УДК 004.056.53

Л.В. Передерій, Бердянський університет менеджменту і бізнесу

СИСТЕМНИЙ ПІДХІД ДО ЗАХИСТУ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ

Передерій Л.В.

Системний підхід до захисту інформації в автоматизованих системах

На даний час існує багато різних підходів до захисту інформації, але системний підхід, який застосовується у даних дослідженнях, гарантує цілісність і послідовність застосованих методів захисту інформації при проектуванні комплексних засобів захисту інформації. Дослідження проблеми захисту інформації базується на принципах системного підходу, які сформульовані як основні принципи захисних заходів від несанкціонованого доступу в АС. Досліджується методика аналізу ефективності використовуваних захисних методів для об'єктів різного класу.

Ключові слова: захист інформації, системи безпеки, комплексні засоби захисту інформації.

Передерий Л.В.

Системный подход к защите информации в автоматизированных системах

На данное время существуют много разных подходов к защите информации, но системный подход, который применяется в данных исследованиях, гарантирует целостность и последовательность примененных методов защиты информации при проектировании комплексных средств защиты информации. Исследование проблемы защиты информации базируется на принципах системного подхода, которые сформулированы как основные принципы защитных мероприятий от несанкционированного доступа в АС. Исследуется методика анализа эффективности используемых защитных методов для объектов разного класса.

Ключевые слова: защита информации, системы безопасности, комплексные средства защиты информации.

Постановка проблеми. Захист інформації – це комплекс заходів, направлених на забезпечення інформаційної безпеки. Системи безпеки повинні не тільки і не стільки обмежувати допуск користувачів до інформаційних ресурсів, скільки визначати і делегувати їх повноваження в сумісному вирішенні завдань, виявляти аномальне використання ресурсів, прогнозувати

аварійні ситуації і усувати їх наслідки, гнучко адаптуючи структуру в умовах відмов, часткової втрати або тривалого блокування ресурсів.

Підходи до забезпечення захисту інформації, що існують сьогодні, декілька відрізняються від тих, що існували на початковому етапі. Головна відмінність сучасних концепцій в тому, що сьогодні не говорять про якийсь один універсальний засіб захисту, а мова йде про комплексні засоби захисту інформації (КЗЗІ), що включають:

– нормативно-правовий базис захисту інформації;

– засоби, способи і методи захисту;

– органи і виконавців.

Захист інформації є комплексом регулярно використовуваних засобів і методів, запобіжних заходів, що приймаються, і здійснюваних заходів з метою систематичного забезпечення необхідної надійності інформації, що генерується, зберігається і оброблюється в автоматизованій системі (АС), а також передається по каналах. Захист повинен носити системний характер, тобто для отримання якнайкращих результатів всі розрізнені види захисту інформації повинні бути об'єднані в одне ціле і функціонувати у складі єдиної системи, що є злагодженим механізмом взаємодіючих елементів [1, с. 34], призначених для виконання завдань з забезпечення безпеки інформації . КЗЗІ призначений забезпечувати, з одного боку, функціонування надійних механізмів захисту, а з іншого – управління механізмами захисту інформації. У зв'язку з цим повинна передбачатися організація чіткої і відлагодженої системи управління захистом інформації та підготовка кваліфікованих фахівців.

Аналіз досліджень і публікацій. Разом з існуючими нормативно-правовими документами теоретичну базу у проведених дослідженнях склали праці відомих учених в області захисту інформації від витоку по технічних каналах В.В. Домарева та А.А. Хорева.

Мета дослідження. Бурхливе зростання конфіденційної і комерційної інформації, а також істотне збільшення фактів її розкрадання викликає підвищений інтерес все більшого числа організацій до створення власних

захищених інформаційних систем. Підготовка фахівців з цих питань стає все більш актуальною. Метою статті є дослідження методологій проектування КЗЗІ автоматизованих систем різного класу.

Виклад основного матеріалу. Проектування захищених інформаційних систем – процес досить складний, який припускає наявність відповідних знань і досвіду у її творців. Процес проектування захищених інформаційних систем повинен ґрунтуватися на знанні і строгому виконанні вимог існуючих нормативних документів як з боку її розробників, так і з боку користувачів.

Поняттям «комплексність» є рішення в рамках єдиної концепції двох або більшої кількості різнопланових завдань. Сучасна система захисту інформації повинна включати структурну, функціональну і часову комплексність. Структурна комплексність припускає забезпечення необхідного рівня захисту у всіх елементах системи обробки інформації. Функціональна комплексність означає, що методи захисту повинні бути направлені на всі виконувані функції системи обробки інформації. Часова комплексність припускає безперервність здійснення заходів щодо захисту інформації як в процесі безпосередньої її обробки, так і на всіх етапах життєвого циклу об'єкту обробки інформації [2, с. 156].

