## ІНФОРМАЦІЙНО-ДІАГНОСТИЧНІ СИСТЕМИ

УДК 681.3.06 (045)

[1]**Г.Ф. Конахович,** д.т.н., проф.
[2]**М.Г. Луцький,** к.т.н.

# ОЦІНКА ЕФЕКТИВНОСТІ ПОБУДОВИ КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Національний авіаційний університет
[1]E-mail: tks@nau.edu.ua
[2]E-mail: lutskyi.maksym@rada.gov.ua

*Обґрунтовано критерій оцінювання захищеності телекомунікаційні системи на основі технічних та економічних характеристик і показників телекомунікаційних систем, систем реалізації атак на інформаційні ресурси та систем захисту інформації.*

*Обоснован критерий оценки защищенности телекоммуникационных систем на основе технических и экономических характеристик и показателей телекоммуникационных систем, систем реализации атак на информационные ресурсы и систем защиты информации.*

*Grounded criterion for protection of TCS based on technical and economic characteristics and indicators of TCS, the systems of attacks on information resources and information security systems.*

### Постановка проблеми

Сьогодні найважливішим та найдорожчим ресурсом є інформація.

Побудова комплексної системи захисту інформації та оцінювання її ефективності – найважливіша задача на будь-якому підприємстві авіаційної галузі.

У такій ситуації актуального значення набуває задача вибору критеріїв оцінювання захищеності телекомунікаційних систем (ТКС).

Інтенсивне збільшення обсягів інформації, яка передається в корпоративних ТКС, зумовлює застосувувати додаткові заходи для її захисту. При цьому доцільно мати кількісний критерій оцінювання захищеності системи, який залежатиме від деякої множини чинників, що комплексно характеризують як саму ТКС, так і систему захисту інформаційних ресурсів, що циркулюють у ній.

### Аналіз досліджень та публікацій

Одним з напрямів оцінювання ефективності систем захисту інформації в ТКС є формалізація різних методик, змістом яких є системний підхід технічного захисту інформації (ТЗІ) [1–5].

**Мета** роботи – обґрунтування та формалізація критерію оцінювання захищеності ТКС на основі технічних та економічних характеристик і показників ТКС, систем реалізації атак на інформаційні ресурси та систем захисту інформації.

### Виклад основного матеріалу

Кількісний критерій $Z$ оцінювання захищеності ТКС визначають через множину чинників:

$$Z = f(C_i, C_в, C_з, C_д, S, p_к, p_0, \beta, R),$$

де $C_i$ – цінність інформації, що передається;

$C_в$ – загальні збитки від утрати інформації;

$C_з$ – вартість організаційно-технічних заходів із захисту інформації;

$C_д$ – вартість організаційно-технічних заходів з несанкціонованого доступу до інформації;

$S$ – вартість оренди каналів зв'язку;

$p_к$ – імовірність порушення конфіденційності або цілісності інформації;

$p_0$ – імовірність відбиття загрози;

$\beta$ – спектральна ефективність методу передавання в ТКС;

$R$ – швидкість передавання інформації.

Цінність інформації $C_i$ найбільш доцільно виразити через повні збитки $C_в$ від втрати цієї інформації. Для цього необхідно мати відомості щодо доходу $D$, який можна отримати від передавання інформації.

Для визначення доходу, перш за все, необхідно визначити кількість інформації $I$, яка передається каналом зв'язку, швидкість передавання цієї інформації $R$ та інтервал часу, протягом якого здійснюється повне передавання інформації $T$.

Цінність 1 біту інформації позначимо $C_E^{\{1\}}$. Тоді дохід від передавання інформації цифровими каналами зв'язку можна визначити таким чином:

$$D = C_E^{\{1\}} TR .$$

Для випадку повідомлень (наприклад, мовних), які можна формалізувати, використовуючи модель розподіленого за ґаусовим законом випадкового процесу, кількість інформації можна визначити за виразом [6]:

$$E = TF\log_2\left(a\frac{P_c}{P_з}\right),$$

де $F$ − ширина смуги частот, яку займає сигнал;

$a$ − коефіцієнт, який залежить від способу кодування сигнал;

$P_c$ − середня потужність сигналу;

$P_з$ − середня потужність завад з урахуванням складової відхилення сигналу від початкового у разі його перетворень.

У цьому випадку швидкість передавання інформації $R$ визначають таким чином:

$$R = \frac{E}{T} = F\log_2\left(a\frac{P_c}{P_з}\right).$$

Тоді дохід від передавання інформації каналом зв'язку зі швидкістю $R$ за час $T$ визначається з виразу

$$D = C_E^{\{1\}}TR = C_E^{\{1\}}TF\log_2\left(a\frac{P_c}{P_з}\right).$$

Нехай $C_B^{\{1\}}$ − вартість збитків унаслідок утрати 1 біту інформації. Тоді загальні збитки від втрати інформації можна розраховувати за формулою

$$C_в = p_к C_в^{\{1\}} T_a R = p_к C_в^{\{1\}} T_a F\log_2\left(a\frac{P_c}{P_з}\right),$$

де $T_a$ − час атаки, протягом якого здійснюється перехоплення інформації.

