отриманих експертних оцінок. Кожен експерт повинен дати оцінку ймовірності $p_к$ виникнення загрози для витоку інформації, яка має цінність С/ та захищена за допомогою витрат $C_з$. При цьому повинні бути враховані можливість прагнення нанесення максимальних збитків $C_в$ власнику інформації, а також капіталовкладення супротивника $C_д$ у реалізацію несанкціонованого доступу. Разом з тим, зазначена група експертів повинна на підставі відомостей про існуючу систему захисту інформації та ймовірної наявності у супротивника атакуючої системи, оцінити ймовірність відбиття атаки p_0 (ймовірність відсутності загрози), яка може бути представлена у вигляді функції

$$p_0 = \varphi(p_к, C_з, C_д). \qquad (11)$$

Спектральна ефективність методу передавання /?= Я / F [(біт/с)/Гц] характеризує ефективність використання каналу зв'язку зі смугою і7.

Чистий прибуток від передавання інформації орендованим каналом зі смугою пропускання P визначається з виразу

д = о - 8 = с р - т я - с ґ тр =

= (12)

= Т Р - {с ^ ф - С Р)[грн.]

або, для випадку мовних повідомлень,

0 = Х)-5 = С}1}-2У?- ■Сґ ТР =

= С fТ - F.log; Рс/р3 - С Ґ ТР = (13)

= ТР- О◁К а- р/Р,; Сс [грн.]

Далі необхідно визначити доцільність проведення заходів із захисту інформації. У разі проведення заходів щодо захисту інформації чистий прибуток від передавання інформації знизиться і його можна визначити наступним чином:

а = Д - 5 - С 3- ^ - С г-(1-д) =
о

= С[-]-Т-Я-СҐ ТР - С 3~ -

= С ^ - Т - Р - р - С ґ Т Ґ - С , — - (14)
о

= Г.^(с7>-/?-£>)- с 3- | -

-С$'-ТА-Р-/і-р„{1-р0){грн.]

або, для випадку мовних повідомлень,

а = о - ї - с Л - с г-(і-й) =

= с ^ - т - с г - т р - с т з р

= С?1-r-F.log;
зУ
- СР-ТР - С 3~ m/1(- (15)

/
-С І1-IV F.log, рЛ
v

= ^- Ор-т-с^-тА-рк^ - Р , У ^ 41}
Ґ
ХІ0§2 а Р с л -Т- Ґ Сґ Р--~-\[грн.].
V Р3) О

У виразах (14) і (15) складова -С 3-Т/Т^ характеризує зменшення чистого прибутку через частину загальних витрат на систему захисту інформації та є пропорційною часу експлуатації T захищеного за допомогою цієї системи каналу зв'язку. У випадку разового використання системи захисту у деякій ТКС 7о - Т. Складова -С$-ТА-Ярк-(\-р0) враховує збитки через неідеальність системи захисту при вкладених в неї коштах Сз; при цьому $p_к(1-p_0)$ — це умовна ймовірність того, що загроза не буде відбита. Якщо система захисту є ідеальною (ймовірність відбиття загрози p_0 - 1), то збитки через неідеальність системи захисту відсутні.

Введемо поняття коефіцієнта зниження прибутковості захищеної системи

передавання інформації $K_З$ — формула (16), який для випадку мовних повідомлень може бути обчислений за формулою (17):

$$K_З = \frac{Q_З}{Q} = \frac{T\cdot F\cdot\left(C_I^{\{1\}}\cdot\beta - C_F\right) - C_З\cdot\frac{T}{T_0} - C_B^{\{1\}}\cdot T_A\cdot F\cdot\beta\cdot p_к\cdot(1-p_0)}{T\cdot F\cdot\left(C_I^{\{1\}}\cdot\beta - C_F\right)} = \tag{16}$$

$$= 1 - \frac{C_З\cdot\frac{T}{T_0} + C_B^{\{1\}}\cdot T_A\cdot F\cdot\beta\cdot p_к\cdot(1-p_0)}{T\cdot F\cdot\left(C_I^{\{1\}}\cdot\beta - C_F\right)};$$