До складу КЗЗІ входять заходи і засоби, які реалізують способи, методи, механізми захисту інформації від:

– витоків технічними каналами, до яких відносяться канали побічних електромагнітних випромінювань, акустоелектричних і інших каналів;

– несанкціонованих дій і несанкціонованого доступу до інформації, які можуть здійснюватися шляхом підключення до апаратури і ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав'язування помилковій інформації, застосування заставних пристроїв або програм, використання комп'ютерних вірусів і т.п.;

– спеціального впливу на інформацію, який може здійснюватися шляхом формування полів і сигналів з метою порушення цілісності інформації або руйнування системи захисту.

Для кожної конкретної інформаційно-телекомунікаційної системи (ІТС) склад, структура і вимоги до КЗЗІ визначаються властивостями оброблюваної інформації, класом автоматизованої системи (АС) і умовами її експлуатації.

Класи автоматизованих систем:

1) одномашинний однокористувальницький комплекс, який обробляє інформацію однієї або декількох категорій конфіденційності;

2) локалізований багатомашинний багатокористувальницький комплекс, оброблювальний інформацію різних категорій конфіденційності.

3) розподілений багатомашинний багатокористувальницький комплекс, який обробляє інформацію різних категорій конфіденційності.

У загальному випадку, послідовність і зміст науково-дослідної розробки КЗЗІ можна заздалегідь розділити на 4 етапи:

1) Розробка технічного завдання:
   - аналіз стану інформаційної системи;
   - розробка інформаційної моделі КЗЗІ;
   - аналіз уражень інформаційної системи;
   - визначення вимог до системи захисту.

2) Визначення технічного рішення:
   - опис технічного рішення;
   - визначення детального переліку устаткування, програмного забезпечення і змісту робіт;
   - визначення вартості.

3) Реалізація КЗЗІ:
   - побудова повного комплексу засобів захисту;
   - тестування КЗЗІ;
   - отримання експертного висновку (атестату).

4) Експлуатація КЗЗІ:

– підтримка актуальності КЗЗІ протягом життєвого циклу.

Даний алгоритм – це лише основа проектування. Кожен представлений етап відображає безліч рівнів в ході проектування залежно від структури АС – вимоги, що пред'являються до її системи захисту [3, с. 56].

Однією з вимог забезпечення захисту інформації в АС є те, що обробка в АС конфіденційної інформації повинна здійснюватись з використанням захищеної технології, яка містить програмно-технічні засоби захисту і організаційні заходи, які забезпечують виконання загальних вимог з захисту інформації. Загальні вимоги передбачають:

– наявність переліку конфіденційної інформації, яка підлягає автоматизованій обробці; у разі потреби можлива її класифікація в межах категорії за цільовим призначенням, ступенем обмеження доступу окремої категорії користувачів і іншими класифікаційними ознаками;

– наявність певного (створеного) відповідального підрозділу, якому надаються повноваження щодо організації і впровадження технології захисту інформації, контролю за станом захищеності інформації (служба захисту в АС, СЗІ);

– створення КСЗІ, яка являє собою сукупність організаційних і інженерно-технічних заходів, програмно-апаратних засобів, направлених на забезпечення захисту інформації під час функціонування АС;

– розробку плану захисту інформації в АС;

– наявність атестату відповідності КСЗІ в АС нормативним документам із захисту інформації;

– можливість визначення засобами КСЗІ декількох ієрархічних рівнів повноважень користувачів і декількох класифікаційних рівнів інформації;

– обов'язковість реєстрації в АС всіх користувачів і їх дій щодо конфіденційної інформації;

– можливість надання користувачам тільки за умови службової необхідності санкціонованого і контрольованого доступу до конфіденційної інформації, яка обробляється в АС;

– заборона несанкціонованій і неконтрольованій модифікації конфіденційної інформації в АС;

– здійснення за допомогою СЗІ обліку вихідних даних, отриманих під час рішення функціональної задачі, у формі віддрукованих документів, які містять конфіденційну інформацію, відповідно до керівних документів;

– заборона несанкціонованого копіювання, розмноження, розповсюдження конфіденційної інформації, в електронному вигляді;

– забезпечення за допомогою СЗІ контролю за санкціонованим копіюванням, розмноженням, розповсюдженням конфіденційної інформації, в електронному вигляді;

– можливість здійснення однозначної ідентифікації і аутентифікації кожного зареєстрованого користувача;

– забезпечення КСЗІ можливості своєчасного доступу зареєстрованих користувачів АС до конфіденційної інформації.