Повна вартість організаційно-технічних заходів із захисту інформації містить такі складові:

– витрати на організацію (попередні наукові дослідження і впровадження) системи захисту інформації $C_o^з$;

– витрати на устаткування захисту інформації $C_у^з$;

– експлуатаційні витрати $C_е^з$.

Отже, повна вартість системи захисту інформації, зокрема комплексної, визначається з виразу

$$C_з = C_o^з + C_у^з + C_е^з . \quad (1)$$

Зазначену вартість доцільно визначити в сумі, що відповідає інтервалу часу $T_0$, який залежно від стану технічних засобів захисту, процесу розвитку систем захисту, апаратури та методів несанкціонованого доступу являє собою:

– час, що відповідає стадії експлуатації системи захисту інформації і залежить від характеристик надійності обладнання;

– час, за який система захисту інформації втратить можливості ефективного захисту порівняно з більш ефективною апаратурою та методами несанкціонованого доступу.

Повну вартість системи несанкціонованого доступу до інформації визначають за виразом

$$C_д = C_o^д + C_у^д + C_е^д ,$$

де витрати $C_o^д$, $C_у^д$ і $C_е^д$ за своїм змістом аналогічні відповідним компонентам формули (1) з урахуванням спрямованості перших не на захист, а на несанкціонований доступ до інформації.

Позначимо через $C_F$ вартість оренди за одиницю часу 1 Гц каналу зв'язку. Тоді вартість оренди каналу зв'язку зі смугою $F$ за час $T$ визначають за формулою

$$S = C_F TF.$$

Імовірність загрози порушення конфіденційності та цілісності інформації $p_к$ залежить від співвідношення між цінністю інформації, збитками від її втрати, вартістю системи захисту інформації, а також витрат на одержання інформації незаконним шляхом:

$$p_к = \psi\,(C_і, C_в, C_з, C_д).$$

Чисельне значення цієї ймовірності можливо отримати за допомогою багатоетапного групового методу експертного оцінювання (прогнозування) дельфійською групою експертів, яка створюється з метою збирання інформації з визначених джерел з визначеної проблеми, наступним математичним опрацюванням експертних оцінок.

Кожен експерт повинен дати оцінку ймовірності $p_к$ виникнення загрози для витоку інформації, яка має цінність $C_і$ та захищена за допомогою витрат $C_з$. При цьому слід враховувати можливість нанесення максимальних збитків $C_в$ власнику інформації, а також капіталовкладення супротивника $C_д$ у реалізацію несанкціонованого доступу. Зазначена група експертів повинна на підставі відомостей про існуючу систему захисту інформації та ймовірної наявності у супротивника атакуючої системи оцінити ймовірність відбиття атаки $p_0$ (імовірність відсутності загрози), яку можна подати як функцію

$$p_0 = \varphi\,(p_к, C_з, C_д).$$

Спектральна ефективність методу передавання $\beta = R/F$ характеризує ефективність використання каналу зв'язку зі смугою $F$.

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

$$\begin{aligned} Q &= D - S = C_E^{\{1\}} TR - C_F TF = \\ &= T\left(C_E^{\{1\}} R - C_F F\right) = \\ &= TF\left(C_E^{\{1\}}\beta - C_F\right) \end{aligned}$$

або для мовних повідомлень:

$$\begin{aligned} Q &= C_E^{\{1\}} TF \log_2\left(a\frac{P_с}{P_з}\right) - C_F TF = \\ &= TF\left[C_E^{\{1\}} \log_2\left(a\frac{P_с}{P_з}\right) - C_F\right]. \end{aligned}$$

У разі проведення заходів щодо захисту інформації чистий прибуток від передавання інформації знизиться, і його можна визначити так:

$$\begin{aligned} Q_з &= D - S - C_з\frac{T}{T_0} - C_в(1-p_0) = \\ &= C_E^{\{1\}} TR - C_F TF - C_з\frac{T}{T_0} - \\ &- C_в^{\{1\}} T_а R p_к (1-p_0) = \\ &= C_E^{\{1\}} TF\beta - C_F TF - C_з\frac{T}{T_0} - \\ &- C_в^{\{1\}} T_а F\beta p_к (1-p_0) = \\ &= TF\left(C_E^{\{1\}}\beta - C_F\right) - C_з\frac{T}{T_0} - \\ &- C_в^{\{1\}} T_а F\beta p_к (1-p_0) \end{aligned} \qquad (2)$$

або для мовних повідомлень,

$$\begin{aligned} Q_з &= C_E^{\{1\}} TF\log_2\left(a\frac{P_с}{P_з}\right) - \\ &- C_F TF - C_з\frac{T}{T_0} - \\ &- C_в^{\{1\}} T_а F\log_2\left(a\frac{P_с}{P_з}\right) p_к (1-p_0) = \\ &= F\left[C_E^{\{1\}} T - C_в^{\{1\}} T_а p_к (1-p_0)\right]\times \\ &\times \log_2\left(a\frac{P_с}{P_з}\right) - T\left(C_F F - \frac{C_з}{T_0}\right). \end{aligned} \qquad (3)$$

У виразах (2) і (3) складова $-C_з \cdot T/T_0$ 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 $T_0 = T$.

