УДК 621.391.7

СТРУКТУРА СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕННЯ ПРОЦЕСУ УПРАВЛІННЯ ЗАХИСТОМ ІНФОРМАЦІЇ

Михайло Єсаулов, Поліна Калатенко
ВІТІ НТУУ "КПІ"

Анотація: **Розглянуті питання визначення структури системи підтримки прийняття рішення процесу управління захистом інформації, що базується на адаптивній моделі системи інформаційної безпеки.**
Summary: **Considered questions of determination of structure of the system of support of decision-making process management defense of information which is based on the adaptive model of the system of informative safety.**
Ключові слова: **Система інформаційної безпеки, система захисту інформації, адаптивний захист, системи управління, система підтримки прийняття рішення.**

Вступ

Ефективне забезпечення захисту в інформаційно-телекомунікаційних системах (ІТС) можливо тільки на основі комплексного використання всіх відомих методів і підходів до рішення даної задачі. Концепція такого комплексного захисту має задовольняти наступній сукупності вимог. По-перше, мають бути розроблені й доведені до рівня регулярного використання всі необхідні механізми гарантованого забезпечення необхідного рівня захищеності інформації. По-друге, мають існувати механізми практичної реалізації необхідного рівня захищеності інформації. По-третє, необхідно мати в своєму розпорядженні засоби раціональної реалізації всіх необхідних заходів щодо захисту інформації на базі досягнутого рівня розвитку науки й техніки. І, нарешті, по-четверте, мають бути розроблені способи оптимальної організації й забезпечення проведення всіх заходів щодо захисту в процесі обробки інформації. Побудова систем захисту інформації (СЗІ) полягає в тому, щоб для заданої ІТС (або її проекту) створити оптимальні механізми забезпечення захисту й механізми управління ними. При цьому під оптимальністю СЗІ розуміється або досягнення заданого рівня захищеності інформації при мінімальних витратах, або досягнення максимально можливого рівня захищеності при заданому рівні витрат. Отже, питанням управління системою захисту інформації має приділятися певна увага. Тому метою статті є визначення структури системи підтримки прийняття рішення процесу управління системою захисту інформації.

І Аналіз підходів до побудови систем інформаційної безпеки

Побудова системи інформаційної безпеки (СІБ) здійснюється з урахуванням статистичних даних про вже існуючі загрози. Проте, в процесі функціонування системи захисту множина загроз може принципово змінитися. Зокрема, це пов'язано з тим, що багато загроз припускають знаходження порушниками помилок в реалізації системних і прикладних засобів, які можуть бути невідомі на момент створення системи інформаційної безпеки, але мають бути враховані в процесі її функціонування [1,2]. Тому проектування системи інформаційної безпеки – процедура ітераційна, яка в загальному випадку припускає наступні етапи:

- проектування первинної системи захисту (початковий варіант);
- аналіз захищеності на основі статистичних даних, отриманих в процесі експлуатації системи захисту;
- модифікація ,,вузьких місць" системи захисту (налагодження/заміна/доповнення окремих механізмів захисту інформації).

Після модифікації ,,вузьких місць" відбувається повернення до експлуатації системи захисту й накопичення статистичної інформації.

Класифікація можливих підходів до побудови систем інформаційної безпеки представлена на рис. 1.

Альтернативні підходи складають метод необхідного мінімуму й метод повного перекриття. Метод необхідного мінімуму полягає в пошуку варіанту побудови системи за характеристикою необхідного рівня захищеності. Метод повного перекриття полягає в початковій реалізації надмірності механізмів, що спочатку дозволяє побудувати систему захисту з великим запасом в характеристиці захищеності. Дані підходи характеризуються наступними недоліками. Метод необхідного мінімуму з урахуванням специфіки функціонування даного класу систем дозволяє побудувати систему практично без запасу захищеності, що зажадає її достатньо швидкого проектування наново. Метод повного перекриття пов'язаний з істотними втратами, перш за все в продуктивності системи.

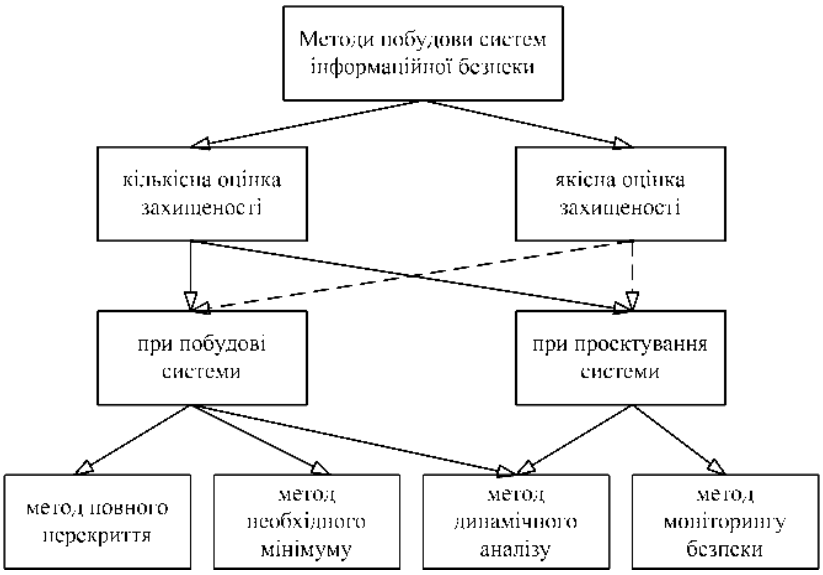

Рисунок 1 – Класифікація методів проектування систем інформаційної безпеки

Найбільш обґрунтованим підходом до побудови систем досліджуваної області є метод динамічного аналізу [1]. Суть цього методу полягає у виконанні наступних дій.

Виходячи з можливих витрат на систему захисту, вибирається варіант, що забезпечує максимальний рівень захищеності (за умови, що він не нижче потрібного). Причому це робиться в рамках заданих обмежень на параметр продуктивності. Потім, в рамках вибраного варіанту, визначається набір механізмів захисту й їх параметри, які мають бути включені для забезпечення необхідного рівня захищеності. Решта механізмів знаходиться в резерві – вимкнені. При впровадженні в систему включаються лише необхідні механізми, але система володіє резервом в захищеності, який може поступово вибиратися при зниженні рівня захищеності.

В процесі функціонування системи збирається необхідна статистика про параметри системи (реалізується метод статистичної оцінки), з використанням якої безперервно оцінюється рівень захищеності. При зниженні рівня захищеності нижче заданого необхідного значення включаються надмірні механізми захисту, що дозволяє підтримувати необхідний рівень захищеності протягом деякого часу функціонування системи.

Таким чином, особливістю методу динамічного аналізу є те, що створюється деякий запас в механізмах захисту, який забезпечує рівень захищеності вищій за необхідний на даний момент. Разом з тим, дані механізми при впровадженні системи захисту в експлуатацію спочатку не використовуються. Вони знаходяться в резерві.