$$K_З = \frac{Q_З}{Q} = \frac{C_I^{\{1\}}\cdot T\cdot F\cdot\log_2\left(a\cdot\frac{P_c}{P_З}\right) - C_F\cdot T\cdot F - C_З\cdot\frac{T}{T_0} - C_B^{\{1\}}\cdot T_A\cdot F\cdot\log_2\left(a\cdot\frac{P_c}{P_З}\right)\cdot p_к\cdot(1-p_0)}{T\cdot F\cdot\left[C_I^{\{1\}}\cdot\log_2\left(a\cdot\frac{P_c}{P_З}\right) - C_F\right]} = \tag{17}$$

$$= 1 - \left\{C_З\cdot\frac{T}{T_0} + C_B^{\{1\}}\cdot T_A\cdot F\cdot\log_2\left(a\cdot\frac{P_c}{P_З}\right)\cdot p_к\cdot(1-p_0)\right\}\Bigg/\left\{T\cdot F\cdot\left[C_I^{\{1\}}\cdot\log_2\left(a\cdot\frac{P_c}{P_З}\right) - C_F\right]\right\}.$$

Цей показник дозволяє оцінити наскільки зменшиться прибуток організації після, впровадження заходів щодо захисту інформації. Якщо організація не бажає впроваджувати заходи щодо захисту власної інформації, необхідно оцінити ймовірне зменшення прибутку в разі перехоплення останньої.

Чистий прибуток від передавання інформації у випадку незахищеної системи ($C_З = 0;\ p_0 = 0$) можна визначити як

$$\begin{aligned} Q_H &= D - S - C_B = \\ &= C_I^{\{1\}}\cdot T\cdot R - C_F\cdot T\cdot F - C_B^{\{1\}}\cdot T_A\cdot R\cdot p_к = \\ &= C_I^{\{1\}}\cdot T\cdot F\cdot\beta - C_F\cdot T\cdot F - C_B^{\{1\}}\cdot T_A\cdot F\cdot\beta\cdot p_к = \\ &= T\cdot F\cdot\left(C_I^{\{1\}}\cdot\beta - C_F\right) - C_B^{\{1\}}\cdot T_A\cdot F\cdot\beta\cdot p_к\ [грн.] \end{aligned} \tag{18}$$

або, для випадку мовних повідомлень,

$$\begin{aligned} Q_H &= D - S - C_B = \\ &= C_I^{\{1\}}\cdot T\cdot R - C_F\cdot T\cdot F - C_B^{\{1\}}\cdot T_A\cdot R\cdot p_к = \\ &= C_I^{\{1\}}\cdot T\cdot F\cdot\log_2\left(a\cdot\frac{P_c}{P_З}\right) - C_F\cdot T\cdot F - \\ &\quad - C_B^{\{1\}}\cdot T_A\cdot F\cdot\log_2\left(a\cdot\frac{P_c}{P_З}\right)\cdot p_к = \\ &= T\cdot F\cdot\left[C_I^{\{1\}}\cdot\log_2\left(a\cdot\frac{P_c}{P_З}\right) - C_F\right] - \\ &\quad - C_B^{\{1\}}\cdot T_A\cdot F\cdot\log_2\left(a\cdot\frac{P_c}{P_З}\right)\cdot p_к\ [грн.]. \end{aligned} \tag{19}$$

Тоді коефіцієнт зниження прибутковості незахищеної системи K_H можна представити формулою (20); у випадку мовних повідомлень коефіцієнт K_H може бути обчислений за формулою (21):

$$K_H = \frac{Q_H}{Q} = \frac{T\cdot F\cdot\left(C_I^{\{1\}}\cdot\beta - C_F\cdot\right) - C_B^{\{1\}}\cdot T_A\cdot F\cdot\beta\cdot p_к}{T\cdot F\cdot\left(C_I^{\{1\}}\cdot\beta - C_F\right)} = 1 - \frac{C_B^{\{1\}}\cdot T_A\cdot\beta\cdot p_к}{T\cdot\left(C_I^{\{1\}}\cdot\beta - C_F\right)}; \tag{20}$$

