НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ

ІНСТИТУТ ПРОБЛЕМ МОДЕЛЮВАННЯ В ЕНЕРГЕТИЦІ
ім. Г.Є. ПУХОВА

Будько Микола Миколайович

УДК 681.3

Методи підвищення захищеності
інформаційних ресурсів автоматизованих систем спеціального призначення та оптимізації структур систем їхнього технічного захисту

Спеціальність 05.13.21 – системи захисту інформації

Автореферат
дисертації на здобуття наукового ступеня кандидата технічних наук

Київ – 2002

Дисертацією є рукопис.
Робота виконана у Відкритому акціонерному товаристві “Київське підприємство обчислювальної техніки та інформатизації (“КП ОТІ”).

Науковий керівник

кандидат технічних наук, доцент Василенко Вячеслав Сергійович, Відкрите акціонерне товариство “КП ОТІ”, начальник відділу Центру технічного захисту інформації.

Офіційні опоненти:

доктор технічних наук, старший науковий співробітник Мохор Володимир Володимирович, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, зав. відділом;

кандидат технічних наук, старший науковий співробітник Кудін Антон Михайлович військова частина А 1906, начальник відділу.

Провідна установа – Інститут проблем реєстрації інформації НАН України, відділ цифрових моделюючих систем.

Захист відбудеться “05“ грудня 2002 р. о 14 годині на засіданні спеціалізованої вченої ради Д.26.185.01 Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України за адресою: 03164, Київ – 164, вул. Генерала Наумова, 15.

З дисертацією можна ознайомитись в бібліотеці Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України за адресою: 03164, Київ – 164, вул. Генерала Наумова, 15.

Автореферат розісланий “01” листопада 2002 р.

Вчений секретар
спеціалізованої вченої ради Д26.185.01
кандидат технічних наук Семагіна Е.П.

* **ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ**

**Актуальність.** Однією з особливостей сучасного етапу розроблення автоматизованих систем керування (АСК) є те, що при їх створенні необхідно вирішувати достатньо суперечливі задачі. Перша з них полягає в створенні АСК як багатокористувацької системи з колективним використанням ресурсів та відповідною організацією безпосереднього чи віддаленого доступу. Однак така організація систем сприяє зниженню захищеності інформації, яка циркулює в таких АСК. Порушення захищеності є еквівалентним заподіянню шкоди власнику АСК, оскільки призводять, як правило, до збитків в тій чи іншій формі. Тому одночасно слід вирішувати і другу задачу, яка полягає в забезпеченні достатнього рівня захищеності інформації від порушень її конфіденційності, цілісності та доступності. Для цього існують певні заходи та засоби захисту. Впровадження засобів захисту, в свою чергу, збільшує вартість АСК, навантаження на системні ресурси та знижує загальну продуктивність АСК. При чому, чим надійніше захист, тим більшими є додаткові витрати на його здійснення. Це породжує достатньо складні проблеми побудови таких АС, в яких рівень захищеності і відповідна складність засобів захисту та їх вплив на характеристики даної АС були б в деякому сенсі оптимальними. Вищевикладене зумовлює актуальність задач оптимізації структур систем технічного захисту інформаційних ресурсів сучасних автоматизованих систем керування від несанкціонованого доступу (НСД) та розробки більш досконалих методів та алгоритмів захисту*.* Дисертаційна робота присвячена питанням теоретичного та практичного розвитку методів, алгоритмів захисту інформації та методик їх застосування.

**Зв’язок роботи з науковими програмами, планами, темами.** Робота виконувалась згідно з планами науково – дослідних та дослідно – конструкторських робіт Відкритого акціонерного товариства “Київське підприємство обчислювальної техніки та інформатизації ("КП ОТІ") у відповідності з договором Державного транспортного галузевого об’єднання "Укрзалізниця" Міністерства транспорту України № ІТ 19/98 від 7 травня 1998 р. та Міністерства внутрішніх справ України у відповідності з договорами № 3/01 від 15.04.1997 р., № 7/01 від 15.04.1999 р.,
№ 13/01 від 14.06.2000 р., № 15/01 від 14.06.2000 р., № 26/01 від 01.12.2000 р. з ВАТ “КП ОТІ”.

**Мета і задачі дослідження.** Метою дисертаційної роботи є розробка структури та засобів математичного забезпечення систем захисту сучасних АСК і оптимізація їх параметрів на базі математичного моделювання процесів технічного захисту інформації АСК.

Для досягнення поставленої мети вирішуються наступні основні задачі:

* аналіз існуючих показників ефективності систем технічного захисту інформаційних ресурсів АСК та визначення показників, необхідних для побудови оптимальних систем;
* розробка математичних моделей процесів в технічному захисті інформації АСК;
* визначення оптимальних параметрів системи захисту інформаційних ресурсів АСК (періодичність, тривалість процесів технічного захисту);
* визначення структури системи захисту та її основних підсистем;
* розроблення методів захисту інформаційних ресурсів АСК та методик їх практичного використання, орієнтованих на запропоновані структури систем захисту.