Складова $-C_в^{\{1\}} T_а R p_к (1-p_0)$ враховує збитки через недосконаліть системи захисту при вкладених у неї коштах $C_з$. При цьому $p_к(1-p_0)$ – умовна ймовірність того, що загроза не буде відбита. Якщо система захисту є ідеальною (імовірність відбиття загрози $p_0 = 1$), то збитків через недосконаліть системи захисту немає.

Коефіцієнт зниження прибутковості захищеної системи передавання інформації $K_з$

$$\begin{aligned} K_з &= \frac{Q_з}{Q} = \left\{TF\left(C_E^{\{1\}}\beta - C_F\right) - C_з\frac{T}{T_0} - \right. \\ &\left. - C_в^{\{1\}} T_а F\beta p_к (1-p_0)\right\} : \left\{TF\left(C_E^{\{1\}}\beta - C_F\right)\right\} = \\ &= 1 - \frac{C_з\frac{T}{T_0} + C_в^{\{1\}} T_а F\beta p_к (1-p_0)}{TF\left(C_E^{\{1\}}\beta - C_F\right)} \end{aligned} \qquad (4)$$

для випадку мовних повідомлень можна обчислити за формулою

$$\begin{aligned} K_з &= \left\{C_E^{\{1\}} TF\log_2\left(a\frac{P_с}{P_з}\right) - C_F TF - \right. \\ &\left. - C_з\frac{T}{T_0} - C_в^{\{1\}} T_а F\log_2\left(a\frac{P_с}{P_з}\right) p_к (1-p_0)\right\} : \\ &: \left(TF\left[C_E^{\{1\}} \log_2\left(a\frac{P_с}{P_з}\right) - C_F\right]\right) = \\ &= 1 - \left\{C_з\frac{T}{T_0} + C_в^{\{1\}} T_а F\log_2\left(a\frac{P_с}{P_з}\right) p_к (1-p_0)\right\} : \\ &: \left\{TF\left[C_E^{\{1\}} \log_2\left(a\frac{P_с}{P_з}\right) - C_F\right]\right\}. \end{aligned} \qquad (5)$$

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 її перехоплення.

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

$$\begin{aligned} Q_{\text{Н}} &= D - S - C_{\text{в}} = \\ &= C_E^{\{1\}} TR - C_F TF - C_{\text{в}}^{\{1\}} T_{\text{а}} R p_{\text{к}} = \\ &= C_E^{\{1\}} TF\beta - C_F TF - C_{\text{в}}^{\{1\}} T_{\text{в}} F\beta p_{\text{к}} = \\ &= TF\left(C_E^{\{1\}}\beta - C_F\right) - C_{\text{в}}^{\{1\}} T_{\text{а}} F\beta p_{\text{к}} \end{aligned}$$

або для мовних повідомлень,

$$\begin{aligned} Q_{\text{н}} &= C_E^{\{1\}} TF\log_2\left(a\frac{P_{\text{с}}}{P_{\text{з}}}\right) - C_F TF - \\ &- C_{\text{в}}^{\{1\}} T_{\text{а}} F\log_2\left(a\frac{P_{\text{с}}}{P_{\text{з}}}\right) p_{\text{к}} = \\ &= TF\left[C_E^{\{1\}}\log_2\left(a\frac{P_{\text{с}}}{P_{\text{з}}}\right) - C_F\right] - \\ &- C_{\text{в}}^{\{1\}} T_{\text{а}} F\log_2\left(a\frac{P_{\text{с}}}{P_{\text{з}}}\right) p_{\text{к}}. \end{aligned}$$

Коефіцієнт зниження прибутковості незахищеної системи $K_H$ можна визначити за формулою

$$\begin{aligned} K_{\text{н}} &= \frac{Q_{\text{н}}}{Q} = \frac{TF\left(C_E^{\{1\}}\beta - C_F\right) - C_{\text{в}}^{\{1\}} T_{\text{а}} F\beta p_{\text{к}}}{TF\left(C_E^{\{1\}}\beta - C_F\right)} = \\ &= 1 - \frac{C_{\text{в}}^{\{1\}} T_{\text{а}}\beta p_{\text{к}}}{T\left(C_E^{\{1\}}\beta - C_F\right)}. \end{aligned} \qquad (6)$$

