УДК 681.3:621.396

А.В. Дудатьев, к.т.н.
О.П. Войтович, к.т.н.
І.А. Дудатьєв

АНАЛІЗ ТА ЗАБЕЗПЕЧЕННЯ КОМПЛЕКСНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ КОНФЛІКТІВ

Вінницький національний технічний університет, o_voytovych@mail.ru

В статті розглянуті сучасні методи оцінювання комплексної інформаційної безпеки підприємства в умовах виникнення конфлікту. Представлені узагальнені математичні моделі для забезпечення необхідного рівня безпеки, як на етапі проектування, так і на етапі експлуатації системи захисту інформацій. Запропонована структура системи захисту інформації, яка реагує на виникнення конфліктної ситуації.

Ключові слова: *інформаційна безпека, конфлікт, оцінювання ризику, проектування системи захисту, інформаційно-аналітичний відділ.*

Вступ

Сучасні конфліктні ситуації характеризуються тим, що у конфліктах беруть участь складні технічні системи, які доцільно представляти математичними моделями. Загальна теорія конфліктів, зокрема, у соціальних, соціально технічних системах дозволяє сформулювати загальні положення щодо причин їх виникнення, протікання та методів їх вирішення. Формалізація життєвого циклу конфлікту дозволяє вирішити актуальні задачі, а саме: причини виникнення конфлікту, мету сторін, задіяних у конфлікті, компромісні дії, які можуть сприяти вирішенню конфліктної ситуації. Останнім часом актуальними є проведення так званих інформаційних атак або війн. Мета таких заходів у більшості випадків формулюється, як спроба реалізації лідерства на відповідному сегменті ринку, тобто викликана конкуренцією у боротьбі за лідерство або проведенні психологічної атаки, що характерно для сучасного тероризму. У цьому випадку забезпечення комплексної безпеки зводиться до забезпечення інформаційної безпеки, практична реалізація якої полягає у розв'язку двох задач: безпосереднього захисту своїх інформаційних ресурсів від ймовірного несанкціонованого доступу та отримання певної інформації щодо дій своїх конкурентів з метою упередження можливих несанкціонованих дій і як наслідок зменшення негативних наслідків.

Таким чином, можна констатувати, що проблема аналізу причин виникнення конфліктних ситуацій у сучасних, в тому числі і інформаційних системах є актуальною, оскільки її рішення дозволить оптимізувати процеси підготовки та прийняття управлінських рішень та мінімізувати ймовірні ризики.

Існуючі моделі інформаційної безпеки

Зараз на практиці використовуються такі моделі для аналізу інформаційної безпеки [1]: модель матриці доступу URL; модель "Take-Grant"; модель "Белла-Лападула"; модель "Low-Woter-Mark".

Перераховані моделі інформаційної безпеки мають ряд недоліків, які пов'язані з відсутністю методичних рекомендацій щодо практичного використання при побудові і експлуатації різних інформаційних систем. Як наслідок, моделі не забезпечують адекватної оцінки ефективності функціонування системи захисту. Крім того представлені моделі не враховують особливості впливу зовнішнього середовища на систему захисту, динаміку змін, як самих інформаційних ресурсів так і механізмів захисту, своєчасність отримання інформації тощо.

Перераховані вище недоліки дозволяють зробити такі висновки.

1. Неперервний процес забезпечення інформаційної безпеки викликає необхідність забезпечення таких напрямків діяльності:

- виявлення загроз та джерел їх виникнення;
- захист інформації від різних загроз та ефективне управління інформаційною безпекою;
- забезпечення захисту від негативного інформаційного впливу та упередження несанкціонованих дій конкурентів.

2. Процес проектування та експлуатації захищених інформаційних систем відбувається в

умовах можливих конфліктів.

Мета та задачі дослідження

Актуальність задачі оцінювання та забезпечення комплексної інформаційної безпеки об'єкта дозволяє сформулювати основну задачу дослідження таким чином: розробка методів та математичних моделей для аналізу ймовірностей виникнення інформаційних конфліктів, що виникають у сучасних системах, та розробка методик для їх вирішення з метою зменшення ризиків втрати конфіденційної інформації.

