_i)+lB(q_i)) + p_{2i}R(q_i) > k(q_i)C(q_i)-S(q_i)-p_{3i}U(q_i)$$

Якщо продавцем конфіденційної інформації є керівник j-*го* підрозділу, то i і q_i слід замінити, відповідно на j і m_j. Якщо ж секретами автоматизованої системи торгує адміністратор, то q слід замінити на Q.

СПИСОК ЛІТЕРАТУРИ

1. Бухарин С.Н. Человеческий фактор в проблеме защиты информации от несанкционированного доступа в автоматизированных системах конфиденциального делопроизводства/С.Н.Бухарин, А.А. Кулемин// Стратегическая стабильность. – 2006. – №4. – С. 120 – 144.

2. Бухарин С.Н. Информационное противоборство. Книга 2. Теоретические основы/С.Н.Бухарин, А.Г. Глушков, И.Д. Ермолаев. М.: Полиори, 2005. – 325 с.

3. Домарев В.В. Безопасность информационных технологий.

Системный подход. – К.: ООО ТИД ДиаСофт, 2004. – 992 с.

4. НД ТЗІ 2.1-001-2001 Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення// Затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 9 лютого 2001 р. № 2

5. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі// Затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28 квітня 1999 р. № 22.

Определение условия неэффективности продажи конфиденциальной информации

В.З.Табаков

Обоснована актуальность учета человеческого фактора при моделировании систем защиты информации в автоматизированных системах. Построена математическая модель для исследования процессов влияния человеческого фактора на утечку конфиденциальной информации. Определено условие, исключающее формирование мотива продажи конфиденциальной информации у секретоносителей.

Ключевые слова: человеческий фактор, защита информации, конфиденциальная информация

Determining the condition of inefficiency selling confidential information

V.Z.Tabakov

The urgency of the human factor in the modeling of systems of information protection in automated systems is grounded. A mathematical model for studying the influence of human factor on the confidential information leakage is builded. The

condition that precluding of formation of a motive for the sale of confidential information is obtained.

Keywords: human factor, information security, confidential information