У випадку мовних повідомлень коефіцієнт $K_{\text{н}}$ може бути обчислений за формулою:

$$\begin{aligned} K_{\text{н}} &= \left\{TF\left[C_?^{\{1\}}\log_2\left(a\frac{P_{\text{с}}}{P_{\text{з}}}\right) - C_F\right] - \right. \\ &\left. - C_{\text{в}}^{\{1\}} T_{\text{а}} F\log_2\left(a\frac{P_{\text{с}}}{P_{\text{з}}}\right) p_{\text{к}}\right\}: \\ &: \left\{TF\left[C_E^{\{1\}}\log_2\left(a\frac{P_{\text{с}}}{P_{\text{з}}}\right) - C_F\right]\right\} = \\ &= 1 - \frac{\left\{C_{\text{в}}^{\{1\}} T_{\text{а}}\log_2\left(a\frac{P_{\text{с}}}{P_{\text{з}}}\right) p_{\text{к}}\right\}}{\left\{T\left[C_E^{\{1\}}\log_2\left(a\frac{P_{\text{с}}}{P_{\text{з}}}\right) - C_F\right]\right\}}. \end{aligned} \qquad (7)$$

Очевидно, що якщо $K_{\text{н}} > K_{\text{з}}$, то будь-які заходи щодо захисту інформації в системі не мають сенсу. Цю нерівність можна записати таким чином:

$$0 < Z = K_{\text{н}} - K_{\text{з}}. \qquad (8)$$

Ураховуючи вирази (4), (6), отримаємо нерівність, при якій виконується умова (8):

$$\frac{C_{\text{з}}\frac{T}{T_0} - C_{\text{в}}^{\{1\}} T_{\text{а}} F\beta p_{\text{к}} p_0}{TF\left(C_E^{\{1\}}\beta - C_F\right)} > 0$$

або для мовних повідомлень, беручи до уваги формули (5), (7):

$$\frac{C_{\text{з}}\frac{T}{T_0} - C_{\text{в}}^{\{1\}} T_{\text{а}} F\log_2\left(a\frac{P_{\text{с}}}{P_{\text{з}}}\right) p_{\text{к}} p_0}{TF\left(C_E^{\{1\}}\log_2\left(a\frac{P_{\text{с}}}{P_{\text{з}}}\right) - C_F\right)} > 0.$$

Отримані результати дозволяють приймати рішення щодо доцільності проведення заходів із захисту інформації в ТКС.

Якщо організація вирішила впроваджувати заходи щодо захисту власної інформації, необхідно розробляти комплексну систему захисту інформаційних ресурсів корпоративної мережі виходячи з загальних положень щодо організації ТЗІ у ТКС.

На інформацію, яка підлягає технічному захисту, у процесі функціонування ТКС можуть впливати загрози, внаслідок чого може виникнути її витік, порушення її цілісності або порушення доступності до неї з боку авторизованих користувачів (Закон України «Про захист інформації у автоматизованих системах», «Положення про технічний захист інформації в Україні», Рекомендації Ради Європи № R (89)2, R (95)4 та ін.).

Спроможність системи ТЗІ протистояти впливу загроз визначає рівень захищеності інформаційних ресурсів ТКС.

Телекомунікаційні системи, як правило, оснащуються штатними і за необхідності додатковими (позаштатними) засобами ТЗІ, які в разі їхнього спільного використання утворюють комплекс засобів і механізмів захисту (КЗМЗ), що забезпечує потрібний рівень захищеності інформаційних ресурсів цих систем.

Основні принципи організації ТЗІ полягають у такому:

1) принцип легітимності ТЗІ у ТКС повинен ґрунтуватися на положеннях і вимогах чинних в Україні нормативно-правових актів і нормативних документів щодо ТЗІ;

2) принцип комплексності ТЗІ у ТКС повинен забезпечуватися комплексом взаємопов'язаних програмно-технічних засобів і організаційних заходів;

3) принцип безперервності ТЗІ у ТКС повинен забезпечуватися на всіх технологічних етапах та режимах її функціонування й надання послуг, зокрема під час проведення ремонтних і регламентних робіт;

4) принцип мінімальної достатності захисту ТКС повинен забезпечувати необхідний рівень захищеності у разі мінімальних витрат ресурсів;

5) програмно-технічні засоби захисту не повинні істотно погіршувати основні характеристики ТКС (пропускну здатність, надійність, можливість зміни конфігурації ТКС);

6) невід'ємною частиною робіт з ТЗІ у ТКС є оцінювання ефективності засобів захисту, що здійснюється згідно з методиками, які враховують всю сукупність технічних характеристик оцінюваного об'єкта, включаючи технічні рішення і практичну реалізацію засобів захисту;

7) технічний захист інформації в ТКС повинен передбачати створення систем керування комплексами засобів захисту, що дозволяють здійснювати безперервний контроль ефективності засобів захисту, підтримку необхідного рівня захищеності інформаційних ресурсів ТКС.