В результаті використання надмірних механізмів в системі захисту дозволяє реалізувати необхідний рівень захищеності без додаткового зниження продуктивності. Це за суттю й відрізняє даний підхід від методу повного перекриття. При зниженні ж рівня захищеності нижче необхідного порогу (виявленні нових загроз) підключатимуться надмірні механізми захисту. Активація надмірних механізмів захисту, які при цьому стають основними, призводить до відповідного зниження продуктивності системи. Проте треба відзначити, що включення з резерву нових механізмів може привести до доцільності відключення деяких задіяних механізмів на підставі часткового дублювання виконуваних ними функцій. В результаті це дозволить мінімізувати вплив системи захисту на продуктивність об’єкту, що захищається.

Найважливішою вимогою до реалізації описаного методу є безперервна оцінка захищеності системи, тобто тут має бути реалізована система моніторингу захищеності, що вирішує наступні завдання:

- безперервний збір статистики й розрахунок поточних значень параметрів захищеності;
- оцінка рівня захищеності системи і його порівняння з поріговим значенням.
- визначення рекомендацій з включення зарезервованих механізмів захисту при зниженні поточного рівня захищеності нижче порігового значення.

Визначення рекомендацій здійснюється на основі порівняння можливих варіантів захисту. При цьому варіанти розрізняються набором механізмів, що включаються, а параметри захищеності визначаються вже на підставі зібраної статистики про конкретну систему.

II Адаптивна модель системи інформаційної безпеки

Аналіз дає можливість зробити висновок, що велика група методик оцінки захищеності систем інформаційних технологій базується на наявності певного набору засобів й механізмів захисту, методик виготовлення, експлуатації й тестування та дозволяють віднести той або інший пристрій або систему інформаційних технологій до одного з дискретних рівнів захищеності відповідно до використовуваних в даній країні стандартів.

Огляд публікацій за даною тематикою [3 – 9] показав, що оцінки відображають статичний стан об'єкту захисту виходячи з наявних механізмів захисту, не враховують дійсну завантаженість цих механізмів захисту щодо нейтралізації наслідку загроз, динаміку зміни множини загроз, можливість адаптації системи захисту інформації до зміни множини загроз, не дають вказівок на зміну складу механізмів захисту та структури багаторівневої СІБ.

Розвиток інформаційно-телекомунікаційних систем відбувається в напрямі створення інтелектуальних засобів з елементами самоорганізації, в яких присутні процеси зародження, адаптації та розвитку.

Модель адаптивного захисту використовує принцип біосистемної аналогії, зокрема, ієрархію системи захисту інформаційних процесів і ресурсів в біологічній системі, згідно з якою на нижніх рівнях ієрархії задіяні механізми імунної системи, а на верхніх – механізми адаптивної пам'яті й накопичення життєвого досвіду нервової системи [10].

Розглянемо адаптивну модель СІБ, в якій реалізована динамічна перебудова багаторівневої моделі СЗІ інформаційно-телекомунікаційної системи. Системний підхід до проектування багаторівневої моделі СЗІ відображається на змісті етапів життєвого циклу системи інформаційної безпеки [11].

На першому етапі життєвого циклу створюється коректна (без несанкціонованих можливостей) інформаційно-безпечна ІТС, тобто формується загальне інформаційне поле захищеної системи – множина функцій ІТС та множина функцій захисту. Багаторівнева модель системи захисту інформації ІТС відповідає мінімальній активації потенційних механізмів захисту й повноті множини відомих загроз.

Метою другого етапу життєвого циклу є коректне виконання системою заданих функцій. Використовується механізм адаптації для реагування на зміну зовнішніх чинників – відбувається збільшення, самонавчання й зміна загального інформаційного поля ІТС та СІБ. Багаторівнева модель системи захисту інформації динамічно поповнюється шляхом переходу механізмів захисту із статусу „потенційний" в статус „активований" і прив'язки активованого механізму до відповідного рівня моделі СЗІ. Збільшується число елементів в підмножині заданих загроз як за рахунок включення елементів з множини відомих загроз, так й за рахунок поповнення самої множини відомих загроз раніше невідомими. Можливе розширення множини потенційних механізмів захисту за рахунок опису й подальшої реалізації раніше відсутніх механізмів захисту.

На третьому етапі життєвого циклу відбувається згортання прикладних функцій системи ІТС при коректній роботі СІБ. Багаторівнева модель інформаційної безпеки системи ІТС містить накопичений досвід нейтралізації механізмами захисту вразливості системи та характеризується максимальною повнотою множини відомих загроз.

Основними механізмами реалізації адаптивних СІБ є: нечіткий логічний висновок, який дозволяє використовувати досвід експертів в області інформаційної безпеки у вигляді системи нечітких предикативних правил для попереднього навчання системи, здатність адаптивних СІБ до класифікації й кластеризації та здатність адаптивного розподіленого інформаційного поля системи до накопичення знань в процесі навчання.

Адаптивна модель системи інформаційної безпеки (рис. 2) в ІТС характеризується наступними атрибутами:

- система інформаційної безпеки є багаторівневою ієрархічною структурою, що використовує експертні оцінки для внесення апріорного досвіду у вигляді системи нечітких предикативних правил;
- еволюційний характер СІБ забезпечується адаптивними властивостями нечітких нейронних мереж, що реалізують систему нечітких предикативних правил.

Рисунок 2 – Адаптивна модель системи інформаційної безпеки

Внизу ієрархії СІБ вирішується завдання класифікації/кластеризації загроз безпеки за сукупністю ознак, що носять неповний і не цілком достовірний характер. Тобто, нейронна мережа нижнього рівня СІБ, виходячи з досвіду експертів з інформаційної безпеки (ІБ), реалізує систему нечітких правил, яка описує процес логічного виведення отримання висновку (тип загрози), використовуючи як нечіткі посилки вектори вхідних ознак.

На нижніх рівнях ієрархії використовують апаратно-програмні засоби ідентифікації атак, у тому числі й нейромережні. Завдання нечіткої класифікації успішно вирішується із застосуванням теорії нечітких множин і ідентифікації. Якщо достовірність класифікації за відомими загрозами менша деякого значення, то за наявності ознак атаки класифікація розширюється за рахунок введення нової градації в класифікацію – вирішується завдання кластеризації загроз. Кластеризація розширює систему предикатних правил відповідних ешелонів багаторівневої СІБ, оскільки класифікується раніше невідома загроза.

На середніх рівнях ієрархії СІБ для кожного рівня багаторівневої СЗІ засоби захисту інформації використовують результати класифікації нижніх рівнів ієрархії у вигляді посилок системи нечітких предикатних правил для формування висновків – відповідностей „загрози – механізми захисту”. Тобто вирішується завдання класифікації механізмів захисту (нечіткі висновки) за вектором нечітких ознак загроз, для нейтралізації наслідків яких дані механізми захисту призначені.