$$K_H = \frac{Q_H}{Q} = \frac{T\cdot F\cdot\left[C_I^{\{1\}}\cdot\log_2\left(a\cdot\frac{P_c}{P_З}\right) - C_F\right] - C_B^{\{1\}}\cdot T_A\cdot F\cdot\log_2\left(a\cdot\frac{P_c}{P_З}\right)\cdot p_к}{T\cdot F\cdot\left[C_I^{\{1\}}\cdot\log_2\left(a\cdot\frac{P_c}{P_З}\right) - C_F\right]} = \tag{21}$$

$$= 1 - C_B^{\{1\}}\cdot T_A\cdot\log_2\left(a\cdot\frac{P_c}{P_З}\right)\cdot p_к\Bigg/\left\{T\cdot\left[C_I^{\{1\}}\cdot\log_2\left(a\cdot\frac{P_c}{P_З}\right) - C_F\right]\right\}.$$

Цілком очевидно, що якщо $K_H > K_З$, то будь-які заходи щодо захисту інформації в системі не мають сенсу. Цю нерівність можна записати таким чином

$$0 < Z = K_H - K_З. \qquad (22)$$

Враховуючи (16) і (20), отримаємо нерівність, при якій виконується умова (22):

$$\frac{C_З \cdot \frac{T}{T_0} - C_B^{\{1\}} \cdot T_A \cdot F \cdot \beta \cdot p_к \cdot p_0}{T \cdot F \cdot \left(C_I^{\{1\}} \cdot \beta - C_F \right)} > 0 \qquad (23)$$

або, для випадку мовних повідомлень, беручи до уваги формули (17) і (21),

$$\frac{C_З \cdot \frac{T}{T_0} - C_B^{\{1\}} \cdot T_A \cdot F \cdot \log_2\left(a \cdot \frac{P_c}{P_З} \right) \cdot p_к \cdot p_0}{T \cdot F \cdot \left(C_I^{\{1\}} \cdot \log_2\left(a \cdot \frac{P_c}{P_З} \right) - C_F \right)} > 0. \qquad (24)$$

Отримані результати дозволяють приймати рішення щодо доцільності проведення заходів по захисту інформації в інформаційно-комунікаційних системах (ІКС). Наприклад, зрозуміло, що якщо ймовірність порушення конфіденційності та цілісності дорівнює нулю ($p_к = 0$) або ж система захисту є цілком неефективною (ймовірність відбиття загрози $p_0 = 0$), то іншого рішення, як $C_З = 0$ не може існувати. У цих випадках витрати на систему захисту не мають сенсу. Якщо ж $p_к \neq 0$, то необхідно сформулювати коло задач, вирішення яких дозволить створювати захищені ІКС.

Проаналізуємо випадок доцільності використання системи захисту інформації на основі запропонованого критерію для телефонного каналу зв'язку, який використовується для передавання цифрової конфіденційної інформації. Нехай $C_I^{\{1\}} = 10^{-4}$ грн./біт, $F = 3100$ Гц (смуга каналу тональної частоти), $T = 120$ сек., використовується модуляція QAM-256 ($\beta = \log_2(256) = 8$ (біт/сек.)/Гц [7, с.586]), $C_F = 1.863 \cdot 10^{-7}$ (грн./Гц)/сек. (вартість розраховано за матеріалами [10]), $p_к = 0.9$, $T_A = T = 120$ сек., $C_B^{\{1\}} = 1$ грн./біт. Тоді чистий прибуток від передавання інформації орендованим каналом (12) становитиме $Q \approx 298$ грн.; чистий прибуток від передавання інформації у випадку незахищеної системи (18) $Q_H = -2.7$ млн. грн., тобто компанія зазнаватиме значних збитків, що пояснюється великим значенням $C_B^{\{1\}}$, яке може характеризувати, наприклад, банківську інформацію (номера рахунків тощо).

Виникає питання проектування такої системи захисту (КСЗІ), яка б, принаймні, забезпечувала незбитковість передавання конфіденційної інформації, іншими словами, — виконання умови $Q_З \geq 0$. Визначимо техніко-економічні показники цієї системи, якщо час експлуатації T_0 системи захисту (КСЗІ) становить, наприклад, 1 місяць. Для цього необхідно розв'язати нерівність, засновану на виразі (14). Розв'язання цієї нерівності при наведених вище параметрах ТКС та інформаційної безпеки наведено на рис. 1.