Приведені вимоги є базовими і застосовуються при захисті інформації від НСД у всіх типах АС [4, с. 85].

Умовно розділивши АС на найважливіші підсистеми забезпечення захисту інформації (рис. 1), можна перелічити також вимоги, що пред'являються для захисту комп'ютерної інформації від НСД в АС кожній окремій підсистемі.

Рис. 1. Підсистеми управління та забезпечення захисту інформації в автоматизованих системах

Підсистема управління доступом повинна задовольняти наступним вимогам:

– ідентифікувати і перевіряти достовірність суб'єктів доступу при вході в систему. Причому це повинно здійснюватися по ідентифікатору (коду) і паролю умовно-постійної дії довжиною не менше шести літеро-цифрових символів;

– ідентифікувати термінали, ЕОМ, вузли комп'ютерної мережі, канали зв'язку, зовнішні пристрої ЕОМ за їх логічними адресами (номерами);

– за іменами ідентифікувати програми, томи, каталоги, файли, записи і поля записів;

– здійснювати контроль доступу суб'єктів до ресурсів, що захищаються, відповідно до матриці доступу;

Підсистема реєстрації і обліку повинна:

– реєструвати вхід (вихід) суб'єктів доступу в систему (з системи), або реєструвати завантаження і ініціалізацію операційної системи і її програмної зупинки. При цьому в параметрах реєстрації указуються:

а) дата і час входу (виходу) суб'єкта доступу в систему (з системи) або завантаження (зупинки) системи;

б) результат спроби входу — успішна або неуспішна (при НСД);

в) ідентифікатор (код або прізвище) суб'єкта, пред'явлений при спробі доступу;

г) код або пароль, пред'явлений при неуспішній спробі.

– реєстрація виходу з системи або зупинки не проводиться в моменту апаратурного відключення АС;

– реєструвати видачу друкарських (графічних) документів на «тверду» копію. При цьому в параметрах реєстрації указуються:

а) дата і час видачі (звернення до підсистеми виводу);

б) короткий зміст документа (найменування, вигляд, код, шифр) і рівень його конфіденційності;

в) специфікація пристрою видачі (логічне ім'я зовнішнього пристрою);

г) ідентифікатор суб'єкта доступу, що запитав документ;

– реєструвати запуск (завершення) програм і процесів (завдань, задач), призначених для обробки файлів, що захищаються. При цьому в параметрах реєстрації указується:

а) дата і час запуску;

б) ім'я (ідентифікатор) програми (процесу, завдання);

в) ідентифікатор суб'єкта доступу, що запитав програму (процес, завдання);

г) результат запуску (успішний, неуспішний – несанкціонований).

– реєструвати спроби доступу програмних засобів (програм, процесів, завдань, задач) до файлів, що захищаються. У параметрах реєстрації указується:

а) дата і час спроби доступу до файлу, що захищається, з вказівкою її результату (успішна, неуспішна – несанкціонована);

б) ідентифікатор суб'єкта доступу;

в) специфікація файлу, що захищається.

– реєструвати спроби доступу програмних засобів до додаткових об'єктів доступу, що захищаються (терміналам ЕОМ, вузлам мережі ЕОМ, лініям (каналам) зв'язку, зовнішнім пристроям ЕОМ, програмам, томам, каталогам, файлам, записам, полям записів). При цьому в параметрах реєстрації указується:

а) дата і час спроби доступу до файлу, що захищається, з вказівкою її результату: успішна, неуспішна, несанкціонована;

б) ідентифікатор суб'єкту доступу;

в) специфікація об'єкту, що захищається [логічне ім'я (номер)].

– проводити облік всіх носіїв інформації, що захищаються, за допомогою їх маркування із занесенням облікових даних в журнал (облікову картку);

– реєструвати видачу (приймання) носіїв, що захищаються;

– здійснювати очищення (обнулення, знеособлення) областей оперативної пам'яті ЕОМ і зовнішніх накопичувачів, що звільняються. При цьому очищення повинне проводитися одноразовим, довільним записом в область пам'яті, що

звільняється, раніше використану для зберігання даних, що захищаються (файлів).

Підсистема забезпечення цілісності повинна:

– забезпечувати цілісність програмних засобів системи захисту інформації від НСД (СЗІ НСД), оброблюваної інформації, а також незмінність програмного середовища. При цьому:

а) цілісність СЗІ НСД перевіряється при завантаженні системи по контрольних сумах компонент СЗІ;

б) цілісність програмного середовища забезпечується використанням трансляторів з мови високого рівня і відсутністю засобів модифікації об'єктного коду програм в процесі обробки і зберігання інформації, що захищається;

– здійснювати фізичну охорону пристроїв і носіїв інформації. При цьому повинні передбачатися контроль доступу в приміщення АС сторонніх осіб, а також наявність надійних перешкод для несанкціонованого проникнення в приміщення АС і сховище носіїв інформації, особливо в неробочий час;

– проводити періодичне тестування функцій СЗІ НСД при зміні програмного середовища і персоналу АС за допомогою тест-програм, що імітують спроби НСД;

– мати в наявності засоби відновлення СЗІ НСД. При цьому передбачається ведення двох копій програмних засобів СЗІ НСД, а також їх періодичне оновлення і контроль працездатності.