Іншими словами, для кожного рівня багаторівневої СЗІ, використовуючи результати нечіткої класифікації (тип загрози) як посилки, системою нечітких правил описується відповідність „загрози – механізми захисту” виходячи з досвіду експертів ІБ. Нейромережа даного рівня СІБ після навчання буде відображати достовірність нейтралізації заданого в окремому правилі набору загроз відповідним механізмом захисту даного рівня багаторівневої СЗІ. Якщо при збільшенні розмірності вектора ознак загроз після навчання

нейромережі достовірність класифікації по механізмах захисту (активність механізмів захисту окремих рівнів) менше деякого значення, то при наявності ознак атаки класифікація механізмів захисту розширюється за рахунок введення нової градації в класифікацію – завдання кластеризації механізмів захисту.

Після навчання нечіткої нейромережі відповідного рівня аналіз нечіткого правила за знов введеним механізмом захисту дозволяє сформулювати специфікацію на механізм захисту, що відсутній. Для кожного рівня багаторівневої СЗІ на основі експертних оцінок для кожної загрози доцільно сформувати лінгвістичні змінні „частота реалізації загрози" й „потенційний збиток".

Верхній рівень ієрархії СІБ необхідний для узагальнення результатів (посилок) у вигляді активності механізмів захисту, частоти реалізації й збитку від загрози з метою формування системи нечітких предикативних правил – висновків про доцільність розширення складу активованих механізмів захисту за окремими рівнями СЗІ. Активація механізмів захисту проводиться, якщо інтегральні оцінки, що враховують величину потенційного збитку, частоту реалізації загрози й достовірність нейтралізації загрози даним механізмом захисту, перевищують задані порогові значення.

Застосування моделі адаптивного захисту, заснованого на принципі біологічної аналогії [10] і, зокрема, ієрархічної організації СЗІ дозволяє:

– забезпечити близьке до оптимального співвідношення „вартість/ефективність" СІБ за рахунок поступового наповнення багаторівневій моделі ІБ тільки необхідними механізмами захисту;
– у динаміці відстежувати найбільш задіяні механізми захисту при зміні множини загроз;
– формувати специфікацію вимог на механізми захисту, що відсутні в системі;
– оцінювати захищеність системи ІТС через величини відносного збитку й інтегральні показники активності розподілених за структурою СЗІ механізмів захисту.

III Структура системи підтримки прийняття рішення процесу управління захистом інформації в ІТС

Результати проведеного аналізу свідчать про те, що дійсно ефективне забезпечення захисту інформації в інформаційно-телекомунікаційних системах можливе лише на основі комплексного використання всіх відомих методів і підходів до вирішення даної проблеми.

Відомо, що забезпечення надійного захисту інформації не разовий захід, а сукупність різних заходів, здійснюваних як під час розробки, так і при експлуатації інформаційно-телекомунікаційних систем.

На основі аналізу розвитку концепції захисту інформації неважко зробити висновок про те, що має місце тенденція постійного зростання зусиль, які вкладаються в захист, вдосконалення підходів до захисту й самих механізмів захисту. Проте слід зазначити й той факт, що традиційна архітектура ІТС і технологія автоматизованої обробки інформації не забезпечує всіх умов, необхідних для надійного захисту інформації.

Розглянемо типову структуру системи захисту ІТС. В системі захисту інформації кожному класу засобів і заходів захисту визначається своє завдання, у зв'язку з чим ряд засобів і заходів об'єднуються в підсистеми, які вирішують строго визначені завдання, але при цьому дотримуються мети створення СЗІ і принципів її побудови [12].

Типова СЗІ (рис. 3) може мати наступну структуру (хоча необхідно відзначити, що в реальній ситуації конфігурація може змінюватися, а принципи розбиття СІБ на підсистеми можуть також відрізнятися від викладених):

– підсистема технічного захисту інформації;
– підсистема захисту інформації в автоматизованих системах;
– підсистема нормативно-правового та організаційного захисту інформації;
– підсистема контролю та реєстрації подій безпеки (залежно від масштабів і складності побудови ІТС дана підсистема може розбиватися на окремі складові);
– підсистема криптографічного захисту інформації;
– підсистема технологічного захисту інформації;
– підсистема управління.

Одним з основних підходів до проблеми захисту інформації є положення про те, що в сучасних і перспективних ІТС ефективний захист інформації не може бути забезпечений простим включенням до складу системи деяких механізмів і пристроїв захисту – захистом інформації необхідно постійно керувати [13].

Управління захистом інформації є складною сукупністю взаємозв'язаних процесів безперервного створення, вдосконалення й контролю над системою механізмів захисту, які використовуються в ІТС. При цьому важливою є та обставина, що підсистема управління захистом інформації є сукупністю однорідних у

функціональному відношенні заходів, регулярно здійснюваних в ІТС з метою створення, підтримки й забезпечення умов, об'єктивно необхідних для забезпечення надійного захисту інформації необхідного рівня.

Під *рівнем захищеності інформації* розуміється відношення поточного значення показника захищеності інформації, що дійсно має місце, до необхідного значення відповідного показника. На основі оцінки цього відношення приймається управлінське рішення щодо використання засобів захисту.