Результати аналізу розв'язків показують, що для того щоб задовольнити умову $Q_З \geq 0$ можна, наприклад, впровадити організаційно-технічні заходи захисту вартістю $C_З = 10^3$ грн. та ймовірністю невідбиття загрози $(1-p_0) \leq 1.1 \cdot 10^{-4}$ (якщо це, звичайно, можливо практично реалізувати при їх вартості $C_З$) або організаційно-технічні заходи захисту вартістю $C_З = 10^6$ грн. та ймовірністю невідбиття загрози $(1-p_0) \leq 0.94 \cdot 10^{-4}$, тобто з вищими показниками ефективності (але й значно більшої при цьому вартості). Таким чином, запропонований підхід дозволяє з множини систем захисту, які можна реалізувати при їх вартості $C_З$, обрати систему найменшої вартості або ж визначити вимоги до необхідного рівня її ефективності при заданій вартості.

Розглянемо задачу з іншого боку: нехай існує система захисту інформації з певною вартістю $C_З$ та ефективністю p_0, необхідно визначити ефективність передавання повідомлень β, яка б забезпечувала деяке значення прибутку $Q_З$. Нехай за наведених вище параметрів $Q_З = 10$ грн. Розв'язуючи рівняння (14) при $Q_З = 10$ отримаємо залежності $\beta(C_З, p_0)$, показані на рис. 2.

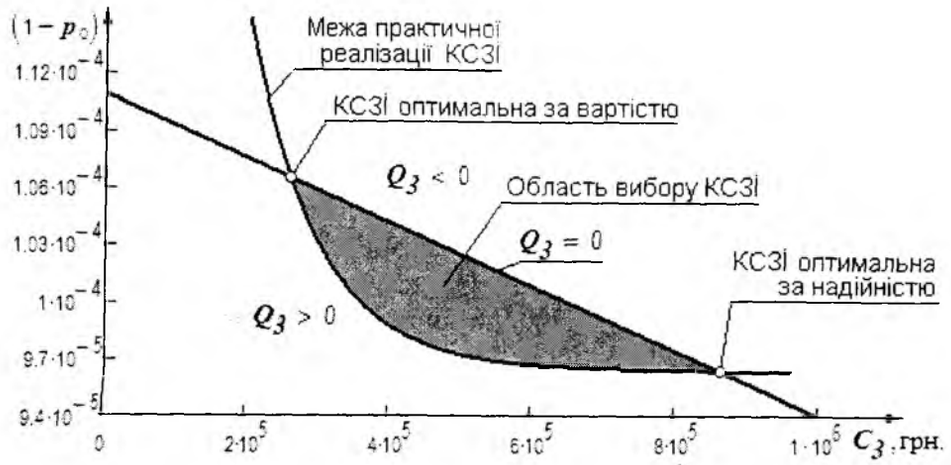

Рис. 1. Залежність прибутку від техніко-економічних показників системи захисту інформації