**Наукова новизна одержаних результатів** полягає в наступному:

* на відміну від більшості відомих систем якісної оцінки таких функціональних властивостей захищених систем як конфіденційність, цілісність та доступність вперше визначені кількісні показники цих функціональних властивостей та запропоновано їх застосування для оцінювання якості систем захисту, в тому числі для задач оцінювання величини залишкового ризику, оптимізації структури та параметрів компонентів систем захисту;
* на основі досліджень математичних моделей процесів забезпечення конфіденційності, цілісності та доступності інформації АСК визначено цільову функцію та розроблено метод оптимізації параметрів системи захисту та її складових, а також визначено структури основних підсистем системи захисту;
* розроблено методи формування ознак цілісності захищених інформаційних об’єктів та контролю і поновлення їх цілісності. Можливе застосування розроблених методів для розробки методів формування цифрового підпису та методів завадостійкого криптографічного захисту інформаційних об’єктів.

**Практичне значення одержаних результатів.**

* Запропоновано інженерну методику оптимізації параметрів засобів захисту ресурсів АСК, використання яких дозволяє значно зменшити сумарні втрати за рахунок порушення конфіденційності, цілісності та доступності інформаційних ресурсів АСК, а також за рахунок застосування системи захисту цих ресурсів;
* Розроблено моделі взаємодії засобів реалізації атак з засобами протидії цим атакам для кожної з властивостей захищеної системи. З застосуванням цих моделей розв’язано задачу оцінювання кількісних показників захищеності інформаційних ресурсів АСК – величин залишкового ризику;
* Розроблено практичні методики застосування методів формування ознак цілісності захищених інформаційних об’єктів та контролю їх цілісності. Їх вживання дозволяє підвищити цілісність та доступність інформаційних об’єктів АСК;

Результати дисертаційної роботи впроваджено в АСК "Експрес – УЗ" Укрзалізниці, а також в розробках ВАТ "КП ОТІ" засобів захисту Єдиної державної автоматизованої паспортної системи.

**Особистий внесок здобувача.** У роботах, що написані в співавторстві, автору належать: [1, 7, 9, 10] – дослідження в частині розробки структури системи технічного захисту інформації в ієрархічних автоматизованих системах керування; [3, 5, 6, 8, 11] – дослідження в частині розроблення методу контролю цілісності інформаційних об’єктів з застосуванням коду умовних лишків (ЛУ – коду) та методик його застосування; [2] – дослідження в частині моделювання процесу захисту інформації в автоматизованих системах та формуванні цільової функції системи; [4] – дослідження в частині розроблення моделей впливів на елементи телекомунікаційних підсистем та взаємодії засобів в процесі технічного захисту інформації, оцінки інтенсивності та ймовірносних характеристик впливів на ресурси телекомунікаційних підсистем та методики застосування методу захисту з використанням ЛУ – коду.

**Апробація результатів.** Основні результати дисертаційної роботи та результати досліджень доповідалися і обговорювалися на Науково – технічній конференції "Правове, нормативне та метрологічне забезпечення Системи захисту інформації в Україні" (Київ, 2000) та на П’ятій Міжнародній науково – практичній конференції “Безпека інформації в інформаційно –телекомунікаційних системах”, 20-24 травня 2002 (Київ).

**Публікації.** Результати дисертаційної роботи опубліковано в 11 статтях у наукових журналах (з Переліку фахових) та 4 матеріалах наукових конференцій.

**Структура та обсяг дисертації.** Робота складається зі вступу, чотирьох розділів та висновків. Загальний обсяг дисертації складає 162 сторінки, з яких основний зміст викладено на 150 сторінках друкованого тексту, 15 рисунках, 4 таблицях. Список використаних джерел складається з 115 найменувань.

**ОСНОВНИЙ ЗМІСТ**

**У вступі** надана загальна характеристика роботи, актуальність проведених досліджень, мета і задачі, що підлягають рішенню, визначені новизна та практичне значення одержаних результатів.

**У першому розділі** зроблено аналіз методів і засобів захисту інформації в сучасних автоматизованих системах керування, тенденцій їхнього розвитку, можливих показників ефективності систем захисту ресурсів АСК, здійснено постановку задачі формалізації процесів технічного захисту їх ресурсів, запропонована узагальнена модель процесу захисту ресурсів АСК та його цільова функція, визначені умови доцільності застосування системи захисту та здійснено оптимізацію параметрів системи захисту.

