УДК 004.056.53:621.39

В.І. ЗАБОЛОТНИЙ, канд. техн. наук, А.В. ЄРМОЛОВИЧ

ДОЦІЛЬНИЙ РОЗПОДІЛ ВИТРАТ НА ВПРОВАДЖЕННЯ ЗАХОДІВ ЗАХИСТУ ВІД ТЕХНІЧНИХ ЗАСОБІВ РОЗВІДКИ

Вступ

Матеріальне виробництво сучасної продукції, розробка новітніх технологій виготовлення споживчих товарів, надання різноманітних послуг потребує захисту від конкурентів, у тому числі і від технічних засобів конкурентних розвідок. Інформацію, що озвучується і, або обробляється технічними засобами, та відомості, які проявляються власне самою продукцією або технологіями її виготовлення, конкуренти спроможні виявляти за рахунок використання різних способів, у тому числі і за допомогою застосування засобів технічних розвідок (ЗТР).

Відомо два шляхи добування даних конкурентами за допомогою ЗТР.

По-перше, це добування інформації про об'єкти розвідки, яка існує у знаковій формі [1]. Знакову форму існування інформації про об'єкти можна віднести до віртуального світу існування продуктів праці. Знакова форма представляє сукупність символів, літер, цифр, звуків, які відображають предмети та явища реального світу у віртуальному світі. Носіями інформації з обмеженим доступом (ІзОД) є документи на папері, магнітна, кіно-, відео-, фотоплівка, інші носії. Також ІзОД може зберігатися, відображатися або передаватися у формі фізичних полів (електромагнітних, оптичних, акустичних), електричних сигналів, вібрацій (у твердих предметах), тобто у вигляді інформаційних сигналів, які є об'єктом діяльності ЗТР.

По-друге, конкуренти можуть спостерігати власне за самими матеріальними об'єктами розвідки. Форма існування відомостей про об'єкти захисту проявляється самими матеріальними об'єктами реального світу у процесі виробництва й застосування продукції, технологій різного призначення теж у вигляді електромагнітних, оптичних, гравітаційних, акустичних та інших полів й випромінювання, хімічних речовин [1]. Розвідка цих ефектів за допомогою ЗТР дозволяє конкурентам синтезувати дані щодо відомостей з обмеженим доступом (ВзОД), які захищають від конкурентів.

В обох випадках виникає потреба проводити заходи захисту від ЗТР. Одним із напрямів захисту інформації, яка виражається у знаковій формі, є технічний захист інформації (ТЗІ). Захист ІзОД від витоку є важливою задачею, і на її рішення потрібні певні витрати.

Напрям захисту ВзОД, що проявляються самими об'єктами матеріального світу, також потребує певних витрат, наприклад, на маскування, приховування певних характеристик, технічну дезінформацію тощо – тобто на захист від технічних розвідок (ЗвТР).

Комплексність захисту інформації та відомостей потребує певних витрат. Оптимальний розподіл витрат на ці напрями захисту дозволить, при обмежених загальних витратах, одержати максимальний ефект.

Захист інформаційних ресурсів повинен бути одним із пріоритетних завдань безпеки підприємств України, оскільки перехід до інформаційного суспільства змінив статус інформації. Наразі вона може бути як засобом забезпечення безпеки, так і загрозою та небезпекою.

За умов постіндустріального етапу інформація перетворилась на стратегічний ресурс економічного і науково-технологічного прогресу. Відтак, захист інформації на підприємствах потребує достатнього теоретичного та методологічного підґрунтя. Дослідження можливості застосування математичних методів для оцінювання захисту інформації на підприємстві є досить актуальним питанням за сучасних умов розвитку економіки.

Серйозна увага до питань конкурентного захисту спричиняє проблеми оцінки рівня безпеки інформації на підприємствах та в організаціях, визначення величини грошових коштів,

які потрібно виділити на вирішення проблем інформаційної безпеки, розподілу грошових коштів між напрямами, які забезпечують захист інформації, зниження інформаційних ризиків. Найчастіше зазначені проблеми розв'язують на інтуїтивному рівні, без обґрунтування фінансової доцільності рішень. Адже керівництво підприємств не завжди оцінює важливість цього питання та має інформацію про співвідношення витрат на забезпечення інформаційної безпеки та збитків від втрати інформації. Іноді на інформаційній безпеці економлять, хоч це найчастіше призводить до істотних фінансових і моральних втрат, які можуть бути причиною краху. Однією з проблем інформаційної безпеки підприємства є її кількісна оцінка, а також необхідність обґрунтування вартості створення корпоративної системи захисту інформації.