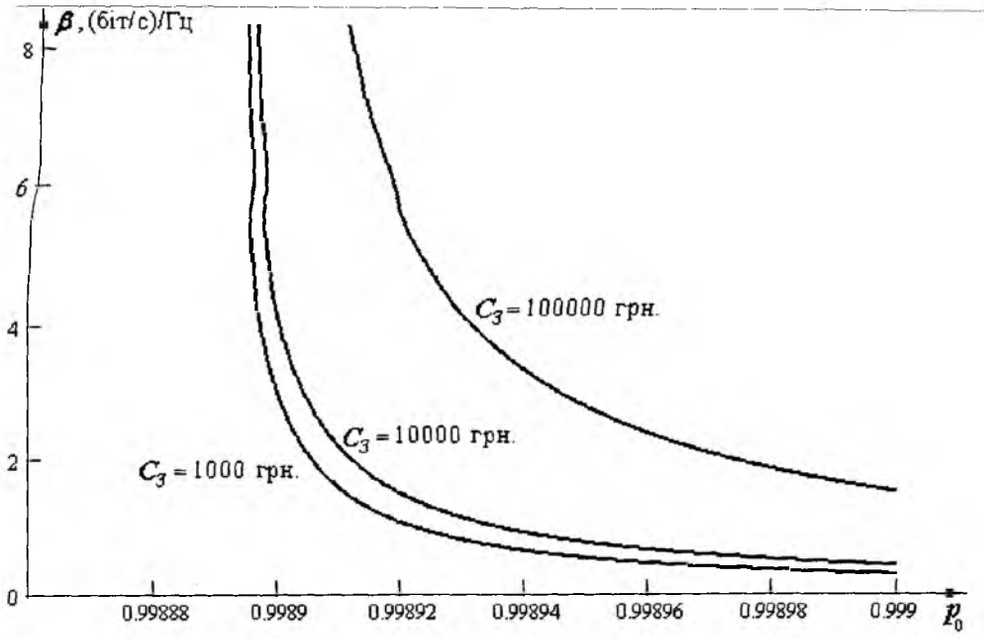

Рис. 2. Залежність ефективності передавання інформації від техніко-економічних показників системи захисту інформації

Найперша вимога до будь-якої ІКС — отримання найбільшого прибутку від інформації, яка передається або циркулює в системі. Оскільки вартість оренди потрібної смуги частот визначається кон'юнктурою ринку, розглянемо низку заходів, які забезпечать максимальний прибуток. Це, перш за все, застосування найбільш ефективних методів модуляції, які забезпечують найкраще використання орендованої смуги частот (параметр F). Великі перспективи з'являються з розробкою раціональних методів кодування сигналів, для усунення їх надлишковості (параметр a), що також надає можливість найкраще використовувати смугу (F).

Велике значення має визначення моменту часу і його величини, за яким здійснюється атака на ІКС. Слід вважати перспективними методи передавання інформації, при яких важко визначити моменти передавання конфіденційної інформації або й взагалі сам факт ведення такого передавання. При цьому можуть бути використані стеганографічні методи передавання інформації, які добре приховують сам факт передавання конфіденційної інформації, дозволяючи значно збільшити ймовірність відбиття загрози p_0 і, як наслідок, отримати запланований прибуток.

У межах запропонованої системи оцінки ефективності захисту інформації в ІКС проаналізуємо чистий прибуток від передавання інформації із застосуванням

широкосмугових методів передавання. При цьому, з точки зору інформаційної безпеки, врахуємо властивість скритності широкосмугових систем зв'язку [9, с.8]. Застосування широкосмугових методів передавання робить складним виявлення прихованих даних та їх видалення. Оскільки сигнали, які розподілені у значно ширшій смузі частот, ніж інформаційний сигнал, важко видалити, методи захисту інформації, побудовані на основі широкосмугових методів передавання, є стійкими до впливу випадкових і навмисних завад [4, с.488].

Імовірність виявлення випромінювання p_{det} широкосмугового сигналу (ШСС), а, отже, й конфіденційної інформації, що передається широкосмуговими методами, можна визначити за формулою [8, с.110-114]

$$p_{det} = \frac{1}{\sqrt{2\pi}} \cdot \int_{-\infty}^{x} \exp\left(-z^2/2\right) \mathrm{d}z. \quad (25)$$

У виразі (25) параметр

$$x = \left[\left(h_0^2/B\right) \cdot \sqrt{\alpha_1} - x_0\right] \Big/ \left(1 + h_0^2/B\right),$$

де $B = F \cdot \Delta T$ – база сигналу (тут ΔT – тривалість ШСС); $h_0^2 = q^2/(2B)$ – співвідношення сигнал/завада на вході приймача-аналізатора; q^2 – співвідношення сигнал/завада на виході приймача-аналізатора; α_1 – параметр, який залежить від характеристик системи обробки сигналу; x_0 – параметр, що визначає ймовірність хибної тривоги P_x приймача-аналізатора (наприклад, при $x_0 = 3.1$ імовірність $P_x = 10^{-3}$ [8]).