Проведений аналіз методів і засобів захисту інформації в сучасних автоматизованих системах керування, тенденцій їхнього розвитку, їх зіставлення з вимогами існуючих стандартів та нормативних документів показали , що захист інформації в існуючих АСК чи в їх складових не може задовольняти всім сучасним вимогам до систем захисту. Тому зрозумілим є актуальність робіт із розроблення та впровадження комплексних систем технічного захисту ресурсів, насамперед інформації в АСК на базі локальних та розподілених інформаційно – обчислювальних мереж. При постановці задач розроблення комплексної системи захисту ресурсів АСК від НСД постає задача забезпечення оптимального (чи досягаємого) рівня ефективності системи захисту шляхом оптимізації витрат на створення та застосування засобів захисту АСК. В роботі запропонована система часткових кількісних характеристик захищеності: порушення конфіденційності інформації; порушення цілісності ресурсу (інформації); порушення доступності ресурсу (інформації). В якості комплексних кількісних характеристик захищеності запропоновано економічні показники: шкоду, яка завдається власнику АСК за рахунок реалізації загроз безпеці ресурсів АСК із – за недосконалості системи їх захисту (вираз 1), чи шкоду, яка запобігається при використанні системи захисту ресурсів АСК (вираз 2). Залежність вартісних показників захищеності від перелічених змінних в роботі пропонується розглядати як цільову функцію**,** а часові та інші характеристикивикористовувати як параметри (в деяких випадках – як обмеження) для оптимізації економічних (вартісних) показників ефективності**.** В якості таких параметрів управління (показників чи обмежень) в роботі запропоновано тривалість періоду (періодичність) контролю, тривалість відповідної процедури контролю та час затримки в наданні послуги, наприклад час затримки повідомлень в каналах зв’язку.

*MQ* = [*Gi·*(*Тkі*-Δ*Тkі*)·(1- *рвi*)+ *рвi·Сi·*Δ*Тkі*]. (1)

*MQзі =*{*Gi·Тkі·рi – [рi·Сi-Gi* (1-*рi*)]·[Δ*tkі*+Δ*tпі·рві*]}. (2)

де: і – номер загрози ресурсам АСК чи засобу протидії цій загрозі; n – кількість загроз; *Gi* – розмір шкоди (в умовних одиницях в одиницю часу), яка може бути завданою при вдалій реалізації кожного з типів загроз, *Сi* – шкода за рахунок простою відповідних ресурсів АСК під час контролю (в умовних одиницях в одиницю часу), *рвi –* ймовірність виявлення і подальшої протидії загрозі *і* – го типу, *Тkі* – період контролю; Δ*Тkі* – загальна тривалість і – го виду контролю; *Δtkі* – тривалість процесу контролю (пошуку факту порушення чи непорушення відповідної функціональної властивості захищеності автоматизованої системи); *Δtпі* – тривалість процесу поновлення цієї ж функціональної властивості.

Аналіз цих виразів дав можливість визначити умови доцільності застосування системи ТЗІ від загроз даного (і – го) типу у вигляді обмеження (вираз 3) на тривалість контролю Δ*Тkі* (при якимось чином визначеній величині *рi*) чи обмеження на ймовірність *рвi* (вираз 4)

Δ*Тkі* = Δ*tkі*+Δ*tпі·рві* < *Тkі ·*(*Gi /Сi*), (3)

*рвi* > Δ*Тkі*/[(*Тkі –* Δ*Тkі*)- Δ*Тkі*·(*Сi / Gi*)]. (4)

Подальшій аналіз цільової функції у вигляді (2) дав змогу знайти оптимальні параметри системи захисту – характеристики системи ТЗІ, в сенсі максимуму шкоди, яка запобігається завдяки застосуванню системи захисту. Визначено, що оптимальне значення параметру оперативного управління (Тkі) можна знайти з виразу (5)

*Тkі* = Δ*Тkі*+1/z+0,5, (5)

s= Δ*Т2kі*∙ (1+4*Cі/Gі*)+4(1/z2+ *Cі* ∙Δ*Тkі* /(*Gі*∙z)),

а величина z – результуюча інтенсивність загроз. Показано також, що для зменшення величини шкоди слід застосовувати чи розробляти засоби захисту з мінімально можливою тривалістю контролю Δ*Тkі*.

**У другому розділі** розроблено методику оцінки кількісного значення величини залишкового ризику при забезпеченні функціональних властивостей захищеності АС, яка передбачає наступні етапи: введення кількісних характеристик функціональних властивостей захищеності ресурсів АСК на основі визначених класу і структури таких АСК; оцінку можливості реалізації загроз ресурсам АСК; аналіз можливих наслідків від реалізації потенційних загроз, тобто оцінку можливого рівня заподіяної ними шкоди – можливого залишкового ризику.

Для вирішення першої задачі – визначення класу і структури АСК, інформаційні ресурси якої слід захищати, та введення кількісних характеристики функціональних властивостей захищеності системи з метою забезпечення інваріантності результатів досліджень щодо класу АСК, розглядається найбільш поширений клас АС – ієрархічна АСК на базірозподіленого багатомашинного багатокористувацького комплексу. Показано, що для кількісної оцінки залишкового ризику в таких АС можна використати величини ймовірностей порушення відповідних функціональних властивостей захищеності ресурсів *q****і*** (*і*=1–3), які є зворотними до введених в першому розділі величин *рві*.