Провівши оцінку необхідності захисту інформації від НСД, стає питання про подальший напрям проектування системи захисту інформації. Адже саме по отриманих результатах можна судити про складність проектованої системи. Маючи такі результати, необхідно оцінити вірогідність погроз, що проявляються, на інформаційну систему, а також сформувати модель порушника, після чого слід приступити до формування захисних заходів. Спираючись на вимоги із захисту інформації від НСД [5, с. 56], можна привести основні принципи захисних заходів від НСД в АС.

Принцип перший – обґрунтованість доступу. Даний принцип полягає в обов'язковому виконанні двох основних умов: користувач повинен мати достатню «форму допуску» для отримання інформації потрібного ним рівня конфіденційності, і ця інформація необхідна йому для виконання його виробничих функцій. У сфері автоматизованої обробки інформації як користувачі можуть виступати активні програми і процеси, а також носії інформації різного ступеня складності. Тоді система доступу припускає визначення для всіх користувачів відповідного програмно-апаратного середовища або інформаційних і програмних ресурсів, які будуть їм доступні для конкретних операцій [6, с. 186].

Принцип другий – достатня глибина контролю доступу. Засоби захисту інформації повинні включати механізми контролю доступу до всіх видів інформаційних і програмних ресурсів АС, які відповідно до принципу обґрунтованості доступу слід розділяти між користувачами.

Принцип третій – розмежування потоків інформації. Для попередження порушення безпеки інформації, яке, наприклад, може мати місце при записі секретної інформації на несекретні носії і в несекретні файли, її передачі програмам і процесам, не призначеним для обробки секретної інформації, а також при передачі секретної інформації по незахищених каналах і лініях зв'язку, необхідно здійснювати відповідне розмежування потоків інформації.

Принцип четвертий – чистота повторно використовуваних ресурсів. Даний принцип полягає в очищенні ресурсів, що містять конфіденційну інформацію, при їх видаленні або звільненні користувачем до перерозподілу цих ресурсів іншим користувачам.

Принцип п’ятий – персональна відповідальність. Кожен користувач повинен нести персональну відповідальність за свою діяльність в системі, включаючи будь-які операції з конфіденційною інформацією і можливі порушення її захисту, а також за випадкові або умисні дії, які можуть привести до несанкціонованого ознайомлення з конфіденційною інформацією, її

спотворенню або знищенню, або виключенню можливості доступу до такої інформації законних користувачів.

Принцип шостий – цілісності засобів захисту. Даний принцип має на увазі, що засоби захисту інформації в АС повинні точно виконувати свої функції відповідно до перерахованих принципів і бути ізольованими від користувачів, а для свого супроводу повинні включати спеціальний захищений інтерфейс для засобів контролю, сигналізації про спроби порушення захисту інформації і дії на процеси в системі.

Реалізація перерахованих принципів здійснюється за допомогою «монітора звернень», контролюючого будь-які запити до даних або програм з боку користувачів (або їх програм) з встановлених для них видах доступу до цих даних і програм. Схемно такий монітор можна представити у вигляді, показаному на рис. 2.