Мета дослідження полягає у розвитку теорії комплексної безпеки складних систем.

Математичні моделі конфліктів у інформаційних системах

Існують різні підходи щодо формалізації конфліктних ситуацій, які можуть виникнути у складних системах:

- підхід, який базується на використанні точних або наближених оптимізаційних методах, які представляють конфлікт;
- підхід, який базується на використанні методів штучного інтелекту у вигляді рішень, що побудовані на основі евристичних знань;
- підхід, який базується на суб'єктно об'єктній моделі системи.

З урахуванням того, що більшість конфліктних ситуацій, які щодо інформаційної безпеки можуть трактуватися, наприклад, як спроба несанкціонованого доступу до інформаційних ресурсів, характеризуються невизначеністю, зокрема, такою як параметрична, процедурна, поведінкова, можна стверджувати, що зняття існуючих невизначеностей на різних етапах життєдіяльності системи досягається комбінацією наведених підходів.

Наприклад, параметрична і процедурна невизначеність може бути знята з використанням класичних методів і теорії нечітких множин, поведінкова з використанням об'єктно-суб'єктних відношень та моделювання нечітких логічних висновків. В цьому випадку можна стверджувати, що ефективність використання того чи іншого підходу або математичного апарату обґрунтовується такими факторами: наявність або відсутність достатньої точної інформації щодо системи, представлення (тип або форма) вхідної і вихідної інформації, етап життєдіяльності самої системи тощо.

Наприклад, інформаційні ресурси, що захищаються, доцільно розглядати як об'єкти системи, а дії, які виконуються над ресурсами, у тому числі і дії, що можуть бути розцінені як небажані, наприклад, несанкціонований доступ, можуть бути представлені як суб'єктна складова системи. Дії, які відбуваються в системі суб'єкт-об'єкт, за певних умов можуть привести до виникнення конфліктних ситуацій. Тут доречно навести аксіому, яка покладена в основу американського стандарту із захисту інформації. Формулюється вона таким чином: питання безпеки формалізується діями суб'єктів відносно об'єктів.

У загальному вигляді математична модель об'єкта взаємодії з урахуванням того, що його необхідно захищати, можна охарактеризувати, наприклад, такими параметрами [2]:

$$O = \{O_s, O_r, O_x, ..., t\}, \quad (1)$$

де O_s – стан системи (захищений або незахищений), O_r - ресурси системи, O_x - швидкодія роботи системи, t - реальний час. В реальному випадку для ідентифікації об'єкта, який захищається, можна використовувати і інший набір параметрів, які є найбільш значущі для даного випадку. Суб'єкт системи характеризується такими параметрами:

$$S = \{S_m, S_r, S_z, S_d, ..., t\}, \quad (2)$$

де S_m – мета суб'єкта, S_r – ресурси суб'єкта, S_z – засоби суб'єкта, S_d – дії суб'єкта, t – реальний час. Аналіз наведених параметрів суб'єкта системи дозволяє сформулювати твердження.

Твердження. Дії суб'єкта S_d завдяки використання його ресурсів S_r та засобів S_z з урахуванням мети S_m можуть привести до виникнення конфліктної ситуації, яка може трактуватися як порушення інформаційної безпеки.

Розвиток загальної теорії безпеки полягає у створенні узагальнених взаємопов'язаних положень та залежностей між складовими комплексної безпеки, такими як техногенна, економічна, екологічна тощо. Наприклад, розвиток методів та засобів для здійснення

несанкціонованого доступу до інформаційних ресурсів обґрунтовується бажанням реалізації ефективного доступу до інформаційних ресурсів, які акумулюють певну корпоративну інформацію. Реалізація цього несанкціонованого доступу приведе до збільшення ризиків економічної, екологічної, техногенної безпеки, створенню несприятливих умов для подальшого функціонування об'єкта захисту. Особливу актуальність рішення питання оцінювання та забезпечення комплексної безпеки набуває тоді, коли об'єктивною є залежність: безпека підприємства - безпека (галузі) регіону - безпека держави.