Для оцінки можливості реалізації загроз ресурсам АСК запропоновано символьну модель порушника та загроз у табличному вигляді. Показано, що модель порушника повинна включати опис: категорій осіб, які можуть бути порушниками; припустимого (можливого) характеру навмисних дій з боку цих порушників; їх можливої кваліфікації та рівня можливостей; можливої метою порушника – зловмисника; характеру дій(випадкові, зловмисні, активні, пасивні, рішучі, терплячі та ін.); використовуємих методів і способів; місця здійснення порушення; можливостей ненавмисних порушників(авторизованих користувачів). Для створення моделі загроз ресурсам АСК проаналізовано можливі канали та основні види цих загроз та найбільш ймовірні властивості захищеності ресурсів, які порушуються внаслідок впливу загроз кожного з їх типів, тобто здійснено їх ідентифікацію – у вигляді переліку загроз з констатацією відповідності властивостям захищеності ресурсів АСК, на порушення яких вони спрямовані (порушення конфіденційності , цілісності, доступності, спостереженості та керованості АСК). Це дало змогу визначити найбільш небезпечні загрози та сформулювати рекомендації щодо спрямованості системи захисту на нейтралізацію саме цих загроз.

Ці рекомендації використано при розробленні моделей взаємодії засобів реалізації атак з засобами протидії цим загрозам - засобами забезпечення конфіденційності, цілісності та доступностіінформації, а також загальної моделі системи захисту інформації АСК. Аналіз таких моделей надав можливість сформулювати події, пов’язані з порушенням функціональних властивостей захищеності і отримати вирази для розрахунків кількісних значень (величин) залишкового ризику – величин ймовірностей порушення цих функціональних властивостей захищеності конфіденційності – *q1* (вираз 6), цілісності *q2* (вираз 7), доступності *q3* (вираз 8) та узагальнену оцінку захищеності інформаційних об’єктів Рзп (вираз 9):

q1 = 1–{1– Ркзі·[1– (1–Р1)·(1– Рзві)}·[1– Рккрз·Ракрз]], (6)

q2 = –{1 – Руд·[1–(1–Роод)·(1–Рос)]}·[1– Ркц]·[1– Рaкц·Рккц]. (7)

q3 = 1 – (1+λ3 tкр)∙exp(–λ3 tкр), (8)

Рзп = 1– Рпфх∙(1 – Рч). (9)

Р1 = Руфд·Рад·[1-(1-Роод)·(1-Рос)],

Ркзі = Рзм·Рзкп·Ркн,

λз = λсз + *λр3*,

*λр3 =* (λші(1– руд)+λі+λспРкпц·Рзсп)·(1–рв3) = (λшіРуд+λі+λспРкпц·Рзсп)·qп3,

Рпфх = 1– (1– q1)·(1– q2)·(1– q3),

де: Ркзі – ймовірність подолання засобів криптографічного захисту інформації; Р1 – ймовірність несанкціонованого отримання користувачем інформації при безпосередньому впливі, Рзві – ймовірність подолання засобів захисту від витоків інформації технічними каналами, Рккрз – ймовірність подолання неавторизованим користувачем засобів канального криптографічного захисту інформації в телекомунікаційних мережах (ТКМ), Ракрз – ймовірність подолання неавторизованим користувачем засобів абонентського криптографічного захисту інформації в ТКМ, Руд – ймовірність подолання засобів управління доступом, Роод – ймовірність подолання засобів організаційного обмеження доступу, Рос – ймовірність подолання засобів охоронної сигналізації, Ркц – ймовірність подолання засобів контролю цілісності інформації відповідного вузла; Рaкц – ймовірність подолання засобів абонентського контролю цілісності інформації в ТКМ; Рккц – ймовірність подолання засобів канального контролю цілісності інформації в телекомунікаційної мережі; λз – інтенсивність запитів на використання ресурсів АС, *tкр* середній час використання захищеного ресурсу; Руфд – ймовірність подоланні порушником засобів управління фізичним доступом, Рад – ймовірність подоланні порушником засобів адміністрування доступом, Рзм – ймовірність того, що порушник знає мову, якою інформація представляється, Рзкп – ймовірність того, що порушник знає і може застосувати програмні засоби або апаратуру для криптографічного перетворення (для дешифрування закритої інформації), Ркн – ймовірність того, що порушник має необхідні ключі (ключові набори) для такого перетворення; *руд* –ймовірність неподолання загрозами засобів управління доступом до захищених ресурсів; λсз – інтенсивність справжніх запитів, *λр3* – результуюча інтенсивність загроз захищеному ресурсу, *λші*–інтенсивність штучних впливів через засоби управління доступом; *λі* –інтенсивність природних впливів; *λсп* – інтенсивність спеціальних впливів по технічним каналам, Рзсп – ймовірність подолання засобів захисту від спеціального впливу на інформацію по технічним каналам; Ркпц – ймовірність подолання засобів контролю та поновлення цілісності інформації вузлів центрального, регіонального чи місцевого рівнів АС, Рпфх – ймовірність порушення функціональних властивостей захищеної системи; Рч – ймовірність того, що математичне сподівання часу функціонування власне засобів захисту tсз не перевищить час обробки впливів завад, безперервних запитів, спроб підбору паролів та т.п. tбз, тобто Рч = Р(tсз≤ tбз).