Якщо рішення завдань в галузі захисту інформації приймають на інтуїтивному рівні, то існує ризик їх неоптимальності, додаткових втрат, у тому числі і економічних. Сучасні вимоги, висунуті до організації режиму інформаційної безпеки, створюють необхідність використання в своїй роботі більшого рівня захисту, а також необхідність оцінити економічну ефективність витрат на інформаційну безпеку. Економічно обґрунтовані комплекси і системи захисту інформації будуються адекватно загрозам її безпеки, що описуються у відповідних моделях.

Витрати на заходи із захисту інформації передбачаються в кошторисах робіт на проектування, будівництво, реконструкцію, розробку, створення, модернізацію, впровадження та експлуатацію об'єктів (систем, зразків, технологій). Витрати на заходи із захисту інформації здійснюються за рахунок суб'єктів, які провадять таку діяльність.

Надалі сформульовано математичну постановку і запропоновано рішення задачі, обґрунтування таких затрат на захист інформації на підприємстві, що забезпечують максимальний прибуток загальної діяльності.

Мета роботи - визначення розподілу витрат між ТЗІ і ЗвТР на забезпечення заданого рівня безпеки підприємства методом математичного моделювання.

Постановка задачі

Постановка задачі на оптимальний розподіл витрат z на захист від технічних розвідок (ЗвТР) – x і на технічний захист інформації (ТЗІ) – y.

Введені позначення:

$P_x(x)$ – ймовірність успішного ЗвТР при витратах x;

$P_y(y)$ – ймовірність успішного ТЗІ при витратах y;

$z=x+y$ – сумарні витрати на рішення задач обох задач захисту;

$P_{xy}(z=x+y)=P_x(x)P_y(y)$ – ймовірність успішного одночасного рішення задач ЗвТР та ТЗІ при витратах $z=x+y$, обумовлене незалежністю рішення задач ЗвТР та ТЗІ

$P_x(x)$, $P_y(y)$, $P_{xy}(z)$ – обмежені від 0 до 1;

$P_x(x)$, $P_y(y)$, $P_{xy}(z)$ – функції, які не зменшуються з ростом відповідного аргументу, тобто їх похідні завжди позитивні.

Задача дослідження: мінімізувати витрати $z=x+y$ при заданій ймовірності успішного одночасного рішення задач ЗвТР та ТЗІ $P_z(z=x+y)$ при їх оптимальному розподілі між ЗвТР та ТЗІ:

$$P_{xy}(z = x + y) = P_x(x)\,P_y(y). \quad (1)$$

Рішення задачі

Знайти таке співвідношення витрат x і y при заданому $P_z(z)$, що дає мінімум величини $z= x + y$, можна аналітичним пошуком екстремуму.

Перехід до однієї величини $y=z - x$ дає змогу записати (1) як

$$P_{x,y}(z) = P_x(x)P_y(z - x). \quad (2)$$

Тоді для визначення екстремуму z при фіксованій величині $P_{x,y}(z)$ по значенню x потрібно знайти похідну $P_{xy}(z)$ по x і прирівняти її 0. Рішення відносно x дасть можливість знайти $y=z-x$.

Отже,

$$P'_{x,y}(z) = (P_x(x)P_y(z-x))' = P'_x(x)P_y(z-x) - P_x(x)P'_y(z-x) \quad (3)$$

З останнього, після порівняння з 0 можна записати

$$P'_x(x)P_y(z-x) = P_x(x)P'_y(z-x), \quad (4)$$

або після перетворення:

$$P'_x(x)/P_x(x) = P'_y(z-x)/P_y(z-x)\ . \quad (5)$$

З врахуванням суті похідних від $Px(x)$, $Py(y)$:

$$w_x(x)/P_x(x) = w(z-x)/P_y(z-x) \quad (6)$$

З (6) можна знайти x , y та їх суму для заданого z пару значень x та y.

Для створення моделі необхідно визначити залежності $P_x(x)$ – ймовірність успішного ЗвТР та $P_y(y)$ – ймовірність успішного ТЗІ при витратах відповідно x та y.

Наприклад, для ілюстрації можна скористатися даними, що відображені на рис. 1 та 2.

На рис. 1 зображено ймовірність ЗвТР при витратах у розмірі x. На рис. 2 зображено ймовірність ТЗІ при витратах у розмірі y.