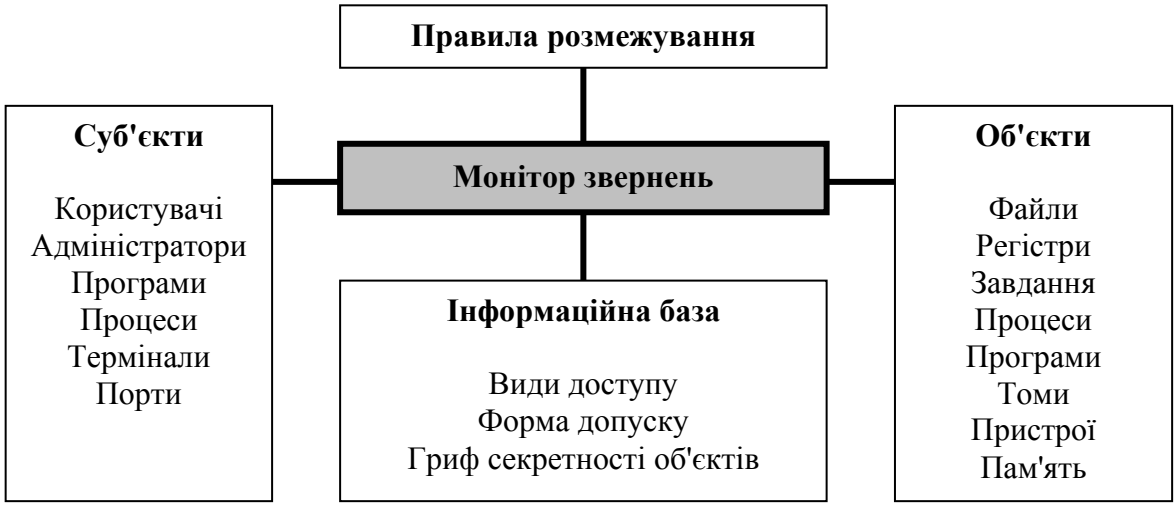

Рис. 2. Структура монітора звернень

Практичне створення монітора звернень, як видно з приведеного рисунка, припускає розробку конкретних правил розмежування доступу у вигляді моделі захисту інформації.

Спроектувавши модель захисту інформації, необхідно виконати аналіз ефективності захисних заходів. Головна функція системи безпеки – протидія погрозам за допомогою людей і техніки. Кожна загроза спричиняє за собою збиток, а протидія покликана понизити його величину, в ідеалі – повністю. Вдається це далеко не завжди. Здатність системи безпеки виконувати свою

головну функцію завжди повинна оцінюватися кількісно. Наприклад, можна зміряти відносний збиток, відвернутий нею (рис. 3).

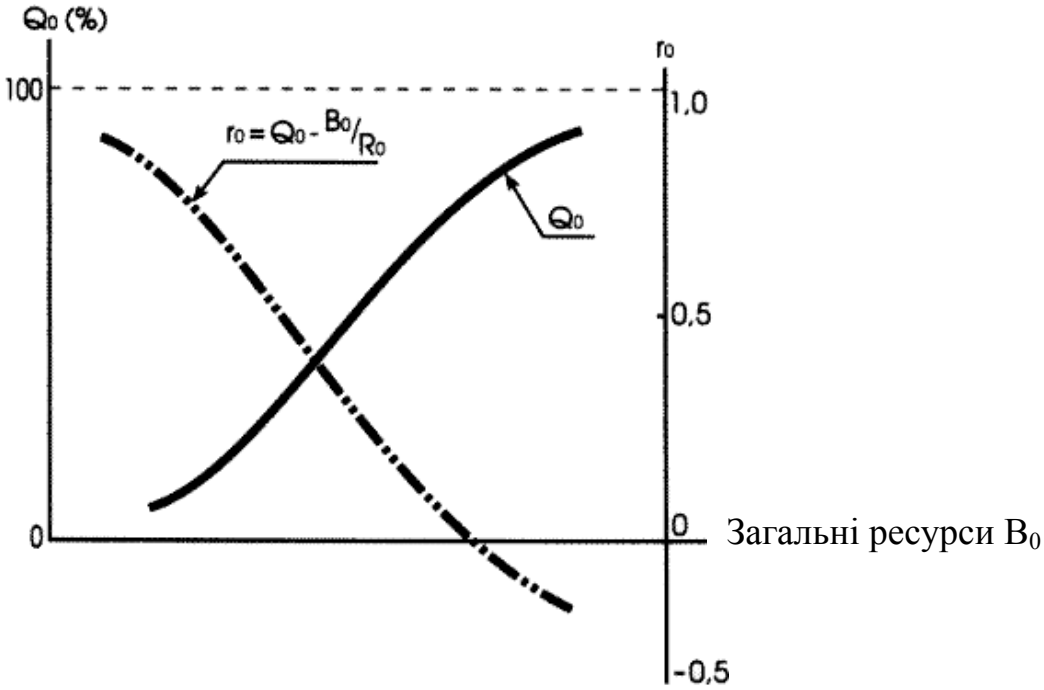

Рис. 3. Типова залежність ефективності Q_0 і рентабельності r_0 захисту від загальних ресурсів

Величина Q_0 – міра загальної ефективності захисту. Чим більше Q_0, тим менший збиток створять погрози. Таким чином, мірою ризику є величина$(1-Q_0)$. Прагнення забезпечити високоефективний захист, коли Q_0 близька до 1 (або 100%), цілком природно, але це спричинить значних витрат на ресурси. Тобто чим вище сукупні асигнування (B_0) на ресурси, тим на велику ефективність захисту можна розраховувати. Виниклу при цьому залежність видно на рис. 3. Проте надмірні витрати на власну безпеку не завжди виправдані економічно. Можна зіткнутися з ситуацією, коли вартість захисту (B_0) перевищить рівень (R_0) максимального збитку від реалізації погроз. В цьому випадку виникає небезпека загрози «саморозорення» від захисту. Її рівень також можна оцінити, наприклад, величиною r різниці відносного «захищеного» збитку Q_0 і відносних витрат B_0/R_0 на ресурси. Назвемо цю величину рентабельністю захисту. Якщо вона позитивна (тобто $B_0<=R_0Q_0$), то захист рентабельний. На відміну від ефективності, чим більше витрати (B_0), тим менше рентабельність. Ця протилежність створює неоднозначну ситуацію у виборі стратегії захисту.