Також при використанні широкосмугових методів передавання зловмиснику необхідно буде витратити певний час T_{det} для виявлення сигналу. Час виявлення ШСС можна визначити [8,9] за формулою $T_{det} = \alpha_2 \cdot F$, де $\alpha_2 = 2 \cdot q^4 \cdot \left(\delta_{Ш}^2 / P_C^2\right)$, $\delta_{Ш}^2$ – потужність власних шумів приймача. Враховуючи час T_{det}, який зловмиснику необхідно витратити для виявлення ШСС, час перехоплення інформації зменшується з T_A до

$$T_A^* = \begin{cases} T_A - T_{det}, & \text{при } T_A \geq T_{det}; \\ 0, & \text{при } T_A < T_{det}, \end{cases} \quad (26)$$

тобто можливий випадок, коли час, який необхідно витратити для виявлення сигналу, перевищуватиме час передавання конфіденційного повідомлення.

Враховуючи імовірність виявлення p_{det} і час виявлення ШСС T_{det} у формулі (18), отримаємо значення чистого прибутку для випадку використання широкосмугових методів передавання:

$$\begin{aligned} Q &= D - S - C_B = \\ &= C_I^{\{1\}} \cdot T \cdot R - C_F \cdot T \cdot F - \\ &\quad - C_B^{\{1\}} \cdot T_A^* \cdot R \cdot p_к \cdot p_{det} \ [грн.]. \end{aligned} \quad (27)$$

Ширину смуги частот виразимо через базу ШСС та швидкість передавання інформації $F = B \cdot R$. Дослідимо чистий прибуток від передавання інформації як функцію від бази сигналу

$$\begin{aligned} Q(B) &= C_I^{\{1\}} \cdot T \cdot R - C_F \cdot T \cdot B \cdot R - \\ &\quad - C_B^{\{1\}} \cdot T_A^*(B) \cdot R \cdot p_к \cdot p_{det}(B) \ [грн.]. \end{aligned} \quad (28)$$

Аналіз виразу (28) показує, що чистий прибуток у разі використання широкосмугових методів передавання, з одного боку, зменшується через необхідність збільшення смуги частот та орендної плати за неї (складова $-C_F \cdot T \cdot B \cdot R$), а з іншого боку (інформаційної безпеки) — збільшується через зменшення часу перехоплення інформації T_A^* та ймовірності визначення p_{det} (складова $-C_B^{\{1\}} \cdot T_A^*(B) \cdot R \cdot p_к \cdot p_{det}(B)$). База сигналу B у даному випадку є не лише характеристикою методу передавання, але й характеристикою певної системи організаційно-технічних заходів захисту інформаційних ресурсів, що заснована на властивостях ШСС.

Вираз (28) дозволяє за критерієм економічної доцільності, змінюючи значення бази ШСС, збалансовувати прибуток від передавання інформації. На рис. 3 наведено *побудовані за виразом (28)* [з урахуванням (25)-(27)] залежності $Q(B)$ при різних $C_B^{\{1\}}$ та $C_I^{\{1\}}$ для випадку деякої ІКС з характеристиками $R = 64$ кбіт/сек., $C_F = 2 \cdot 10^{-6}$ (грн./Гц)/сек., $T = 600$ сек. і системи атаки (приймача-аналізатора) з характеристиками $T_A = T = 600$ сек., $\alpha_1 = 1$, $q^2 = 10$ дБ, $\delta_{Ш}^2 / P_C^2 = 10^{-6}$, $P_x = 10^{-3}$, $p_к = 0{,}9$.