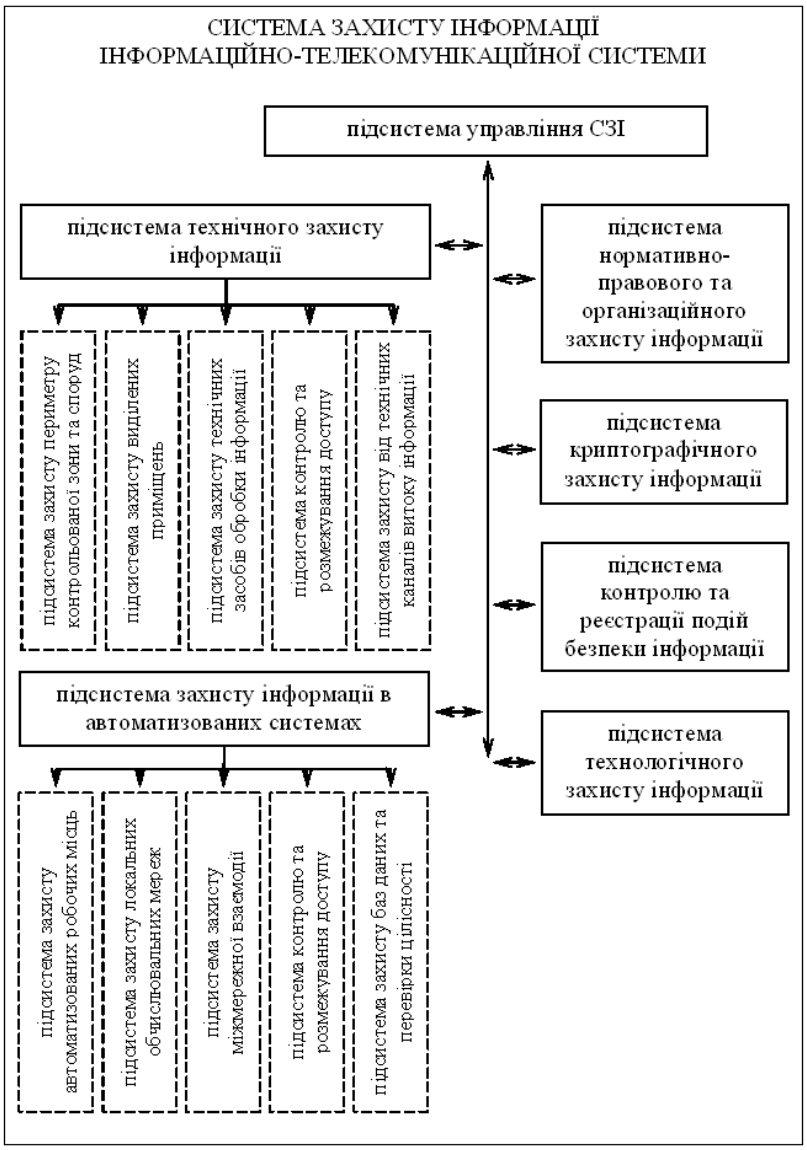

Рисунок 3 – Структура системи захисту ІТС

Відповідно до основного посилання про необхідність постійного управління захистом інформації (рис. 4) всі процеси управління поділені на два напрямки: управління створенням механізмів захисту, управління й контролю використанням механізмів захисту.

При такому підході очевидною є та обставина, що названі процеси мають бути регулярними, постійно керованими, причому управління має здійснюватися з метою досягнення максимального рівня захисту при відповідних мінімальних, в порівняні з цінністю інформації, витратах сил і засобів.

Відповідно до необхідних показників захищеності мають бути визначені оптимально достатні набори засобів захисту (технічних, програмних, організаційних, криптографічних та інших), що забезпечують необхідний рівень захищеності. Обгрунтування таких наборів засобів захисту є загальним завданням механізмів управління засобами захисту.

Обгрунтування вимог до захисту інформації є першочерговим і основоположним завданням розробки систем захисту, оскільки результати її рішення складають початкову базу для вирішення всіх подальших

завдань. В той же час, завдання обґрунтування вимог до побудови підсистеми управління СЗІ може вирішуватися неформальними методами, оскільки формальні методи об'єктивного обґрунтування вимог відсутні й можливості їх розробки для всіх випадків практичного застосування проблематичні.

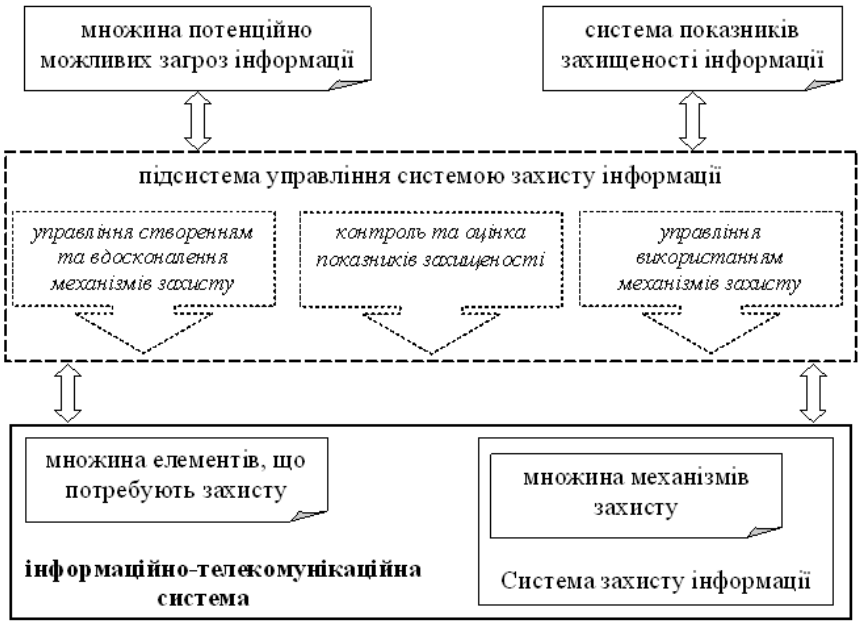

Рисунок 4 – Узагальнена схема процесів управління захистом

Враховуючи той факт, що управління захистом інформації є окремим випадком управління в системах організаційно-технологічного типу, процес проектування СЗІ спрощується, оскільки для цього досить трансформувати загальні положення концепції управління в системах вказаного типу на проблеми управління захистом інформації. Для систем організаційно-технологічного типу повну множину складають наступні чотири функції управління:

– планування, тобто розробка раціональної програми майбутніх дій;

– оперативно-диспетчерське управління, тобто регулювання швидкоплинних процесів в реальному масштабі часу;

– календарно-планове керівництво, тобто періодичний контроль виконання плану й прийняття (при необхідності) управлінських рішень;

– забезпечення повсякденної діяльності системи управління, тобто надання органам цієї системи ресурсів, необхідних для ефективного управління.

Надійний захист інформації в ІТС може бути ефективним лише в тому випадку, якщо він буде виконуватися для всіх елементів системи, що потребують захисту з боку множини потенційно можливих загроз, при постійному контролі показників рівня захищеності системи [14]. Для визначення рівня захищеності має здійснюватися відповідний контроль, на основі якого визначаться показник рівня захищеності. Основними характеристиками контролю є: повнота контролю, кількість охоплюваних контролем елементів системи, час і періодичність проведення контролю, послідовність контрольних операцій, які проводяться, режим проведення контролю, ступінь автоматизації контрольних операцій, аналіз і оцінка ходу виконання контролю механізмів захисту з метою своєчасного й правильного ухвалення рішення.

Повнота контролю передбачає, що всі процедури обробки інформації, яка захищається, мають контролюватися системою захисту в повному об'ємі, причому основні результати контролю мають фіксуватися в спеціальних реєстраційних журналах.

На основі даних контролю визначається показник дійсного рівня захищеності системи. Цей показник зіставляється з необхідним рівнем захисту й якщо різниця вказаних показників перевищує допустимий поріг, то система управління захистом має відреагувати шляхом зміни набору використовуваних засобів захисту або зміною показника необхідного рівня захищеності.

Враховуючи вище вказане відзначимо, що завдання забезпечення управління захистом інформації є комплексним завданням, яке включає наступне [12]:

– збір і аналіз даних за всіма параметрами, що характеризують інформаційну безпеку системи;

– контроль відповідності, стану й правильності функціонування елементів системи, що включає перевірку ідентичності функціонуючих елементів ІТС, в тому числі й елементів СЗІ, перевірку їх стану в контрольований момент часу та відповідності дійсного функціонування елементів елементам заявленим;

– аналіз параметрів зовнішнього середовища, що включає визначення множини загроз, які впливають (або можуть впливати) на безпеку системи в цілому та системи захисту зокрема;

– визначення поточних значень всіх необхідних параметрів;

– визначення та оцінка поточних значень показників захищеності;

– прийняття рішення про використання механізмів захисту й раціональна організація системи захисту інформації;

– обґрунтування оптимально достатніх наборів механізмів захисту;

– прийняття рішення про модифікацію та вдосконалення системи захисту інформації.