**Третій розділ** призначено питанням оцінки ефективності організації обміну в телекомунікаційних мережах на основі аналізу задач забезпечення цілісності та доступності інформаційних об’єктів в таких мережах, оцінки впливу способів організації обміну та можливих методів підвищення цілісності та доступності інформації в ТКМ на їх ефективність. Зроблено висновок про суттєву вразливість стану захищеності АСК як раз через телекомунікаційні мережі, канали обміну інформацією та через їх елементи, а, відтак, про актуальність та важливість досліджень та розробок щодо методів, способів, засобів та методик оцінки та забезпечення властивостей захищеності інформації в таких мережах, каналах обміну інформацією та їх елементах.

Для оцінки захищеності інформаційних ресурсів в телекомунікаційних мережах в даному розділі розроблено методики: оцінки цілісності інформаційних об’єктів в ТКМ при реалізації того чи іншого способу організації обміну. Оцінка цілісності здійснюється з використанням такої характеристики як правильність передачі даних (ймовірність правильної доставки повідомлення чи отримання на приймальному боці невикривленої інформації); а оцінка доступності ТКМ – через абсолютну швидкість обміну інформації в ТКМ та час затримки в доставлянні повідомлень при реалізації того чи іншого способу організації обміну; запропонована оцінка можливої шкоди із-зі неефективної організації обміну.

На основі аналізу топології ТКМ та потоків загроз тій чи іншій функціональній властивості захищеної системи чи її елементам задача забезпечення властивостей захищеності ресурсів ТКМ розподілена на: задачу забезпечення властивостей захищеності ресурсів в каналах (канальні цілісність та доступність) та задачу забезпечення властивостей захищеності ресурсів ТКМ вцілому (абонентські цілісність та доступність). Розглянута модель взаємодії засобів в процесі ТЗІ в телекомунікаційних системах дозволила отримати вирази для розрахунку результуючих інтенсивностей загроз доступності *λрд* (вираз 10), цілісності *λр*ц(вираз 11) ресурсів ТКМ та результуючу інтенсивність λн загроз, які не усунуті системою ТЗІ (вираз 12)

λрд = λшаРуд + λшк + λ, (10)

λрц = λшаРуд + λшк + λРккц (11)

λн =λрцРaкц = (λшаРуд + λшк + λ Рккц)∙Рaкц, (12)

де λша , λшк та λ – інтенсивності штучних впливів на абонентському та канальних рівнях ТКМ, а λ – інтенсивність природних загроз в ТКМ. Найбільший вплив на ресурси ТКМ, як витікає з виразу (12),слід очікувати від штучних впливів на канальному рівні,оскільки вони не зменшуються (не проріджуються) ніякими засобами, окрім засобів забезпечення цілісності ресурсів ТКМ на абонентському рівні, та особливу необхідність при цьому збільшення ймовірності виявлення та усунення впливу засобами абонентського контролю цілісності інформації (1-Рaкц).

Аналіз можливостей забезпечення цілісності інформації в умовах природних впливів (проблеми завадостійкості) для каналів ТКМ (взагалі для мереж передачі даних) надав можливість зробити висновок, що найбільш прийнятними для того класу АСК, який розглядається в роботі, є способи з використанням зворотного вирішуючого зв’язку (ЗВЗ) та способи з використанням завадостійких корегуючих кодів (ЗКК). Для їх більш ретельного порівняння здійснено порівняння цих способів за абсолютною швидкістю передачі даних (вирази 13, 14) та ймовірністю правильної доставки повідомлення (вирази 15, 16) при використанні при обміні зворотного вирішуючого зв’язку та корегуючих кодів відповідно:

Вазвз = exp(–λtпk)∙m/{n/В+ Δtк1+Δtп1∙(1–exp(–λtпk))} (13)

Bазкк = (1+*λtпk*)exp(–*λtпk*)∙*mзкк/*{*n/В+ Δtк*2+*Δtп*2∙(1–exp(–*λtпk*))}, (14)

де відповідно: λ – інтенсивність впливів; tпk – часова тривалість (*tпk =* n/В) повідомлення в канальній ланці захисту; n, m, mзкк – загальна кількість та кількість інформаційних символів в повідомленнях; В – технічна швидкість передачі даних; (∆tк1 ) ∆tк2 – час, потрібний для контролю цілісності повідомлень; (*∆tп*1) *∆tп*2∙– час, потрібний для виправлення викривлень в повідомленні (в разі їх виявлення).