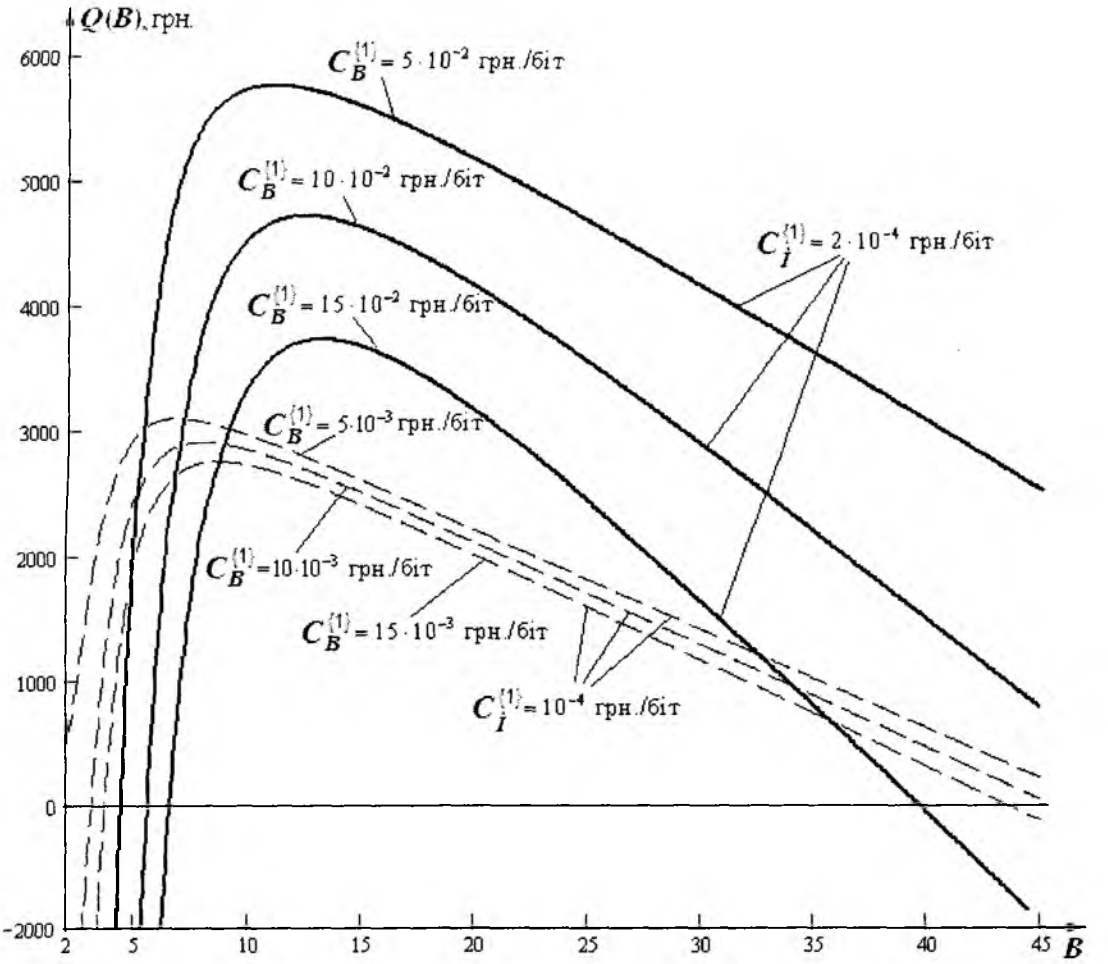

Рис. 3. Залежність прибутку від бази сигналу та вартості інформаційних ресурсів при використанні широкосмугових методів передавання

Як видно з рис. 3, при збільшенні ширини смуги частот прибуток спочатку зростає до певного значення Q_{max} при оптимальному значенні бази B_{opt}, що пояснюється суттєвим зменшенням збитків від втрати інформації при деякому збільшенні вартості оренди смуги частот; при $B > B_{opt}$ прибуток зменшується через таке збільшення витрат на оренду необхідної смуги частот, яке вже не окупає вартість інформаційних ресурсів. При $B = B_{opt}$ відбувається баланс між витратами на оренду смуги частот та збитками від втрати інформації, який призводить до максимуму прибутковості ІКС, тобто витрати на оренду смуги частот окупаються найоптимальнішим чином. Очевидно, що чим більшою є вартість інформаційних ресурсів ($C_B^{\{1\}}$ та $C_I^{\{1\}}$), тим більшою може бути ширина смуги частот (B_{opt}). Таким чином, при використанні широкосмугових методів передавання, збільшення ширини смуги частот сигналу (B) і відповідної вартості оренди цієї смуги частот окупається за рахунок збереження конфіденційності та цілісності конфіденційної інформації і є виправданим при її передаванні. Крім того, чим більшою є вартість інформації ($C_I^{\{1\}}, C_B^{\{1\}}$), тим більшою повинна бути база сигналу для того, щоб досягнути максимум прибутку (рис. 3).