Рішення цього комплексного завдання передбачає реалізацію визначеної послідовності заходів: оцінку фактичного стану інформаційної безпеки ІТС, прогнозування стану інформаційної безпеки системи й ступеню впливу загроз і дестабілізуючих чинників, планування системи заходів захисту інформації відповідно до факторів загроз і поточних значень захищеності системи, визначення методів і механізмів забезпечення необхідного рівня захищеності та прийняття рішення щодо управління системою захисту інформації.

Для виконання даних заходів своєчасно та якісно необхідно здійснювати збір, обробку та аналіз інформації про велику кількість факторів, врахувати дану інформацію при прийняті рішення щодо використання й вдосконалення механізмів захисту та управління системою захисту інформації. Ці функції й повинна реалізовувати система підтримки прийняття рішення.

Розглянемо систему підтримки прийняття рішення (СППР) процесу управління захистом інформації в ІТС, яка базується на адаптивній моделі інформаційної безпеки (рис. 5).

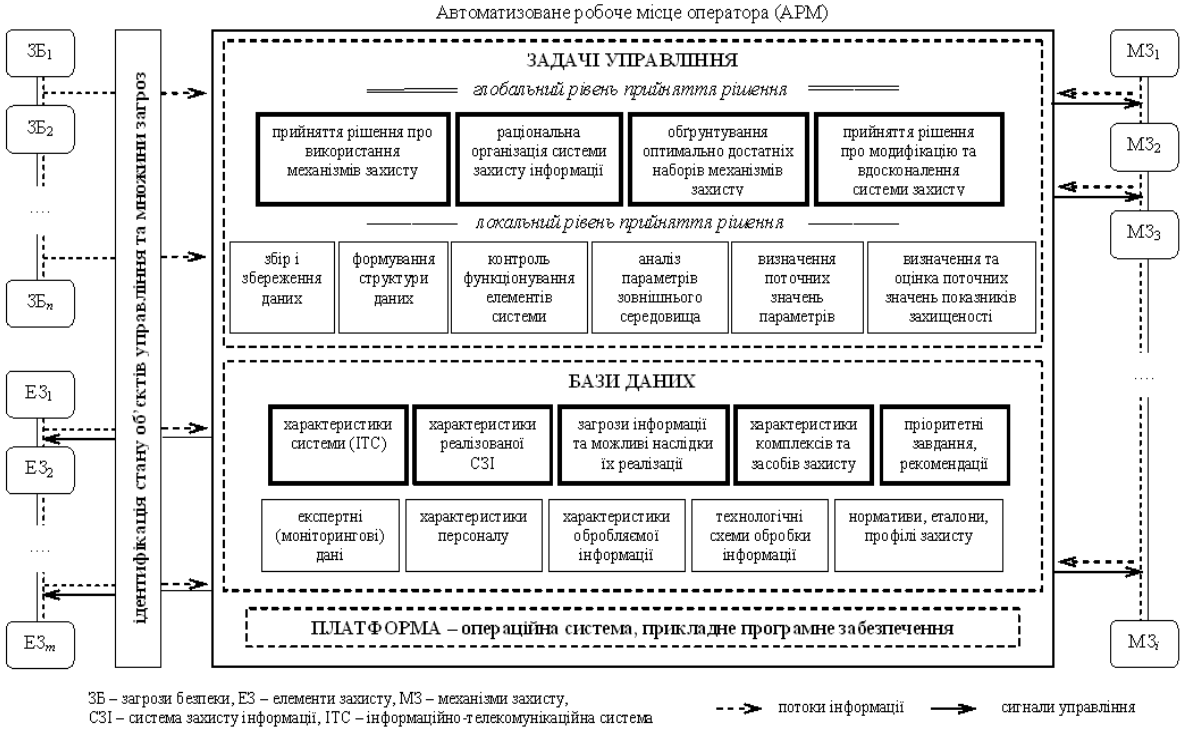

Рисунок 5 – Структура системи підтримки прийняття рішення процесу управління захистом інформації в ІТС

Основні принципи створення системи базувалися на загальних принципах створення автоматизованих систем – системності, розвитку (відкритості), сумісності, стандартизації (уніфікації) й ефективності, – та відповідали основним вимогам до систем підтримки прийняття рішення [15].

Основними вимогами до системи підтримки прийняття рішення підсистеми управління СЗІ є:

1. наявність засобів, які створюють комфортні умови для користувача (посадової особи): діалог, видача рекомендацій в наглядному вигляді, можливість контролю процесу рішення задач;

2. можливість обробки даних на основі як класичних методів прийняття оптимальних рішень, так і методів логічного аналізу неформалізованої інформації, яка закладена в знаннях і досвіді конкретного фахівця з інформаційної безпеки;

3. наявність засобів, які дозволяють користувачу (посадовій особі) використовувати ПЕОМ для виконання робіт, що пов'язані з традиційною обробкою інформації.

Також при побудові даної СППР використовувалися основні підходи до розробки автоматизованих систем, що залежать від мети функціонування: параметри управління розраховуються на весь період управління, управління за впливами, коли зовнішні некеровані фактори заздалегідь відомі до прийняття рішення та управління зі зворотнім зв'язком за станом системи, якщо можливо кількісно виразити стан системи. Перший – при реалізації підсистеми комплексного захисту інформації; другий – при реалізації підсистеми прогнозування; третій – при реалізації підсистеми збору й попередньої обробки інформації та формування управлінських рішень.

В таблиці наведений опис задач управління, а також вхідної інформації, яка необхідна для їх рішення, й вихідної інформації (результатів рішення задач управління).

Таблиця – опис задач управління, вхідної інформації й вихідної інформації

підсистема	вхідна інформація (джерело активізації)	задачі управління	вихідна інформація (результат рішення)
збір та попередня обробка інформації	експертна інформація про об'єкт управління, база знань (методи аналізу, нормативи, еталони, профілі захисту)	збір і збереження даних, контроль відповідності, стану й правильності функціонування елементів системи, аналіз параметрів зовнішнього середовища	бази даних про елементи системи, класи потенційних загроз і вразливостей системи
прогнозування	множина класів потенційних загроз, експертна інформація про значення достовірності нейтралізації загроз та потенційного збитку, база знань (методи розрахунку)	визначення поточних значень всіх необхідних параметрів, визначення та оцінка поточних значень показників захищеності	інтегральні показники захищеності системи
формування управлінських рішень	інтегральні показники захищеності системи, база знань (методи розрахунку, еталони, нормативи)	прийняття рішення про використання механізмів захисту, раціональна організація системи захисту інформації	рекомендації щодо використання механізмів захисту
комплексний захист інформації	інтегральні показники захищеності системи, база знань (методи розрахунку, еталони, нормативи, профілі захисту)	обґрунтування оптимально достатніх наборів механізмів захисту, прийняття рішення про модифікацію та вдосконалення системи захисту інформації	рекомендації щодо вдосконалення системи захисту інформації

Аналіз таблиці дозволяє зробити висновок про необхідність створення баз даних, а також відокремлення двох їх основних груп. До першої групи відносять бази даних, які утворюються стаціонарними джерелами даних і дозволяють активізувати систему й підтримувати її працездатність. Друга група формується динамічними джерелами даних і будується самою системою при обробці експертної (моніторингової) інформації.