Технічний захист інформації у ТКС – це запобігання за допомогою інженерно-технічних заходів реалізаціям загроз для інформаційних ресурсів ТКС, що створюються через технічні канали, канали спеціальних впливів та шляхом несанкціонованого доступу.

Канали спеціальних впливів на елементи ТКС – це канали, через які впливи на технічні (апаратні) засоби ТКС призводять до створення загроз для інформації.

Реалізація загроз для інформації у ТКС через канали спеціальних впливів можлива за таких умов:

– кількісної недостатності компонентів ТКС;

– якісної недостатності компонентів і (або) всієї ТКС у цілому;

– навмисної або ненавмисної діяльності осіб, які, в свою чергу, впливають на елементи ТКС з використанням програмних і (або) технічних засобів;

– несправностей апаратних елементів ТКС;

– виходів за межі допустимих значень параметрів зовнішнього середовища функціонування ТКС, у тому числі пов'язаними зі стихійними лихами, катастрофами й іншими надзвичайними подіями;

– помилок і некоректних дій суб'єктів доступу до ресурсів ТКС на стадії її промислової експлуатації.

Функціональна послуга захисту – взаємопов'язана множина виконуваних ТКС елементарних функцій, яка дозволяє протистояти певним загрозам для інформації.

База захисту ТКС – сукупність усіх елементів системи ТЗІ (методологічних, методичних, проектних, програмних, апаратних, організаційних, які відносяться до організації протидії загрозам для інформаційних ресурсів у ТКС.

Комплекс засобів і механізмів захисту – взаємопов'язаний набір засобів і механізмів ТЗІ, що реалізують обрану модель захисту інформаційних ресурсів у ТКС.

Оцінка ТКС за критеріями ТЗІ – комплекс спеціалізованих дослідницько-аналітичних та експериментальних робіт, що виконуються з метою визначення відповідності системи захисту інформації у ТКС до вимог (специфікацій) нормативних документів з ТЗІ.

Експертиза ТКС за критеріями ТЗІ – діяльність, метою якої є дослідження, перевірка, аналіз та оцінювання науково-технічного рівня системи захисту інформації у ТКС, а також підготовка обгрунтованих висновків для прийняття рішення щодо рівня захищеності інформаційних ресурсів ТКС в описаних заявником умовах експлуатації ТКС та рівня довіри до результатів оцінювання.

Зміст і послідовність робіт з протидії загрозам та їх нейтралізації повинні відповідати вказаним у ДСТУ 3396.0-96 і ДСТУ 3396.1-96 етапам створення системи захисту інформації:

– розроблення технічної політики забезпечення захисту інформаційних ресурсів ТКС, що знаходиться в експлуатації (розроблення моделі загроз інформаційним ресурсам ТКС, розроблення технічного та робочого проектів системи ТЗІ у ТКС);

– впровадження розробленої технічної політики забезпечення захисту інформаційних ресурсів ТКС в експлуатаційну практику (реалізація технороботочого проекту системи ТЗІ – опції робіт );

– підтримка впровадженої технічної політики забезпечення захисту інформаційних ресурсів ТКС у процесі її експлуатації (оцінювання ТКС за критеріями ТЗІ).

Технічну політику забезпечення захисту інформаційних ресурсів іноді скорочено називають політикою безпеки. Зазвичай розроблення політики безпеки полягає у розробленні та реалізації технороботочого проекту системи ТЗІ у ТКС.

На початковому етапі для вперше створюваних ТКС (інформаційні мережі з розподіленим керуванням і з розподіленим опрацюванням даних або систем комутації телефонних каналів зв'язку), у складі яких планується використання ТКС, розроблюється технічне завдання на створення ТКС – вимоги до ТЗІ у ТКС. Ці вимоги включають до складу розділу технічного завдання (ТЗ), що відображає вимоги з ТЗІ у ТКС у цілому і оформлюється згідно з ГОСТ 34.602-89.

Крім того, в інших розділах ТЗ на ТКС мають бути враховані вимоги з ТЗІ.

Для вже введених в експлуатацію ТКС, але не атестованих за критеріями ТЗІ, технічні вимоги до системи ТЗІ у ТКС розроблюються у вигляді окремого документу згідно з ГОСТ 34.602-89.

Зазвичай розроблення технічної політики захисту починають з розроблення ТЗ або технічних вимог до створюваної системи захисту.