Розглянемо типову залежність ефективності захисту (Q_0) і її рентабельності (r_0) від максимального збитку R_0 (рис. 4).

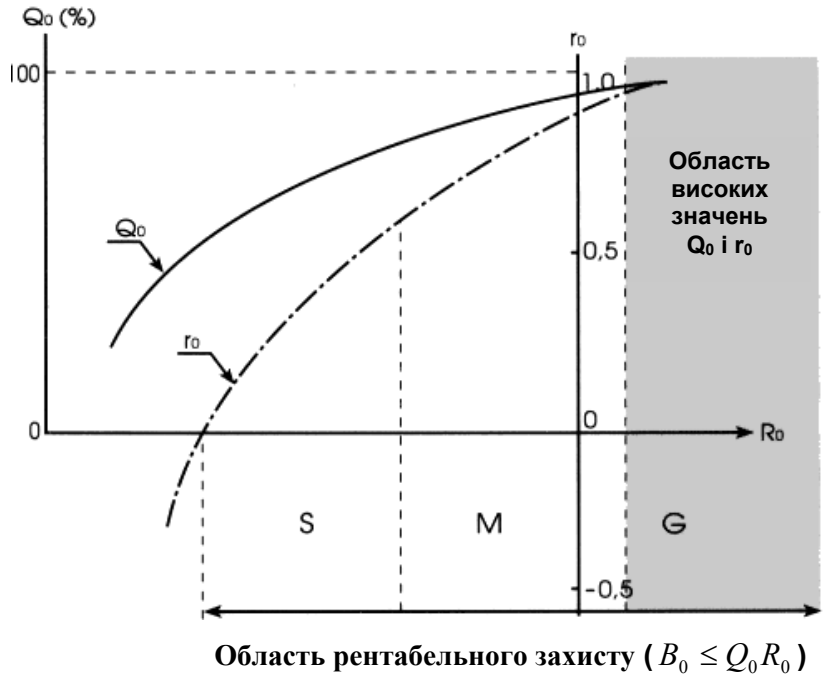

Рис. 4. Залежність ефективності і рентабельності захисту від максимального збитку R_0

По суті, це є мірою масштабності бізнесу. Неважко побачити, що зробити захист одночасно і високоефективною, і високорентабельною під силу лише крупним комерційним структурам (область G), для яких характерні великі величини максимального збитку. Достатньо, наприклад, щоб $B_0=R_0(1-Q_0)$. Тоді при $r \to 1$, $Q_0 \to 1$. У гіршому положенні опиняються інтереси середнього (область M) і малого (область S) бізнесу, оскільки із-за обмеженості ресурсів вибір стратегії захисту складніший. Тут рекомендації прості. Треба забезпечити максимально можливу ефективність при позитивному показнику рентабельності захисту. Тобто в першу чергу слід протидіяти найбільш вірогідним і небезпечним погрозам. У будь-якому випадку не можна забувати про економію ресурсів. Абсолютно ясно, що вибір стратегії захисту полегшується, якщо при менших витратах вдасться забезпечити рівну або навіть велику ефективність захисту.

Очевидні і джерела економії витрат: використання економічніших засобів і рішень універсального характеру; раціональний розподіл ресурсів і досконаліші форми управління ними; залучення кооперативних форм забезпечення безпеки і ін.

Весь цей перелік властивий крупним комерційним структурам, проте для середнього і малого бізнесу він істотно звужується. Ідеологія їх системи безпеки повинна будуватися на рентабельному захисті лише від окремих видів погроз. Інакше захист може себе не виправдати. Тому треба мати на увазі, що економії ресурсів в цих умовах сприятимуть кооперативні форми захисту в рамках єдиної місцевої або регіональної системи безпеки. Вигоду кооперативних форм протидії погрозам ілюструє рис. 5.