Перша група баз даних містить наступну інформацію:

- про загальну структурну схему, склад і характеристики інформаційно-телекомунікаційної системи;
- про характеристики інформації, що обробляється (категорії інформації);
- про технологічну схему обробки інформації в системі;
- про характеристики персоналу (кількість і категорії користувачів);
- про реалізовану систему захисту інформації (функціональний профіль захищеності системи);

– про потенційно можливі загрози інформації, а також можливі наслідки їх реалізації.

Основу другої групи складають моніторингові дані, пріоритетні завдання, рекомендації.

Подальшим напрямком досліджень є визначення структури та змісту основних задач управління, які зазначені в структурі системи підтримки прийняття рішення.

Висновки

Таким чином, визначена структура системи підтримки прийняття рішення процесу управління захистом інформації в ІТС, що базується на адаптивній моделі системи інформаційної безпеки. Це дозволяє реалізацію наступної послідовності заходів: оцінку фактичного стану інформаційної безпеки ІТС, прогнозування стану інформаційної безпеки системи й ступеню впливу загроз і дестабілізуючих чинників, планування системи заходів захисту інформації відповідно до факторів загроз і поточних значень захищеності системи, визначення методів і механізмів забезпечення необхідного рівня захищеності та прийняття рішення щодо управління системою захисту інформації.

Література: ***1.*** *Щеглов А. Ю. Защита компьютерной информации от несанкционированного доступа. – С.Пб., 2004. – 384 с.* ***2.*** *Щеглов А. Ю. Проблемы и принципы проектирования систем защиты информации от НСД. // "Экономика и производство",№ 3 – М.: 2001. – С. 34 – 46.* ***3.*** *Вертузаев М. С., Юрченко О. М. Защита информации в компьютерных системах от несанкционированного доступа. – К., 2001. – 321 с.* ***4.*** *Осовецкий Л., Шевченко В. Оценка защищенности сетей и систем // Экспресс электроника, № 2-3, 2002. – С.20-24.* ***5.*** *Жижелев А. В., Панфилов А. П., Язов Ю. К., Батищев Р. В. К оценке эффективности защиты информации в телекоммуникационных системах посредством нечетких множеств //. Приборостроение. 2003. – Т. 46, № 7. – С. 22-29.* ***6.*** *Карпычев В. Ю., Минаев В. А. Цена информационной безопасности // Системы безопасности. № 5, 2003. – С. 128-130.* ***7.*** *Девянин П. Н. и др. Теоретические основы компьютерной безопасности. – М.: ,,Радио и Связь", 2000. – 352 с.* ***8.*** *Партыка Т. Л., Попов И. И. Информационная безопасность. Учебное пособие. М.: ФОРУМ: ИНФРА-М, 2002. – 368 с.* ***9.*** *Габарчук В., Зинович З., Свиц А. Кибернетический подход к проектированию систем защиты информации. – К.: Киев-Луцк-Любляны, 2003. – 653 с.* ***10.****. Нестерук Г. Ф., Осовецкий Л. Г., Нестерук Ф. Г. Адаптивная модель нейросетевых систем информационной безопасности // Перспективные информационные технологии и интеллектуальные систем, № 3 (15), 2003.– С. 14-16.* ***11.*** *Нестерук Г. Ф., Осовецкий Л. Г., Нестерук Ф. Г. К оценке защищенности систем информационных технологий // Перспективные информационные технологии и интеллектуальные системы. № 1, 2004. – С. 48-54.* ***12.*** *Петров В. А., Компьютерная безопасность. Криптографические методы защиты. – М.: ДМК, 2000. – 448 с.: ил.* ***13.*** *Бриль В. М. К построению рациональной системы управления защитой информации в системах обработки данных. // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. К.: – 2003. – С. 199-201.* ***14.*** *Бриль В. М., Нестеренко С. Д., Шаталюк В. В. Оценка показателей уязвимости информации при несанкционированном доступе. Научный сборник "Защита информации", К.: – 2000. – 156 с.* ***15.*** *Герасимов Б. М., Дивизюк М. М., Субач И. Ю. Системы поддержки принятия решений: проектирование, применение, оценка эффективности. Севастополь. – 2004. – 318 с.*

УДК 004.056

ПРИМЕНЕНИЕ МОТИВАЦИОННО-СТОИМОСТНЫХ МОДЕЛЕЙ ДЛЯ ОПИСАНИЯ ВЕРОЯТНОСТНЫХ СООТНОШЕНИЙ В СИСТЕМЕ «АТАКА-ЗАЩИТА»

Александр Архипов, София Архипова

Национальный технический университет Украины ,,КПИ"

Анотація: **Розглядається методика експертно-аналітичного оцінювання параметрів системи „атака-захист". Методика базується на аналізі витратно-вартісних мотивацій суб'єктів.**

Summary: **The technique of expert-analytical evaluation of parameters of system "attack – protection" is examined. The technique is based on the analysis of expenditure / cost motivations of subjects of this system.**

Ключові слова: **Вартість втрат, витрати на захист, витрати на атаку, ймовірність загрози, ймовірність атаки, експертне-аналітичне оцінювання, витратно-вартісні мотивації**.

I Введение

На сегодняшний день наиболее эффективным подходом к проектированию и исследованию систем защиты информации (СЗИ) в информационных системах (ИС) считается метод анализа информационных рисков [1–4]. В основе методологии информационных рисков лежит измерение рисков угроз защищенности информации, обрабатываемой в ИС. Существуют различные способы измерения информационных рисков. На практике чаще всего применяют так называемые табличные методы нахождения рисков, использующие качественные шкалы для оценивания вероятностных характеристик угроз и степени тяжести последствий, наступающих в случае реализации этих угроз [1, 2]. Табличные методы удобны и достаточно адекватны задачам, решаемым на ранних стадиях проектирования СЗИ, в частности, на этапе предпроектных исследований.

Однако по мере конкретизации структуры СЗИ, детализации механизмов защиты, средств и элементов, реализующих эти механизмы, появляется необходимость в более точном измерении рисков, требующем применение количественных шкал для оценивания вероятностных параметров угроз и уязвимостей ИС, определения ущерба, в частности, стоимости потерь, обусловленных успешной реализацией угроз. Особенно актуальным данное требование становится при оценивании остаточных рисков, характеризующих степень эффективности СЗИ, при решении задачи оптимизации выбора механизмов и средств защиты информации в ИС. В этой ситуации для получения количественных оценок обычно используются экспертные методы (индивидуальные или групповые эксперты) [2, 5, 6]. Наибольшее распространение получили групповые методы экспертного оценивания, в которых эксперт непосредственно указывает количественные значения анализируемых параметров: вероятностей, ущерба, стоимости потерь и т. п. Менее известны экспертно-аналитические методы получения оценок, базирующиеся на применении составляемых экспертом логико-эвристических схем (конструкций, моделей), с помощью которых он пытается упорядочить и по возможности логически увязать совокупность разрозненных и часто неполных сведений в сфере проводимой экспертизы. Параметры этих схем или их соотношения задаются экспертным путем, позволяя в конечном итоге получить искомые оценочные суждения относительно анализируемых характеристик.