У процесі розроблення ТЗ на систему ТЗІ у ТКС:

– аналізуються інформаційні потоки через ТКС, характер і зміст розв'язуваних її користувачами задач, рівень цінності (ступінь конфіденційності) інформації користувачів;

– оцінюються характеристики технологічного середовища експлуатації ТКС, що підлягає захисту;

– створюються моделі порушників;

– виявляються дестабілізуючі чинники та загрози для інформаційних ресурсів;

– прогнозуються ймовірності прояву загроз, потенційно можливі та припустимі втрати власників і користувачів ТКС, пов'язаних з такими проявами;

– будується модель загроз;

– задаються вимоги до необхідного рівня захищеності інформаційних ресурсів у ТКС.

На стадії розроблення ТЗ на систему ТЗІ у ТКС виконуються такі види робіт:

– аналіз інформаційного середовища, створеного або створюваного на базі використання ТКС, що потребує захисту;

– аналіз середовища користувачів ТКС;

– аналіз середовища потенційних порушників;

– оцінювання основних характеристик технологічного середовища функціонування штатних засобів ТКС до проведення заходів захисту;

– побудова моделі загроз для інформації у ТКС, включаючи аналіз ризиків, пов'язаних із можливими реалізаціями загроз;

– визначення необхідного рівня захищеності інформаційних ресурсів ТКС;

– формування основних технічних вимог до розроблення моделі захисту ТКС, яке здійснюється на стадії технічного проектування.

Аналіз передбачуваних середовищ функціонування ТКС виконується на якісному рівні в загальному вигляді, враховуються основні характеристики об'єктів й особливості взаємовідносин суб'єктів у досліджуваних середовищах.

На першому етапі розробклення ТЗ визначають:

– необхідний рівень довіри до коректності створюваної системи ТЗІ, оскільки зміст і обсяг потрібних вихідних даних, виконуваних спеціальних досліджень і аналізів, рівень глибини (деталізації, формалізації) необхідних обгрунтувань залежать від потрібного рівня довіри до коректності або рівня гарантій системи захисту;

– призначення ТКС, що потребує захисту, і основні розв'язувані на її базі задачі;

– обсяги та ступінь важливості (цінності, конфіденційності) оброблюваної та транспортованої інформації;

– структуру основних інформаційних взаємозв'язків;

– основні характеристики технологічного середовища експлуатації ТКС, включаючи основні умови, режими та способи опрацювання і транспортування інформації;

– передбачувані межі зон, що потребують захисту;

– рівні інформативних випромінювань і наведень від побічних явищ;

– основні види загроз для інформації та технічні канали реалізації цих загроз;

– основні характеристики організаційних структур потенційних порушників.

Вихідними даними для робіт, що виконуються в процесі розроблення ТЗ, є:

– вимоги до функцій (задач), що виконуються системою, і вимоги до видів забезпечення ТЗ на вперше створювані і (або) вже створені автоматизовані системи, у складі яких використовується або планується використання ТКС, що потребує захисту;

– організаційно-розпорядницька й експлуатаційна документація на фрагмент (ділянку) телекомунікаційної мережі, у складі якої використовується або планується використання ТКС, що потребує захисту;

– документи, що містять описи організаційних структур користувачів (абонентів) ТКС, що потребує захисту;

– документи, що містять описи організаційних структур потенційних порушників;

– комплект технічної документації, включений до складу поставленої конфігурації ТКС;

– нормативні документи ТЗІ.

Результатом виконання першого етапу розроблення ТЗ є обране значення необхідного рівня довіри до коректності створюваної системи ТЗІ.

На другому етапі розроблення ТЗ здійснюють:

– визначення необхідного рівня захищеності інформаційних ресурсів ТКС, що потребує захисту;

– розроблення основних технічних вимог до забезпечення ТЗІ з метою їх використання в процесі техноробочого проектування системи захисту.

За високих рівнів оцінювань, починаючи з рівня довіри Е4 (для АТС) та рівня гарантій ГЗ (для комп'ютерних систем) і вище, необхідно:

– розробити модель політики безпеки;

– виконати аналіз середовищ функціонування ТКС;

– створити моделі порушників;

– створити та проаналізувати модель загроз;

– виконати аналіз ризиків;

– обґрунтувати необхідний рівень захищеності інформаційних ресурсів ТКС для конкретних або передбачуваних умов її експлуатації.

Результатами виконання другого етапу розроблення ТЗ є:

– отриманий перелік суттєвих потенційних загроз для інформаційних ресурсів ТКС із зазначеними граничнодопустимими рівнями втрат від їхніх можливих реалізацій;

– основні технічні вимоги до розроблення моделі захисту.

У процесі аналізу інформаційного середовища ТКС досліджується:

– характер і зміст задач користувачів і персоналу телекомунікаційної системи;

– структура інформаційних взаємозв'язків;

– об'ємно-часові характеристики і ступінь важливості (цінності, конфіденційності) інформації, що циркулює у ТКС.