Інтегральною характеристикою захищеності об'єкту є політика інформаційної безпеки (ПІБ), яка повинна підтримувати необхідний рівень захищеності у часі, тобто враховувати динамічний характер як небезпек, так і механізмів захисту. В узагальненому вигляді рішення сформульованої задачі дослідження можна представити у вигляді структурної схеми реалізації комплексної безпеки, яка представлена на рис. 1.

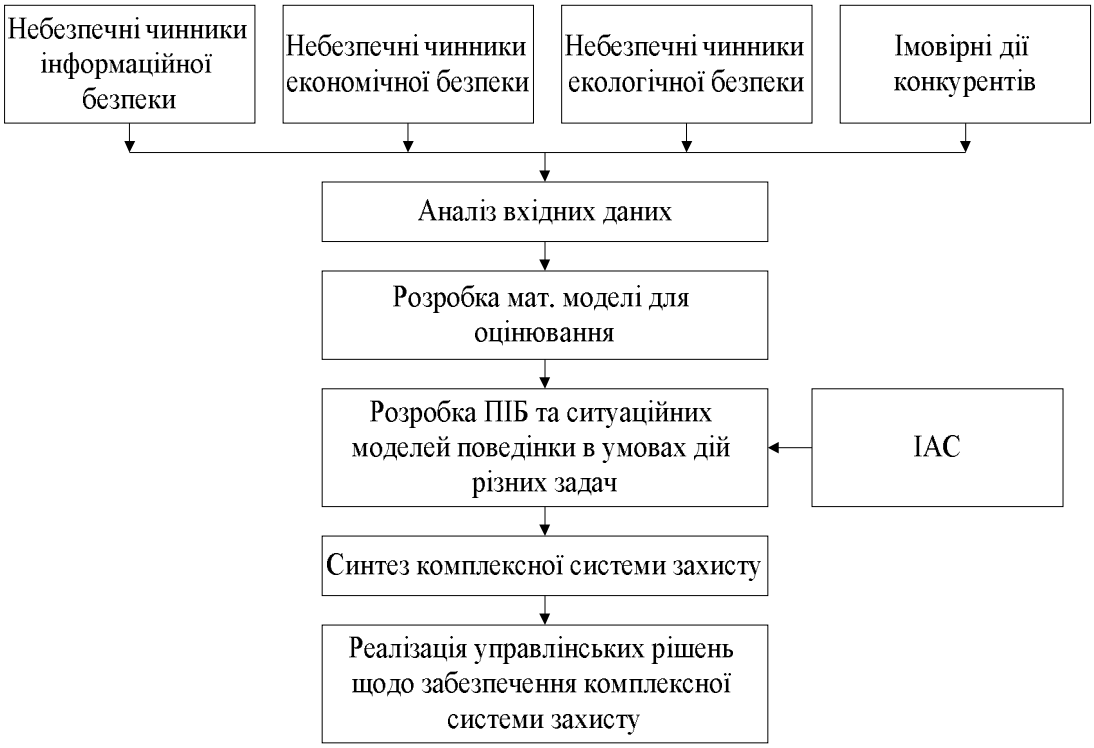

Рис. 1. Структура реалізації комплексної безпеки

Разом із врахуванням небезпечних, як внутрішніх так і зовнішніх чинників, вхідними параметрами для розробки ефективної ПІБ є певні вказівки та замовлення служби безпеки та її підрозділу інформаційно-аналітичної служби (ІАС). Це повністю об'єктивний процес, оскільки служба безпеки підприємства в більшості випадків є замовником ПІБ.

Ефективність системи, яка знаходиться у стані конфлікту, залишається основним показником працездатності системи. Оцінку ефективності функціонування можна оцінити, якщо визначити значення, наприклад, у абсолютному вигляді [3]:

$$E_i = | W_i - X_i | \qquad (3)$$

де X_i - поточне значення рівня захищеності, W_i - значення, яке необхідно досягти.

Знаходження E_i у певних межах означає, що ефективність функціонування системи достатня. В якості прикладу можна обрати сценарій, який демонструє дії потенційного порушника, що спрямовані на несанкціонований доступ до інформаційних ресурсів і таким чином викликає конфлікт. На рис.2 представлена структура системи, у якій виникає подібний конфлікт.