В частности, при оценивании вероятностных характеристик угроз, используемых для вычисления информационных рисков, можно применить стоимостные схемы, имеющие место в ситуации «атака-защита» ИС. Так, в [7, стр. 263] отмечается, «что как затраты на атаку, так и затраты на защиту от возможных атак следует соотносить со стоимостью защищаемых ресурсов». В [8, стр. 66] для получения характеристик интенсивности потока угроз авторы предлагают применить так называемый оптимистически-пессимистический подход, основывающийся на существовании прямой пропорциональности между интенсивностью потока угроз и обусловленных их реализацией потерь (ущерба): «чем больше потери от взлома (успешной атаки), тем чаще осуществляются попытки несанкционированного доступа (НСД) к этой информации. В [9] предпринята попытка игровой интерпретации финансово-экономических интересов злоумышленника и владельца критической информации в ситуации «атака-защита». Следует отметить, что не все из приведенных выше схем удачны или хотя бы допускают рациональную интерпретацию, Например, при проведении атак на ресурсы ИС атакующую сторону к повторению попыток НСД будут стимулировать размеры выгоды, полученной в случае успешного завершения атаки, тогда как возникшие при этом потери касаются исключительно владельца ИС и, скорее всего, подтолкнут его к усилению уровня защищенности ИС.

В целом наличие подобных логико-эвристических схем позволяет надеяться на более обоснованные и более высокоточные экспертные оценки, получаемые экспертно-аналитическим методом, по сравнению с другими способами осуществления экспертизы.

II Постановка задачи

Рассмотрим ситуацию, возникающую при реализации атакующей стороной (злоумышленниками) угрозы t относительно некоторого информационного ресурса I. Полагаем, что D – общая стоимость затрат атакующей стороны на реализацию угрозы t, g – полученный при этом «выигрыш», определяемый ценностью ресурса I для злоумышленников. Урон, причиненный в этой ситуации владельцу ресурса I, т. е. стоимость критической информации с точки зрения ее владельца оценивается им как g, а общая стоимость осуществленного в ИС комплекса защитных мероприятий равняется C.

Приведенные данные дают стоимостную характеристику ситуации «атака-защита». Требуется на базе этих сведений построить логико-эвристическую схему экспертного оценивания вероятностных характеристик, используемых для вычисления информационных рисков.

III Мотивационно-стоимостные модели действий атакующей и защищающейся сторон

Очевидно, что чистая прибыль злоумышленников в случае успешной реализации угрозы *t* составит:

$$Q = g - D, \tag{1}$$

а эффективность их действий можно оценить отношением

$$E_t = \frac{Q}{D} = \frac{g}{D} - 1. \tag{2}$$

Если интерес атакующей стороны к критической информации *I* носит не разовый, а долговременный характер, т. е. можно предположить, что *g=const*, то естественной является мотивация злоумышленников к уменьшению значений *D* (росту прибыли *Q*). При этом интенсивность потока попыток доступа злоумышленников к ресурсу I будет возрастать, а вероятность угрозы *t* можно будет оценить выражением:

$$P_t = (1 + E_t^{-1})^{-1} = (1 + \frac{D}{Q})^{-1} = 1 - \frac{D}{g}. \tag{3}$$

Ясно, что если ценность ресурса *I* для атакующей стороны очень высока, злоумышленники готовы идти на значительные затраты средств для реализации угрозы *t*. Поэтому в случае *g>>D* вероятность P_t будет практически равна 1. При малых значениях *g* мотивированность злоумышленников к реализации угрозы *t* низка, в частности при *Q*=0 (т. е. *g=D*) теоретически P_t=0, а при *g<D* формула (3) теряет смысл. На практике это означает, что вероятность применения для реализации угроз высокозатратных атак низка. Атаки, подготовка, организация и проведение которых сопряжена со значительными затратами, оправданы лишь в случае, если, например, информация *I* составляет государственную тайну, т. е. уровень ее критичности может быть чрезвычайно высок и даже для значительных *D* (*D/g*<1). Кроме того, важным аспектом в анализе вероятности затратных атак является то, что их организация и проведение связаны со значительными финансовыми рисками, позволить которые себе могут далеко не многие фирмы или организации.

Мотивацию действий владельца информации (владельца ИС) по защите *I* можно проанализировать, введя понятие вероятности безопасности критической информации по отношению к угрозе *t*:

$$P_S = (1 + \frac{q}{SC})^{-1} = \frac{SC}{q + SC}, \tag{4}$$

где *S* – некоторый коэффициент, необходимость введения которого рассмотрим ниже. Как следует из формулы (4), вероятность P_S =1 при *q*=0, т. е. критическая информация в ИС отсутствует. При *q>>SC*, т.е. при значительном уровне критичности ресурса I и низких затратах на создание и функционирование СЗИ, следствием чего является объективная невозможность обеспечить адекватный уровень защиты критической информации в ИС, вероятность $P_S \to 0$.

Для достижения требуемого уровня защищенности необходимо нейтрализовать имеющиеся в ИС уязвимости, повысив эффективность функционирования СЗИ. Это неминуемо повлечет увеличение затрат *C* на реализацию дополнительных защитных мероприятий и *SC* станет сопоставимым с *q*. Естественно, что рост затрат *C* должен происходить в условиях рационального расходования выделенных на совершенствование СЗИ средств и правильно скорректированной политике безопасности ИС.

Рассмотрим причины введения коэффициента *S* в формуле (4) и определимся с его значением. Обычно ресурс *I* является одним из множества информационных элементов, составляющих общий информационный ресурс *I*. Учитывая, что СЗИ защищает не каждый ресурс в отдельности, а всю их совокупность в целом, стоимость защитных мероприятий оказывается ниже значения *q*. Из практики разработки и построения СЗИ известно, что стоимость затрат на защиту в большинстве случаев не должна превышать 10% цены защищаемого ресурса [7] (по другим данным – 5÷15% [1]). Наиболее конкретные сведения приведены в [24], согласно которым P_S ≈0,5 при C=0,1q и P_S ≈0,9 при C=(0,15÷0,2)q. Перечисленные условия удовлетворяются при различных значениях S, лежащих в диапазоне 10÷50. Далее в качестве константы *S* в формуле (4) будем использовать *S*=30.