На підставі аналізу цих виразів визначено межі більшої ефективності способів організації обміну із ЗВЗ по швидкості передачі порівняно із способами організації обміну із ЗКК (при доброму стані каналу – малому значенні *λ<λгр*1, де *λгр*1 – така величина інтенсивності впливів, при якій абсолютні швидкості передачі інформації для різних методів організації обміну є однаковими). Окрім того, при наближенні надлишковості mзкк до m величина *λгр*1 наближається до нуля, тобто діапазон значень інтенсивностей впливів, при яких способи організації обміну із ЗКК є більш прийнятними. Показано, що ймовірність правильної доставки повідомлення при використанні при обміні зворотного вирішуючого зв’язку та корегуючих кодів відповідно можна оцінити із виразів

Рзвз = 1–2–(n–m) = const, (15)

Рзкк = (1–2–(n–m1))·(1+ λn /В)·exp{– λn /В}, (16)

де *m*1 = *mзкк*. При цьому способи організації обміну із ЗКК дещо перевершують способи організації обміну із ЗВЗ лише тоді, коли інтенсивність впливів *λ* є незначною (*λ<λгр*2), в решті випадків канали з ЗВЗ є, з погляду цього показника, більш ефективними.

Таким чином, виходячи з аналізу цих двох окремих показників, неможливо віддати незаперечну перевагу тому чи іншому способу організації обміну даними, оскільки спосіб більш ефективний за одним показником є менш ефективним за іншим. Тому в роботі введено комплексний показник ефективності у вигляді добутку швидкості на ймовірність правильної доставки повідомлення – ефективну швидкість обміну *Е*. Вирази для розрахунків такої ефективної швидкості для способів організації обміну із ЗВЗ мають вигляд (вирази 17, 18):

*Езвз ≈ Ва =* exp(–*λtпk)*∙*m/*{*n/В+ Δtк*1+*Δtп*1∙(1–exp(–*λtпk*))} (17)

*Езкк* ≈(1+*λn/В*)·*exp*{–*λn/В*}∙(1+*λtпk*)exp(–*λtпk*))∙*mзкк/*(*n/В+ Δtк*2+*Δtп*2∙(1–exp(–*λtпk*))). (18)

З аналізу цих залежностей витікає, що ефективна швидкість способів організації обміну із ЗКК переважає ефективність способів організації обміну із ЗВЗ, коли інтенсивність впливів *λ* є більшою за деяке її граничне значення *λгр*. Визначено граничні значення інтенсивність впливів *λ* для абсолютної та ефективної швидкостей.

Останні вирази дозволяють в залежності від стану каналів вибирати чи один, чи інший спосіб організації обміну, чи побудувати адаптивні комбіновані системи передачі даних, в яких залежно від інтенсивності завад використовується режим роботи або із ЗВЗ, або із ЗКК, тобто можна побудувати комбіновануСПД. Аналогічні висновки витікають і з проведеного в даному розділі аналізу залежності часу затримки доставки повідомлення від інтенсивності впливів для різних способів організації обміну. Показано напрямки підвищення ефективності обміну інформацією в ТКМ.

Для оцінки методів підвищення цілісності та доступності інформації в ТКМ, варіантів побудови ТКМ з мінімізованим значенням можливої шкоди розглянуто загальну модель ТКМ в розумінні складу та взаємних зв’язків засобів захисту інформації в ТКМ та методику оцінки ефективності обміну в телекомунікаційних мереж в розумінні можливої шкоди.

**У четвертому розділі** розроблено метод забезпечення цілісності інформаційних ресурсів АСК на основі завадостійкого корегуючого ЛУ–коду та методики його використання, які забезпечують застосування погоджених між собою швидкодіючих процедур як виявлення порушення цілісності інформації, так і її поновлення. З цією метою здійснено аналіз можливостей цього коду по виявленню, корекції порушень цілісності в умовах зберігання чи передавання інформаційних об’єктів, потрібної при цьому надлишковості та імітостійкості, яка забезпечується при застосуванні розробленого методу. Показано, що запропонований код в поєднанні з умовним перемежуванням дозволяє використовувати надзвичайно прості алгоритми кодування та декодування, які можливо застосовувати для визначення наявності викривлень та їх корекції суто розрахунковими процедурами, тобто без використання для поновлення засобів резервного копіювання, причому з забезпеченням унеможливлення наявності таких викривлень, які порушник навмисно приховує. При цьому імітостійкість механізмів контролю цілісності інформації визначається стійкістю обчислень контрольних ознак, яка залежить від довжини вибраних ключів захисту (кількості основ – констант ЛУ – коду), а також від статистичної пов’язаності початкового тексту (інформаційного блоку) з його перетвореним відображенням. Показано, що при контролі та поновленні цілісності запропонований механізм забезпечує кількість варіантів ключів, яка суттєво перевищує кількість варіантів ключів відомих механізмів, та має, відповідно, значно вищу імітостійкість. Ця кількість варіантів ключів задовольняє вимогам навіть гарантованого криптозахисту. При цьому методика застосування ЛУ – коду для контролю цілісності інформаційних об’єктів передбачає виконання наступної послідовності процедур: відокремлення від інформаційного об’єкту його певної частини – узагальненого кодового слова довжиною *N* інформаційних символів (*N*–число байтів в узагальненому кодовому слові (в блоці інформації)). формування контрольних ознак базових кодових слів; формування контрольних ознак узагальнених кодових слів; формування контрольних ознак інформаційного об’єкту, наприклад деякого (*і*–го) файлу чи інформаційного набору; організацію контролю цілісності інформаційного об’єкту**;** організацію поновлення цілісності інформаційного об’єкту. В розділі наведено необхідні для цього формульні вирази та співвідношення.