Загальний підхід [3] дозволяє подану структуру представити у вигляді узагальненої моделі

$$Y := F : X , \qquad (5)$$

де $Y = \{y_1, y_2, \ldots, y_m\}$ - вихідна реакція системи, $X = \{x_1, x_2, \ldots, x_n\}$ - множина факторів, які

впливають, $F = \{F_1,F_2,\ldots,F_j\}$ - множина операторів, які реалізує система.

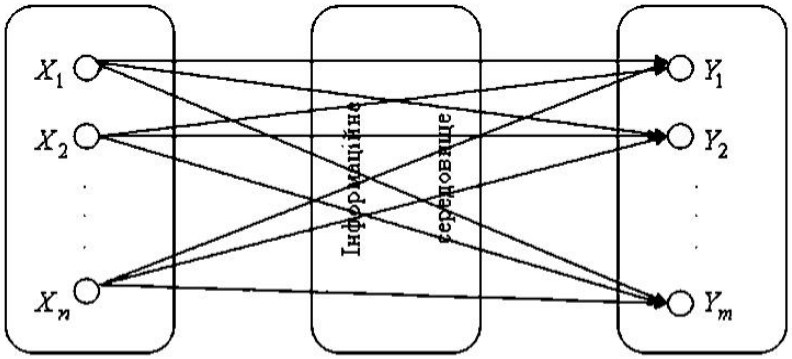

Рис. 2. Узагальнена структура системи з виникненням конфлікту

З урахуванням існування множини T існуючих загроз і множини M механізмів захисту узагальнену модель можна представити у вигляді:

$$F_j(t, A) : X(t, A) \rightarrow y_i(t - t_0, A), \tag{6}$$

де $A = \{\alpha_1,\alpha_2,\ldots\alpha_k\}$ - множина факторів, які генеруються множиною загроз T, і яким відповідно протиставляються механізми захисту M.

З урахуванням розв'язку головної задачі – забезпечення необхідного рівня захищеності ефективність функціонування даної системи можна представити:

$$\sum_{i=1}^{n} (\| Y_{Ei} - F : X(T \times M) \|) \le E_i \ , \tag{7}$$

де Y_{Ei} - множина еталонних реакцій системи на i-й тип небезпеки, E_i - множина меж порогів i-безпеки системи.

З точки зору забезпечення необхідного рівня безпеки і стійкого функціонування системи загальна постановка може бути представлена у вигляді оптимізаційної задачі:

$$\sum_{i=1}^{n} \left(\max_{A} \left\| Y_E - F : X(T \times M) \right\| \right) \rightarrow \min \tag{8}$$

Відповідно до існуючих вимог сучасні методики для оцінювання рівня безпеки та системи захисту інформації мають будуватися на базі математичних моделей, за допомогою яких теоретично обґрунтовується і практично реалізується відповідність системи захисту і політики безпеки.

Реалізація представленої структури на рис.1 у практичній площині дозволяє вирішувати задачу, яка формалізована виразами (7) та (8), або іншими словами забезпечити необхідний рівень безпеки системи. Рішення двох задач забезпечення необхідного рівня безпеки формалізується таким чином. Рішення першої задачі, тобто оцінювання та забезпечення необхідного рівня захищеності, на етапі проектування системи представлено у [4]. Результатом розв'язку першої задачі є розроблена політика інформаційної безпеки та синтезована, оптимальна за певними показниками система захисту інформації.

На етапі експлуатації для організації комплексного захисту і ефективної протидії потенційним порушникам або конкурентам прийняття управлінських рішень щодо забезпечення ефективного функціонування об'єкту захисту повинні ґрунтуватися на результатах повного аналізу і оцінювання, існуючих і потенційних загроз. Рішення цієї задачі ускладнюється у зв'язку із суттєвою невизначеністю, яка пов'язана із динамічною природою всіх елементів системи. У зв'язку з цим є доцільною організація в структурі служби безпеки об'єкта захисту спеціальної ІАС, яка повинна забезпечити впорядковане накопичення, науково обґрунтоване узагальнення і аналіз інформації відносно різних напрямів, що впливають на захист конфіденційної інформації, і на цій основі - вироблення прогнозу з подальшого розвитку подій, їх можливий вплив на стійкість і життєспроможність об'єкту захисту.