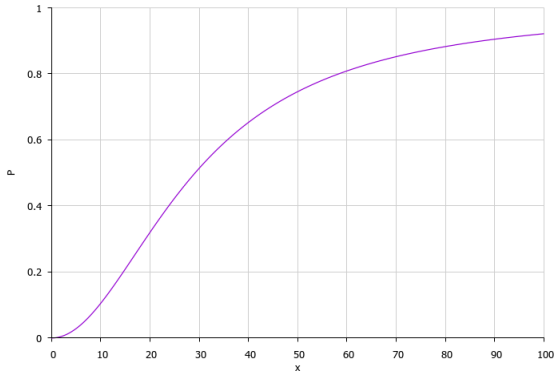

Рис. 1. Ймовірність ЗвТР при витратах x

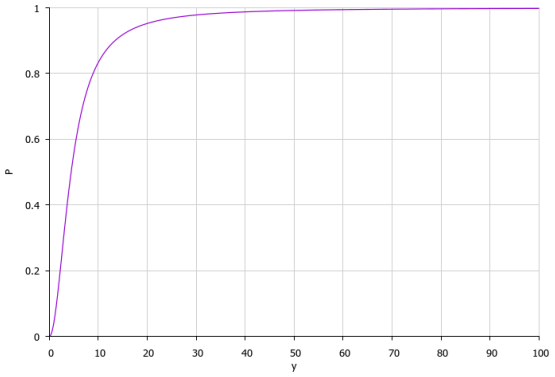

Рис. 2. Ймовірність ТЗІ при витратах y

Захист буде успішний при одночасному рішенні задач ТЗІ та ЗвТР, тобто $P_{xy}(z=x+y)=P_x(x)P_y(y)$.

Ілюстрація залежності розподілу витрат на захист у вигляді 3D-графіку функції $P_{xy}(z=x+y)$ для заданого рівня захисту, наприклад P_{xy} = 0,8, наведена на рис. 3 як перетин площини, P_{xy}=0,8 і поверхні $P_{xy}(z=x+y)$. На рисунку наведено також перетин площиною $x+y= z$, для мінімального значення z.

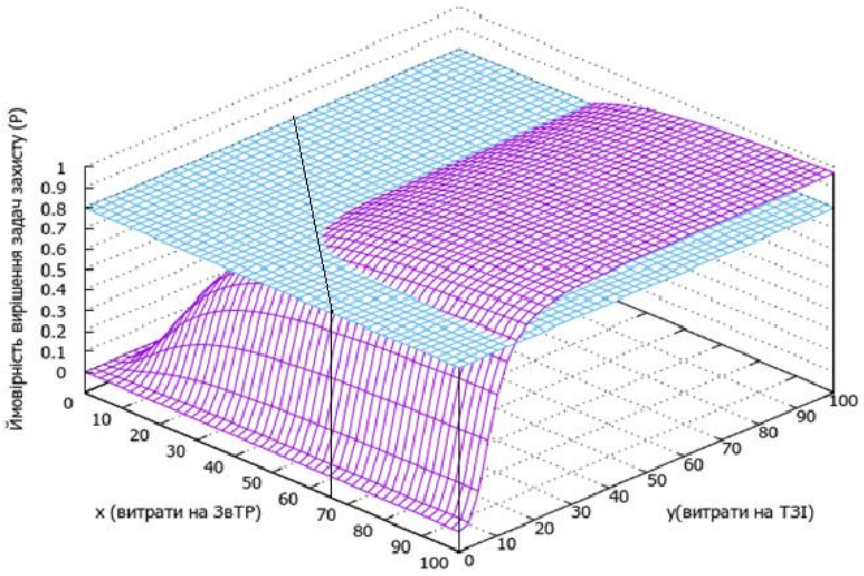

Рис. 3. Модель ймовірності захисту *P(z)* при обмежених загальних витратах *z*

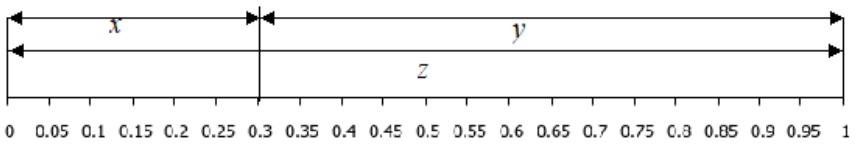

Рис. 4. Співвідношення розподілу витрат на ЗвТР та ТЗІ для наведеного прикладу

На рис. 5 наведено переріз площиною $x+y= z$ поверхні $P_{xy}(z=x+y)$. На проекції відображено розподіл витрат z між заходами ЗвТР та ТЗІ, x та y відповідно. Оптимальний розподіл визначається найбільшою ймовірністю захисту інформації. Слід зазначити, що невеликий градієнт зміни $P_{xy}(z=x+y)$ від співвідношення x та y в області оптимальних рішень дозволяє бути впевненим в надійності забезпечення задач захисту.