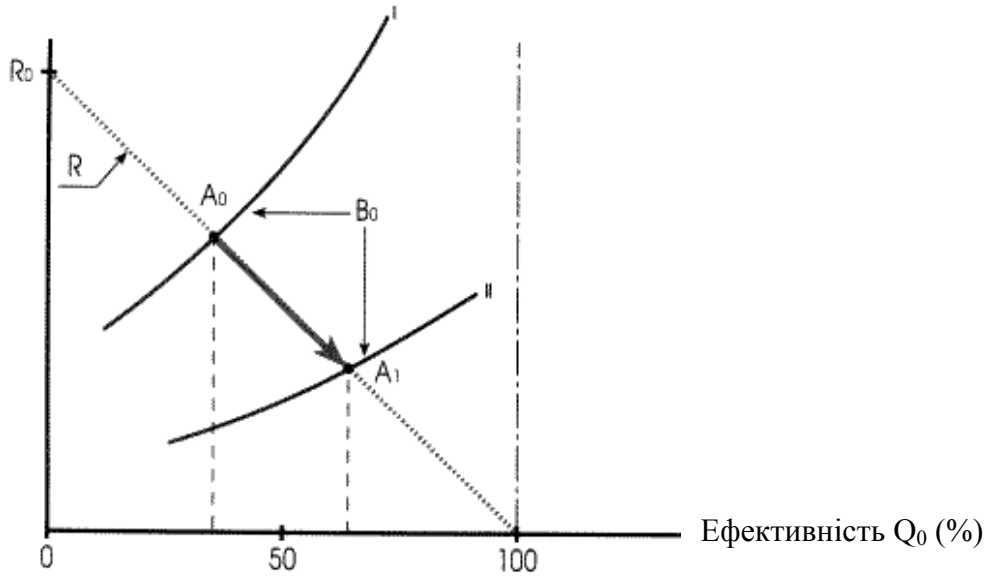

Рис. 5. Характерні залежності ризику R і витрат на ресурси B_0 як функцій від ефективності захисту Q_0

На рисунку представлені характерні залежності величини ризику ($R=R_0(1-Q_0)$ і загальних витрат (B_0) на ресурси від ефективності автономного (I) і кооперативного (II) захисту. Точка перетину (A_0) залежностей R(Q) і B(Q) для автономного захисту відповідає приблизно області мінімальних загальних втрат $R_0(1-Q_0)+B_0$. Економія ресурсів виразиться в тому, що початкова залежність (I) виявиться «вищою» за нову залежність (II), яка відображає кооперацію у використанні ресурсів. Відповідно нова точка перетину кривих (A_1) виявиться правіше колишньої (A_0). Практично це означає, що при збереженні рентабельності захисту збільшується її ефективність. Причому виграш тим істотніше, чим більше економія. На практиці в основному кооперуються по двох формах – матеріально-технічних і кадрових ресурсах, які і є складовими частинами загального. Що стосується першої форми, то вона характерна для

ситуацій, коли простір погроз не розширюється. Іншими словами, об'єднуються лише матеріально-технічні засоби одного і того ж підприємства, але призначені для різних цілей.

Будь-яка загроза і протидія їй відбуваються у часі і характеризуються певними його масштабами. Виходячи з цього збиток від реалізації погроз визначатиметься тим, наскільки повно дані події перетинаються в часі. Самий небажаний варіант – протидія, що запізнюється, коли реакція системи захисту починається до моменту завершення загрози або після неї. Він характерний для систем інформаційного захисту. Декілька кращий варіант – одночасна протидія, тобто вона починається з появою загрози. І, нарешті, якнайкращий варіант – протидія, що носить випереджаючий характер: реакція системи захисту починається до початку реалізації загрози. Підставою для реакції можуть бути оперативні дані, сигнали тривоги раннього сповіщення і тому подібне.

На рис. 6 представлена характерна залежність ефективності захисту від відносного часу реакції системи (T_p/T_y) для всіх трьох варіантів протидії.

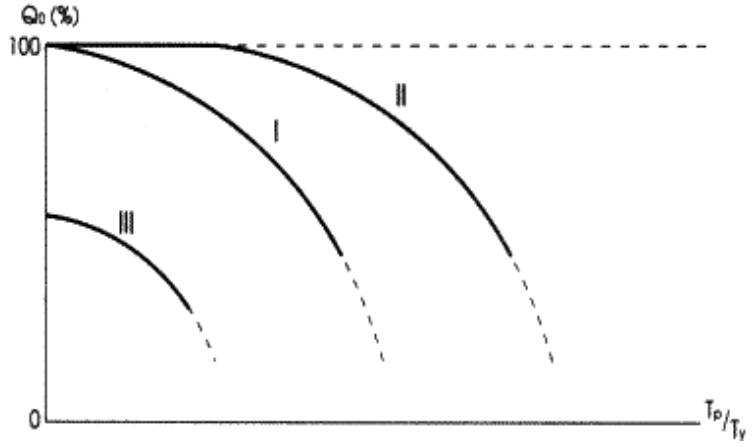

Рис. 6. Залежність ефективності захисту Q_0 від відносного часу T_p/T_y реакції системи з одночасною (I), випереджаючою (II) і такою, що запізнюється (III) протидією