Розв'язок другої задачі виконується у площині організаційного захисту і передбачає цілу низку заходів, таких як організація служби безпеки, інформаційно-аналітичної служби тощо. Формалізація рішення другої задачі ускладнюється такими проблемами:

1. Розв'язок задач забезпечення конфліктностійкої взаємодії об'єкту захисту із зовнішнім

середовищем здійснюється в широкому просторово - тимчасовому діапазоні, і воно ґрунтується на парируванні множини способів протидії, що розширюється, з боку конкурентів.

2. Більшість рішень щодо оцінювання і управління безпекою приймаються в умовах обмежень в часі і високій мірі невизначеності, пов'язаної з неоднозначністю цілей, критеріїв, способів дій і результатів їх наслідків з боку конкурентів.

3. Вміст і структура ресурсної взаємодії (ресурсного конфлікту) із зовнішнім середовищем пов'язані з вирішенням «кінцевих» конфліктів. Тому конфліктна стійкість є визначальною властивістю будь-якого об’єкту захисту, що забезпечує можливість протистояти діям зовнішнього середовища. Функціонування інформаційно-аналітичної служби представлено на рис. 3.

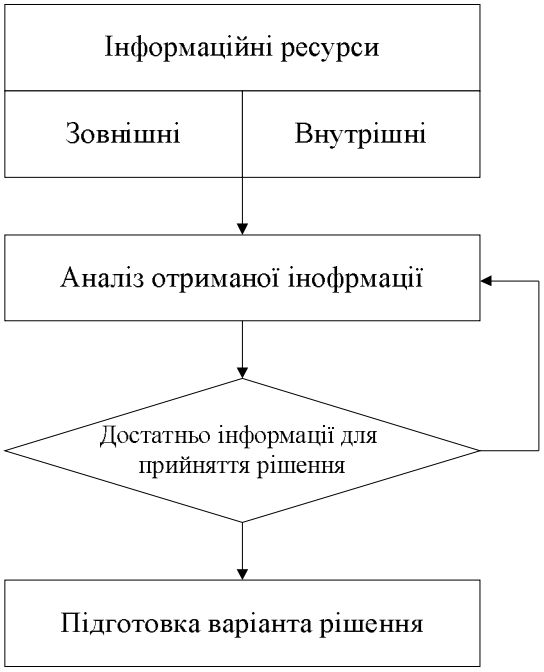

Рис. 3. Структура функціонування ІАС

Для забезпечення стійкості функціонування об’єкту захисту, або для забезпечення його своєчасної адаптивності до змін зовнішніх і внутрішніх чинників, ІАС повинна забезпечити можливість вибору безконфліктних операцій [5]. Залежно від умов взаємодії, пріоритету можливих дій та стану зовнішнього середовища пропонується така методика для практичної реалізації безконфліктних операцій:

1. Визначається множина можливих дій в межах відносин об’єкт - суб’єкт D_s та *Do* і аналізується їх можливий вплив або ранг на об’єкт захисту, де D_s - множина можливих операцій суб’єкта, а *Do*- множина можливих операцій об’єкта.

2. Аналіз рангів можливих дій дозволить визначити підмножину операцій, які не приводять до виникнення конфлікту. Це забезпечує формування безконфліктної множини операцій $D'_s(\overline{K}_o) \subset D_s$, де $D'_s(\overline{K}_o)$ - множина безконфліктних операцій.

3. На підставі аналізу відповідних показників вибір раціональної операції D'_S з множини $D'_s(\overline{K}_o)$ відбувається за варіантом $D'_s = \min\limits_{DD'_s(\overline{K}_o)}(R)$, де R – це ймовірне значення ризику операції, що обрана.

Реалізація запропонованої методики роботи ІАС представлена на рис.4. у вигляді структурної схеми системи захисту інформації, що реагує на виникнення конфліктної ситуації.