У процесі аналізу середовища користувачів ТКС досліджуються:

– організаційні структури користувачів;

– склад і функціональні обов'язки користувачів;

– повноваження користувачів.

У процесі аналізу технологічного середовища ТКС досліджуються:

– основні характеристики ТКС, що потребує захисту;

– характеристики середовища транспортування інформації;

– умови та способи опрацювання інформації штатними засобами ТКС, що потребує захисту з позицій ТЗІ;

– зовнішні чинники середовища експлуатації ТКС (спеціальні дослідження) з позицій ТЗІ.

У процесі аналізу середовища потенційних порушників досліджуються:

– організаційні структури потенційних порушників;

– склад і можливості потенційних порушників, що загрожують інформації у ТКС;

– моделі потенційних порушників.

У процесі аналізу середовища функціонування ТКС виконуються:

– аналіз ризиків, пов'язаних із можливими реалізаціями загроз;

– побудова моделі загроз.

За результатами побудови моделі загроз визначається необхідний рівень захищеності інформаційних ресурсів ТКС.

На завершальному етапі визначаються основні технічні вимоги до розроблення моделі захисту ТКС.

У процесі технороботочого проектування системи ТЗІ у ТКС послідовно розроблюють:

– технічний проект моделі захисту інформаційних ресурсів ТКС;

– робочий проект КЗМЗ.

Створення моделі захисту містить у собі:

– визначення множини функціональних послуг захисту, які протидіють загрозам, що включені в модель загроз;

– визначення мінімально необхідних рівнів стійкості механізмів захисту, що реалізують послуги захисту з обраної множини функціональних послуг;

– оптимізація проекту моделі захисту за критеріями дієвості;

– забезпечення функціональної достатності моделі захисту;

– усунення функціональної надмірності моделі захисту.

З метою спрощення процесу проектування системи ТЗІ і полегшення сприйняття результатів оцінювання захищеності інформації у ТКС за аналогією з Європейськими критеріями безпеки (ITSEC) доцільно специфікувати перелік стандартних профілів захищеності інформації у ТКС для різних умов їхнього застосування.

Створення проекту КЗМЗ містить у собі:

– визначення множини засобів і механізмів захисту, які коректно реалізують функціональні послуги, що входять до моделі захисту;

– проектування (вибір) засобів та механізмів захисту з заданими стійкостями (НД ТЗІ 1.1-001-99) від прямих впливів загроз [12];

– усунення слабких місць у проекті КЗМЗ з урахуванням передбачуваних умов експлуатації комплексу;

– забезпечення функціональної достатності проекту КЗМЗ;

– усунення функціональної надмірності в проекті КЗМЗ.

У процесі реалізації технороботочого проекту системи ТЗІ у ТКС виконують:

– програмну та апаратну реалізацію розробленого КЗМЗ, який забезпечує наведений у ТЗ рівень захищеності інформаційних ресурсів ТКС;

– випробування реалізованого КЗМЗ на відповідність нормативним специфікаціям і проектній документації ;

– оцінювання реальних характеристик технологічного середовища функціонування захищеної ТКС після проведення заходів захисту;

– оцінювання ефективності нейтралізації слабких місць у захисті;

– оцінювання досягнутого рівня довіри до коректності реалізованої системи ТЗІ у ТКС, що потребує захисту .

Механізми захисту, які включені в проект КЗМЗ, але не реалізовані штатними засобами ТКС, що потребує захисту, створюються на базі програмних й (або) апаратних засобів і включаються до складу поточної конфігурації ТКС.

Обсяг і глибина впроваджуваних випробувань реалізованого КЗМЗ на відповідність нормативним специфікаціям і проектній документації, а також повнота охоплення випробуваннями елементів ТКС залежить від потрібного рівня довіри або гарантій до коректності системи ТЗІ.

Результат випробувань – підтвердження потрібного рівня довіри або гарантій до того, що реалізований КЗМЗ відповідає проектній документації.

Технологічне середовище функціонування захищеної ТКС оцінюються з метою отримання впевненості в тому, що реальні характеристики функціонування захищеної ТКС після проведення заходів захисту знаходяться в припустимих діапазонах значень, що вказані в нормативній документації. Змістом робіт є визначення, у тому числі й експериментальним шляхом згідно зі спеціалізованими методиками вимірів сигналів та полів від побічних явищ, реальних характеристик і параметрів середовища функціонування захищеної ТКС і порівняння отриманих оцінок із нормованими припустимими значеннями відповідно до розробленої програми та методики проведення вимірювань.

Обсяг виконуваних спеціальних досліджень середовища, а також повнота охоплення дослідженнями елементів середовища залежить від потрібного рівня довіри або гарантій до коректності системи ТЗІ.

Результат оцінки – підтвердження впевненості в тому, що реальні характеристики технолог-гічного середовища функціонування захищеної ТКС після проведення заходів захисту знаходяться в припустимих діапазонах значень.