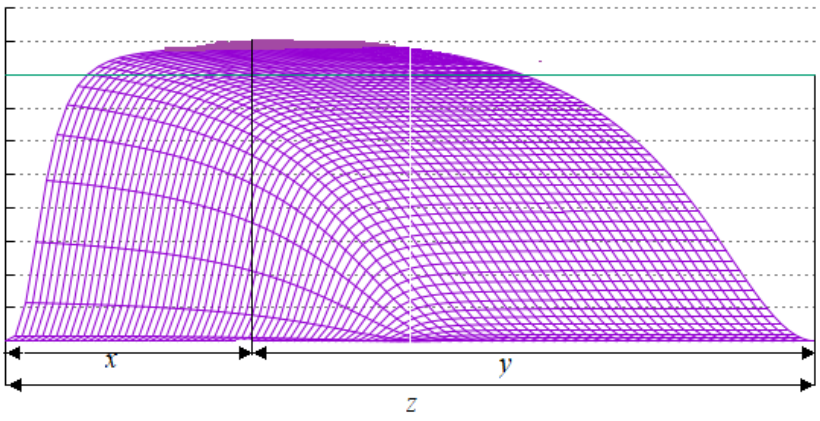

Рис. 5. Розділ витрат *z* між заходами ЗвТР та ТЗІ

Побудована модель відображає ймовірність забезпечення успішного вирішення задач захисту при сталих витратах на ТЗІ та ЗвТР. Аналізуючи схему, доцільно припустити, що лише за умов, наближених до отриманого розподілу витрат на обидва види захисту, можливо забезпечити високу ймовірність вирішення задач захисту. При проведенні розподілу витрат на два напрями є обґрунтування на розподіл коштів на ТЗІ та ЗвТР. Дуже часто ці задачі

захисту здійснюють різні підрозділи підприємства, які зацікавлені у результатах лише своєї роботи. Отже, запропонована модель дає об'єктивні засади на розподіл витрат між двома напрямами захисту таким чином, щоб вони в комплексі забезпечували задану ймовірність успішного вирішення задач захисту.

Висновки

Дослідження показали, що, незважаючи на різноманітність специфіки підприємств, існує єдність у підході до визначення витрат на створення системи захисту інформації.

Оцінка розміру показника захищеності інформації є найважливішою ланкою у виборі того чи іншого заходу. Реалізація запропонованих заходів технічного захисту інформації повинна постійно оцінюватися, як за своєчасністю й повнотою їх виконання, так і за їх ефективністю.

Визначення на основі моделі оптимізації економічно обґрунтованого обсягу коштів, що доцільно виділити на інформаційну безпеку підприємства, спрощує процес прийняття рішень керівництвом підприємства. Рішення задачі оптимального розподілу коштів між окремими напрямами захисту інформації дозволяє підприємству забезпечити мінімально можливий у межах виділеної суми рівень інформаційного ризику та витрат на проведення заходів захисту інформації. Тобто, обрати оптимальний розподіл витрат на заходи захисту, отримуючи максимальну ймовірність успішного захисту при загальних витратах.

Запропонований підхід до постановки задачі захисту інформації має деякі особливості.

По-перше, керівництво підприємства має усвідомлювати наявність існування певного рівня ймовірності захисту інформації.

По-друге, для одержання обґрунтованих рекомендацій щодо необхідних затрат на захист інформації потрібні вихідні дані про рівень захисту інформації.

Результати досліджень доцільно використовувати для визначення оптимального обсягу грошових коштів та його розподілу між окремими напрямами захисту інформації організації

Список літератури:

1. ДСТУ3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.

2. . Заболотний В.І. Варіант оптимізації витрат на систему захисту інформації / В.І. Заболотний, К.В. Петросян // Междунар. радиоелектрон. форум «Прикладная радиоэлектроника. Состояние и перспективы развития». Сб. науч. тр. Харьков, 2008. Т. 5.

3. Заболотний В.І. Обґрунтування вибору заходів захисту характеристик продукції від конкурентної розвідки / В.І. Заболотний, Є.В. Задорожна // Прикладна радіоелектроніка. 2013. Т. 12. №2. С. 351-356.

Харківський національний
університет радіоелектроніки

Надійшла до редколегії 04.03.2018