Результат рішення другої задачі захисту власних інформаційних ресурсів, спрямованих упередити дії ймовірних конкурентів і нейтралізацію їх поточних ресурсів, можливих дій та зміни мети. Досягається це завдяки рішенню таких задач і забезпеченню керівництва об’єктивною і своєчасною інформацією про наміри конкурентів, їхні сильні та слабкі сторони, збір та узагальнення даних, які дозволять вплинути на позицію конкурентів, наприклад, у ході переговорів, моніторинг та контроль процесу виконання певних договорів, оцінювання та

управління ризиками тощо.

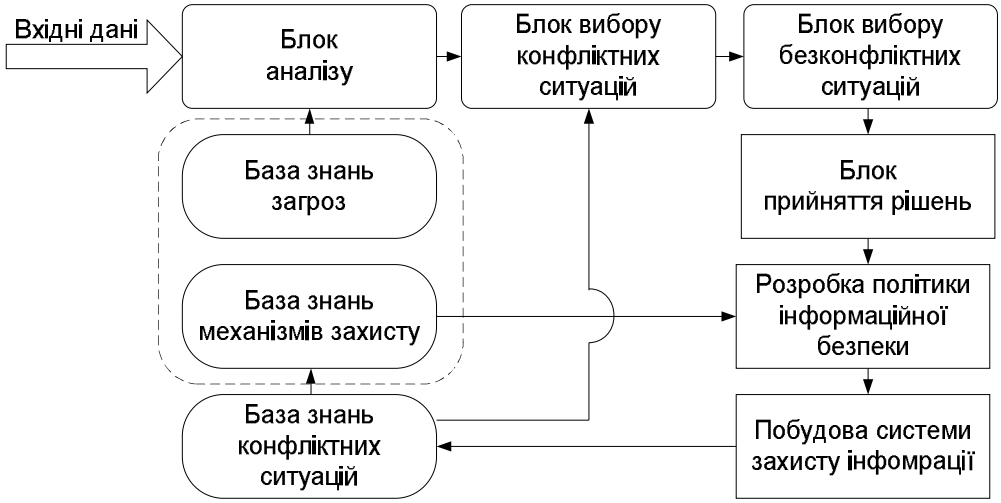

Рис. 4. Структурна схема СЗІ, що реагує на виникнення конфліктної ситуації

Рішення поставленої задачі оцінювання і забезпечення комплексної безпеки в більшості випадків може супроводжуватися невизначеністю, що суттєво підвищує ризик. Невизначеність може бути викликана неточністю, неповнотою або відсутністю інформації. У цьому випадку формалізація процесу відбувається з використанням так званих експертних оцінок, які формалізуються за допомогою теорії нечітких множин.

Висновки

Оцінювання та забезпечення інформаційної безпеки – складний процес, який вимагає прийняття відповідних рішень, як на етапі проектування так і на етапі експлуатації системи захисту інформаційних ресурсів.

В статті представлена методика отримання оптимальної системи захисту інформаційних ресурсів на етапі проектування та методику, що дозволяє формалізувати діяльність інформаційно-аналітичної системи на етапі експлуатації СЗІ. Це надає можливості отримати ефективну політики інформаційної безпеки підприємства, яка має важливу властивість враховувати можливі зміни, як внутрішніх так і зовнішніх чинників, зокрема конфліктні ситуацій, що впливають на рівень безпеки об’єкту захисту.

Список літературних джерел

1. Завгородний В.И. Комплексная защита информации в компьютерных системах. – М.: ЛОГОС, 2001.– 264 с.

2. Дудатьєв А.В. Аналіз та забезпечення комплексної інформаційної безпеки в умовах інформаційних війн та конфліктів//Вісник Східноукраїнського національного університету ім. Даля. – 2009. - №6(136). – Ч1. – С. 64-71.

3. Остапенко Г.А. Информационные операции и атаки в социотехнических системах. М.: Горячая линия – Телеком, 2007. – 134 с.

4. Дудатьєв А.В. Розробка уніфікованих моделей системного проектування оптимальних систем захисту інформаційних ресурсів //Вісник ЧДТУ.- 2008.- №1.-С.3-8.

5. Ярочкин В.И., Бузанова Я.В. Корпоративная разведка. – М.: Ось-89, 2008. – 304 с.