Для знаходження оптимального значення бази сигналу B_{opt}, яке забезпечить максимальне значення прибутку Q_{max}, необхідно розв'язати рівняння

$$\frac{\partial Q\left(B, T, R, C_F, C_I^{\{1\}}, C_B^{\{1\}}, q^2, \delta_{Ш}^2 / P_C^2, P_x, T_A, \alpha_1, p_к\right)}{\partial B} = 0, \qquad (29)$$

яке враховує характеристики ІКС (B, T, R, C_F), вартість інформаційних ресурсів ($C_i^{\{1\}}$, $C_B^{\{1\}}$), характеристики системи нападу (q^2, $\delta_{Ш}^2 / P_C^2$, P_x, T_A, α_1, $p_к$).

Висновки та перспективи подальших досліджень

Обґрунтовано критерій оцінки захищеності ТКС на основі технічних та економічних характеристик і показників ТКС, систем реалізації атак на інформаційні ресурси та систем захисту інформації. Запропонований підхід, зокрема, дозволяє з множини систем захисту (організаційно-технічних заходів захисту) обрати систему найменшої вартості або визначити вимоги до необхідного рівня її ефективності при заданій вартості. У межах запропонованої системи оцінки ефективності захисту інформації в ІКС проаналізовано ефективність застосування ШСС для передавання та захисту конфіденційної інформації. Визначено підходи до оптимізації широкосмугових методів передавання (B_{opt}) при їх використанні для передавання конфіденційної інформації, які ґрунтуються на збалансуванні витрат на організацію широкосмугового каналу зв'язку та збитків від порушення конфіденційності та цілісності. Важливим напрямом досліджень для обґрунтованого визначення ймовірностей p_0 і $p_к$ є математичне моделювання моделі загроз. Треба визначити характер та величину напруженості поля, яке утворюється внаслідок побічних електромагнітних випромінювань та наводок в ІКС, та від засобів знятя інформації (радіозакладок, телефонних ретрансляторів тощо). Математичне моделювання цих загроз дозволяє науково обґрунтувати контрольовану зону та визначити ймовірність перехоплення інформації за межами цієї зони. Перспективним напрямком дослідження, для визначення p_0 і $p_к$ є вдосконалення методології експертних оцінок на базі нечіткої логіки [3]. Вирішення цієї проблеми дозволить суттєво вплинути на обґрунтованість рішень при побудові захищених ІКС.

Список літератури

1. *Щеглов А.Ю.* Защита компьютерной информации от несанкционированного доступа. — СПб.: «Наука и техника», 2004. — 384 с.

2. *Малюк А.А.* Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. пособие для вузов. — М: «Горячая линия − Телеком», 2004. — 280 с.

3. *Корченко А.Г.* Построение систем защиты информации на нечётких множествах. Теория и практические решения. — К.: «МК-Пресс», 2006. — 320 с.

4. *Хорошко В.А., Чекатков А.А.* Методы и средства защиты информации / Под ред. Ю.С. Ковтанюка. — К.: «Юниор», 2003. — 504 с.

5. *Домарев В.В.* Безопасность информационных технологий. Системный подход. — К.: ООО «ТИД "ДС"», 2004. — 992 с.

6. *Куликовский Л.Ф., Мотов В.В.* Теоретические основы информационных процессов: Учеб. пособие для вузов. — М.: «Высшая школа», 1987. — 248 с.

7. *Скляр Б.* Цифровая связь. Теоретические основы и практическое применение. Изд. 2-е, испр.: Пер. с англ. — М.: «Вильямс», 2004. — 1104 с.

8. *Супутникові* системи авіаційного зв'язку / В.П. Харченко, С.М. Паук, Л.М. Нестерова, Є.А. Знаковська. — К.: НАУ, 2003. — 188 с.

9. *Варакин Л.Е.* Системы связи с шумоподобными сигналами. — М.: «Радио и связь», 1985. — 384 с.

10. *Укртелеком* − Тарифи на користування телефоном для підприємств та організацій // http://www.ukrtelecom.ua/services/business/cityphone/using