Основні виводи і рекомендації очевидні. Одночасна протидія буде достатньою для високоефективного захисту від загрози, якщо реакція на неї буде швидкою. Це завдання цілком реальне для об'єктів великого бізнесу. Кооперативні ж форми протидії в умовах повільної реакції на погрози не принесуть ефекту, якщо відсутні засоби затримки і блокування погроз. Кажучи

про тактичні питання системи безпеки бізнесу в частині технічних каналів зв'язку, перш за все мають на увазі швидкість її реакції, надійність рішень, блокування розвитку погроз і їх ліквідацію. Особливо важливо забезпечити жорсткі вимоги до надійності всіх систем захисту, які залежать від часу їх функціонування і періодичності оновлення ресурсів. Якщо цей час перевищує 5 років, то вимога надійності реалізується декількома способами, серед яких – резервування рішень, багаторубіжність захисту, автоматизація первинних рішень, централізоване управління ресурсами в кризових ситуаціях і тому подібне Перш ніж визначитися в питаннях тактики, треба пам'ятати, що вона повинна відповідати стратегії і спиратися на точний кількісний аналіз. Для об'єктів середнього і малого бізнесу такий аналіз цілком реальний навіть без засобів автоматизації. Проте, необхідно привернути фахівців і експертів, які б проаналізували обстановку і властивості об'єкту захисту, розробили модель погроз, вивчили ринок існуючих засобів і методів. Ці дані і допомогли б оцінити саму систему і при необхідності модернізувати її.

Висновки. Проведені дослідження містять методичні рекомендації до проектування комплексних систем захисту інформації. В процесі дослідження визначені етапи розробки КСЗІ. Найбільш відповідальним є третій етап, оскільки саме на даному етапі реалізуються всі захисні заходи щодо вимог і технічного рішення, прийнятих на попередніх етапах. Встановлені основні вимоги до захисту як конфіденційної, так і секретної інформації від несанкціонованого доступу. Проаналізовані основні принципи захисних заходів від несанкціонованого доступу в АС, реалізація їх здійснюється за допомогою «монітора звернень».

Аналіз використовуваних захисних методів і заходів свідчить, що їх реалізація для кожного об'єкту різна, відповідно і ефективність таких заходів від НСД для одних об'єктів вища (об'єкти великого бізнесу), а для інших нижча (об'єкти малого бізнесу). Результати дослідження можуть бути використані при підготовці фахівців з питань захисту інформації, або при розробці комплексних систем захисту інформації для підприємств різного класу. Подальший розвиток

досліджень базується на реалізації проектних рішень засобами CASE-технології.

Література

1. **Катренко А.В.** Системний аналіз об’єктів та процесів комп’ютеризації/ Навчальний посібник. – Львів : Новий світ-2000, 2003. – 424 с.

2. **Домарев В.В.** Безопасность информационных технологий. Методология создания систем защиты. – К. : ООО ТИД-ДС, 2001. – 688 с.

3. **Бугров Ю.Г.** Системные основы оценивания и защиты информации. Учебное пособие / Воронеж: Воронеж. гос. техн. ун-т, 2005. – 354 с.

4. **Хорев А.А.** Способы и средства зашиты информации. – М. : МО РФ, 2000. – 316 с.

5. **Хорев А.А.** Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. Учебное пособие. – М. : Гостехкомиссия России, 1998. – 320 с.

6. **Хорев А.А.** Методы и средства поиска электронных устройств перехвата информации. – М. : МО РФ, 1998. – 224 с.

Perederiy L.V.

Approach of the systems to the defence of information in the automated systems

On this time there are a lot of the different going near a defence of information, but approach of the systems, which is used in these researches, guarantees integrity and sequence of the applied methods of defence of information at planning of complex facilities of defence of information. Research of problem of defence of information is based on principles of approach of the systems, which are formulated as basic principles of protective measures from an unauthorized division in ACE. The method of analysis of efficiency of in-use protective methods is probed for the objects of different class..

Keywords: defence of information, systems of safety, complex facilities of defence of information..

Відомості про автора

Передерій Людмила Василівна – доцент кафедри інформаційних систем і технологій Бердянського університету менеджменту і бізнесу. Основні наукові

інтереси зосереджені навколо проблематики безпеки інформаційних систем, проектування інформаційних систем методами системного аналізу та CASE–технології.