**ВИСНОВКИ**

В процесі виконання дисертаційної роботи отримані наступні результати:

1. Запропоновано кількісні характеристики захищеності інформації в АСКу вигляді імовірнісних, вартісних (економічних) та часових показників забезпечення відповідних функціональних властивостей захищеності інформації (конфіденційності, цілісності, доступності) засобами системи технічного захисту інформації (ТЗІ). Розроблено математичні моделі процесів захисту інформаційних ресурсів АСК та на їх основі визначено цільову функцію таких процесів. Сформулювано умови економічної доцільності застосування систем ТЗІ та визначено обмеження на основні їх характеристики. Отримано функціональні залежності для визначення оптимальних значень параметрів системи ТЗІ. Сформулювано умови мінімізації тривалості процедур виявлення та усунення порушень властивостей інформаційних ресурсів АСК.
2. Для інформаційних ресурсів АСК розроблено моделі порушників та на їх основі здійснено аналіз загроз і можливих наслідків від реалізації потенційних загроз (аналіз залишкового ризику), як базис для формування моделей забезпечення захищеності інформації в АСК. Розроблено математичні моделі взаємодії засобів реалізації загроз кожній з функціональних характеристик захищеності інформації (конфіденційності, цілісності, доступності тощо) та засобів протидії цим загрозам. Запропоновано методики розрахунку величин залишкового ризику у вигляді ймовірностей подолання порушником засобів захисту відповідних функціональних властивостей.
3. Визначено потрібний склад заходів та засобів для забезпечення кожної з властивостей захищеності АСК та розроблено узагальнену модель взаємодії атак та засобів захисту інформаційних ресурсів АСК. Окрім імовірнісних та часових характеристик конфіденційності, цілісності і доступності запропоновано узагальнені кількісні характеристики системи захисту, а саме: – ймовірність порушення функціональних властивостей захищеної системи; – час затримки при використанні авторизованими користувачами ресурсів автоматизованої системи з засобами захисту порівняно з випадком, коли такі засоби відсутні.
4. Доведено актуальність та важливість застосування результатів досліджень та розробок щодо методів, способів, засобів та методик забезпечення захищеності інформації в телекомунікаційних мережах (ТКМ), підсистемах, каналах обміну інформацією та їх елементах. Запропоновано моделі заважаючих впливів на інформацію в елементах ТКМ та взаємодії цих впливів з засобами ТЗІ. На їх основі сформульовані задачі:

забезпечення захищеності ресурсів в каналах (канальні цілісність та доступність) та забезпечення захищеності ресурсів ТКМ в цілому (абонентська цілісність та доступність);

забезпечення цілісності і доступності інформації (задачі забезпечення правильності та мінімального часу затримки інформації).

1. Запропоновано оцінки способів організації та реалізації ефективного інформаційного обміну в телекомунікаційних мережах сучасних ієрархічних АСК з погляду забезпечення цілісності та часу доставки повідомлень (як однієї з кількісних характеристик доступності), визначено способи організації обміну, які забезпечують удосконалення та підвищення рівня захисту інформаційних об’єктів (інформаційних повідомлень) під час обміну.
2. Здійснено аналіз впливу способів організації обміну в ТКМ на показники захищеності інформаційних об’єктів, зокрема на цілісність та доступність інформаційних повідомлень (через час затримки доставки повідомлення). Показано, що способи (протоколи) організації обміну з використанням завадостійких корегуючих кодів підвищують ефективність ТКМ порівняно із іншими.
3. Запропоновано використання завадостійкого корегуючого ЛУ–коду для контролю та поновлення цілісності інформаційних об’єктів та лише контролю цілісності; розроблено методики його звживання, які розраховані на різні умови застосування, складність та потрібну надлишковість.