Підтримка впровадженої технічної політики забезпечення захисту в період експлуатації – одне з основних завдань персоналу, що експлуатує ТКС, у сфері ТЗІ – оцінити достатність і ефективність побудованої моделі захисту, а також повноту, коректність і ефективність реалізації створеним КЗМЗ функціональних послуг захисту у реальних умовах функціонування ТКС [7; 11].

У процесі виконання оціночних робіт на основі матеріалів ТЗ на систему ТЗІ:

– аналізуються умови, в яких повинна працювати ТКС;

– оцінюється слушність вибору необхідного рівня захищеності інформаційних ресурсів, структурованого за видами;

– на основі матеріалів технороботочого проекту на систему ТЗІ, технічної документації на ТКС (особливо опису комплексу засобів захисту), програми, методики і протоколів випробувань системи ТЗІ перевіряється ефективність і коректність реалізації обраної моделі захисту.

Під ефективністю реалізації моделі розуміється:

– взаємна узгодженість відображених у моделі функціональних послуг захисту між собою;

– спроможність механізмів захисту, що реалізують на практиці задані в моделі функціональних послуг захисту, протистояти прямим атакам;

– неможливість практичного використання слабкості в архітектурі ТКС,

– неможливість практичного використання слабкості в експлуатаційному середовищі КТС,

– неможливість небезпечного конфігурування або використання ТКС в умовах, коли засоби, що інформують персонал про перехід станції в небезпечний стан, відсутні або дають помилкові показання.

Під коректністю реалізації моделі захисту розуміється кон'юнкція таких подій:

– проект КЗМЗ містить реалізації усіх без винятку ФПЗ, що включені у модель захисту;

– система ТЗІ, що реально створена на ТКС, містить у собі всі без винятку засоби і механізми захисту, які відображені у проекті КЗМЗ;

– технічний проект системи ТЗІ містить опис функціональних послуг захисту, що відповідає нормуючим специфікаціям;

– робочий проект системи ТЗІ містить опис механізмів захисту, що відповідає нормуючим специфікаціям;

– механізми захисту, що належать до складу КЗМЗ, реально функціонують відповідно до специфікацій робочого проекту та нормуючих специфікацій за результатами випробувань системи ТЗІ, зокрема її тестування у процесі експлуатації.

Аналіз слабких місць робиться в контексті забезпечення необхідного рівня захищеності ін.-формаційних ресурсів.

Наприклад, можливо примиритися з наявністю таємних каналів передавання інформації, якщо немає вимог до навмисних порушень конфіденційності.

Слабкість конкретного захисного механізму стосовно певного виду загроз може не мати значення, якщо вона компенсується іншими засобами забезпечення безпеки.

**Висновки**

Обгрунтовано критерій оцінювання захищеності ТКС на основі:

– технічних та економічних характеристик і показників ТКС;

– систем реалізації атак на інформаційних ресурсів;

– систем захисту інформації.

Запропонований підхід дозволяє з множини систем захисту (організаційно-технічних заходів захисту) обрати систему найменшої вартості або визначити вимоги до необхідного рівня її ефективності за заданої вартості.

У межах запропонованої системи оцінювання ефективності захисту інформації в ТКС приймають рішення щодо можливості побудови комплексної системи захисту інформаційних ресурсів корпоративної мережі.

Запропоновано підходи до побудови комплексної системи захисту інформації корпоративної ТКС виходячи з загальних положень щодо організації технічного захисту інформації.

Важливим напрямом досліджень для ефективної побудови та подальшої експлуатації комплексних систем захисту є математичне моделювання моделі загроз.

Треба визначити характер та важливість загроз для корпоративної ТКС і на основі цього будувати ефективну систему захисту.

Перспективним напрямком дослідження є вдосконалення методології експертного оцінювання ефективності захисту.

Вирішення цієї проблеми дозволить суттєво вплинути на обґрунтованість рішень під час побудови захищених ТКС.

**Література**

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

2. *Малюк А.А.* Информационная безопасность: концептуальные и методологические основы защиты информации: учеб. пособ. для вузов / А.А. Малюк . – М.: Горячая линия − Телеком, 2004. – 280 с.

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

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

5. *Домарев В.В.* Безопасность информационных технологий. Системный поход / В.В. Домарев . – К.: ООО «ТИД “ДС”», 2004. – 992 с.

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

7. *Скляр Б.* Цифровая связь. Теоретические основы и практическое применение. Изд. 2-е, испр. / Б. Скляр / 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 / Л.Е. Варакин. – М.: «Радио и связь», 1985. – 384 с.

10. *Защита* информации в телекоммуникационных системах / Г.Ф.Конахович, В.П. Климчук, С.М. Паук, В.Г. Потапов – К.: «МК-Пресс», 2005. – 279 с.

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

Стаття надійшла до редакції 20.04.10.