Вероятность безопасности ресурса *I* по отношению к угрозе *t* связана с вероятностью P_V наличия уязвимостей ИС, способствующих реализации угрозы *t*, очевидным соотношением $P_S + P_V = 1$, откуда

$$P_V = 1 - P_S = \frac{q}{q + SC}. \quad (5)$$

Если по аналогии с формулой (2) ввести понятие эффективности защиты $E_v = q / C$, выражение (5) можно представить в виде:

$$P_V = 1 - \frac{S}{E_V + S} = \frac{E_V}{E_V + S}. \quad (6)$$

При проведении практических расчетов оценивание вероятностей P_t, P_V через значения эффективностей E_t, E_V имеет определенные преимущества по сравнению с соотношениями, содержащими в своем составе стоимостные показатели *g, q, D, C*. Во-первых, исчезает необходимость в нахождении прямых количественных значений этих показателей и, в частности, в выборе единиц измерения. Во-вторых, эффективности E_t, E_V – оценки относительной ценности, для получения которых можно применить метод парных сравнений, дающий достаточно надежные результаты [11].

Приведенные выше формулы (3), (5) позволяют оценить, исходя исключительно из стоимостных характеристик ситуации «атака-защита», значения вероятностей угрозы P_t и уязвимостей P_V, необходимые для вычисления информационного риска по так называемой трехфакторной формуле [1]:

$$R_t = P_V P_t q = \frac{q^2 (g - D)}{g(q - SC)}, \quad (7)$$

где произведение $P_V P_t$ определяет вероятность успешной реализации угрозы *t*.

Структура выражений (3), (6) являющихся эвристическими моделями, определяется мотивационными аспектами действий атакующей и защищающейся сторон, обусловленными экономико-стоимостными факторами.

При детализации действий атакующей и защищающейся сторон до уровня отдельных уязвимостей и атак и возможности получения на этом уровне соответствующих экономико-стоимостных описаний изложенный выше подход к оцениванию вероятностей P_t и P_V можно распространить на получение оценок вероятностей атак и вероятностей уязвимостей. Так, располагая сведениями о совокупности возможных атак $A = \{a_1, ..., a_i, ..., a_N\}$, позволяющих реализовать угрозу *t*, и стоимостей $d = \{d_1, ..., d_N\}$ на организацию и проведение каждой из них, можно, по аналогии с (3), рассчитать вероятности $p(a_i)$, $i = \overline{1, N}$ этих атак:

$$p(a_i) = 1 - \frac{d_i}{g} = \frac{1}{1 + E_{t_i}^{-1}}. \quad (8)$$

При наличии списка возможных уязвимостей ИС $V = \{v_1, ..., v_j, ..., v_H\}$ и справедливости предположения о том, что стоимость затрат на защитные мероприятия *C* допускает фрагментирование на неравные доли $c_1, c_2, ..., c_H$ соответственно элементам этого списка, вероятности уязвимостей можно определить по формуле, аналогичной (6):

$$p(v_j) = \frac{q}{q + Sc_j}, \quad j = \overline{1, H}. \quad (9)$$

При определении вероятностей $p(a_i)$ и $p(v_j)$ в максимальной степени проявляются преимущества использования оценок эффективности E_{t_i}, E_{v_j}, вычисляемых методом парных сравнений, который обеспечивает возможность применения общей базы сравнения для соответствующих классов оценок («выигрыша» *g* для множества оценок $E_{t_i} = d_i / g$ и потерь *q* для множества оценок $E_{v_j} = C_j / q$).

Обобщая информацию, содержащуюся в совокупностях рассчитанных значений $\{p(a_i)\}$, $i = \overline{1, N}$ и $\{p(v_j)\}$, $j = \overline{1, H}$, получим оценки вероятности угрозы *t*

$$P_t^* = 1 - \prod_{i=1}^{N} (1 - p(a_i)) \tag{10}$$

и вероятности уязвимости ИС относительно этой угрозы:

$$P_V^* = 1 - \prod_{j=1}^{H} (1 - p(v_j)) = 1 - \prod_{j=1}^{H} p_S(v_j), \tag{11}$$

где

$$p_S(v_j) = 1 - p(v_j) = \frac{Sc_j}{q + Sc_j} \tag{12}$$

– безопасность ресурса *I* по отношению к уязвимости v_j, $j = \overline{1, H}$.

Можно предположить, что степень субъективизма экспертно-аналитических оценок вероятностей, рассчитанных по (10), (11), ниже, чем оценок P_t, P_V, ранее полученных по (3), (6). Это следует из того, что сама процедура нахождения оценок P_t^*, P_V^* позволяет достаточно объективно выявить, детализировать и учесть причины и факторы, влияющие на возникновение угрозы *t* и формирование условий, определяющих возможность ее реализации.

IV Выводы

Анализ экономико-стоимостных соотношений в системе «атака-защита» при исследовании угроз НСД в ИС позволяет построить эвристические модели для оценивания вероятностей угроз и уязвимостей информационных ресурсов.

Использование в эвристических моделях безразмерных относительных показателей экономико-стоимостного описания системы «атака-защита» в форме оценок эффективности действий атакующей и защищающейся сторон упрощает вопросы практического применения предложенных моделей, в частности, устраняется необходимость прямого количественного измерения затрат и потерь и обеспечивается их шкалирование на основе экспертных сравнительных суждений методом парного сравнения.

*Литература: **1**. Петренко С. А., Симонов С. В. Управление информационными рисками. Экономически оправданная безопасность. М.: Компания Ай Ти; ДМК Пресс, 2004. - 348 с. **2**. Симонов С. В. Методология анализа рисков в информационных системах// Конфидент. Защита информации. - № 2. – 2001. – с. 48-53. **3**. Петренко С. А., Петренко А. А Аудит безопасности Intranet. –М.: ДМК Пресс, 2002. –416 с. **4**. Архипов А. Е. Применение среднего риска для оценивания эффективности защиты информационных систем.// Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні.// науково-техн. зб. – Київ, 2007. – Вип.1(14). – с. 60-67. **5**.Гладыш С. Организационные и методологические аспекты экспертной оценки информационной безопасности информационно-телекоммуникационных систем.// Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні.// науково-техн. зб. – Київ, 2006. – Вип. 1(12). – с. 178-188. **6**. Архипов А. Е., Архипова С. А., Носок С. А. Технологии экспертного оценивания в задачах защиты информации. // Інформаційні технології та комп'ютерна інженерія. - 2005.- № 2.-с. 61-66. **7**. Гринберг А. С., Горбачев Н. Н., Тепляков А. А. Защита информационных ресурсов государственного управления. – М.: Юнити-ДАНА, 2003. – 327 с. **8**. Щеглов Ю. А. Защита компьютерной информации от несанкционированного доступа.- СПб: Наука и техника, 2004–384 с. **9.** Герасименко В. А. Защита информации в автоматизированных системах обработки данных. Кн. 1. – М.: Энергоатомиздат, 1994. – 400с. **10.** Андрощук Г. А., Крайнев П. П. Экономическая безопасность предприятия: защита коммерческой тайны. – К.: Изд. Дом «Ин Юре», 2000. – 400 с. **11.** Толстова Ю. Н. Измерение в социологии.- М.: ИНФРА – М, 1998. – 224 с.*