**ПУБЛІКАЦІЇ ПО ТЕМІ ДИСЕРТАЦІЇ**

1. Будько М.М., Волков О.М. ,Короленко М.П. Принципи побудови систем захисту інформації в різнорідних автоматизованих системах //Правове, нормативне та метрологічне забезпечення Системи захисту інформації в Україні. – К. НТУ “КПІ”. – 1998, – С. 123 – 129.
2. Будько М.М., Василенко В.С., Короленко М.П. Варіант формалізації процесу захисту інформації в комп’ютерних системах та оптимізації його цільової функції // Реєстрація, зберігання і обробка даних. – 2000. – Т. 2, № 2. – С. 73 – 84.
3. Будько М.М., Василенко В.С., Короленко М.П. Проблеми забезпечення цілісності інформації в телекомунікаціях // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – К.: НТУ “КПІ”. – 2000. – С. 123 – 129.
4. Будько М.М., Василенко В.С., Короленко М.П. Ефективність забезпечення цілісності інформації у телекомунікаціях. // Реєстрація, зберігання і обробка даних. – 2000. – Т. 2, № 3. – С. 43 – 65.
5. Будько М.М., Василенко В.С., Короленко М.П. Управління контролем та оперативним поновленням цілісності інформації в корпоративних мережах..// УСиМ. – 2000. – № 5/6. – С.128 – 134.
6. Будько М.М., Василенко В.С., Балидін Р.М. Варіант підвищення швидкості формування ознак цілісності в механізмах контролю цілісності. // Правове, нормативне та метрологічне забезпечення Системи захисту інформації в Україні. – К.: НТУ “КПІ”. – 2001. – Вип. 2, С. 137 – 140.
7. Будько М.М. Василенко В.С., Короленко М.П. Система захисту інформації від НСД “Рубіж”. Практичні аспекти реалізації концепції централізованого управління безпекою корпоративної системи. // Правове, нормативне та метрологічне забезпечення Системи захисту інформації в Україні. – К.: НТУ “КПІ”. – 2002. – Вип. 4. С. 154 – 161.
8. Будько М.М., Василенко В.С., Короленко М.П. Механізми контролю цілісності інформації та її поновлення // Правове, нормативне та метрологічне забезпечення Системи захисту інформації в Україні. – К.: НТУ “КПІ”. – 2000. – С. 130 – 139.
9. Будько М.М., Василенко В.С., Короленко М.П. Архитектура системы технической защиты информации. К.: НТУ “КПІ” //Правове, нормативне та метрологічне забезпечення Системи захисту інформації в Україні. – К.: НТУ “КПІ”. – 2000, С. 62–68.
10. Будько М.М. Василенко В.С., Короленко М.П., Матов О.Я., Дмитрук Ю.В. Архитектура системы защиты информации для АС. // “Безопасность информационных технологий. Методология создания систем защиты. Часть V. Решения и средства защиты информации. – К.: ООО “ТИД “ДС”, 2001. –
С. 528 –533.
11. Будько М.М. Василенко В.С., Короленко М.П. Контроль и восстановление целостности информации в автоматизированных системах. // Правове, нормативне та метрологічне забезпечення Системи захисту інформації в Україні. К.: НТУ “КПІ”. – 2002, Вип. 4. С. 119-128.

**АНОТАЦІЇ**

***Будько М.М. Методи підвищення захищеності інформаційних ресурсів автоматизованих систем спеціального призначення та оптимізації структур систем їхнього технічного захисту. –*** Рукопис.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – “Cистеми захисту інформації”. – Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, Київ, 2002.

У дисертації розглянуті питання вибору показників ефективності систем захисту, оптимізації їх параметрів, оцінки множини можливих загроз, побудови моделей процесів та засобів захисту, визначення часткових та узагальнених кількісних оцінок захищеності інформаційних об’єктів. Показана їх суттєва залежність від захищеності інформаційних об’єктів в телекомунікаційних мережах. Здійснена оцінка впливу способів організації обміну на захищеність інформаційних об’єктів в телекомунікаційних мережах та оцінка методів підвищення їх цілісності та доступності. Розроблена методика оцінки можливої шкоди через за неефективний обмін. Розроблені методи та механізми контролю цілісності інформаційних ресурсів автоматизованих систем на основі завадостійкого корегуючого коду та методики застосування цих методів. Здійснено оцінку імітостійкості запропонованого механізму та його можливостей щодо контролю та поновленню цілісності інформаційних об’єктів.

Ключові слова: безпека інформації, загрози безпеці, характеристики захищеності, залишковий ризик, цілісність, доступність, телекомунікаційні мережі.

***Budko M.M. Methods for information resources security increasing in special – purpose control systems and its protection systems optimization. –*** Manuscript.

Thesis for a candidate’s degree by speciality 05.13.13 – Information security systems. – The G.E. Pukhov’s Institute of Simulation Problems in Power Engineering of National Academy of Sciences of Ukraine, Kyiv, 2002.

The thesis is devoted by the problems of indicators choosing for protection systems, their parameters optimization , rating of set of probable threats, build-up of the partial and generalized quantitative estimates of information objects hardening. Their essential dependence on hardening of information objects in telecommunication networks is exhibited. The rating of influence of ways of organization of exchange on hardening of information objects in telecommunication networks and rating of methods of their integrity increasing and availability is realized. The technique of a rating of possible damage owing to ineffective exchange is designed. The methods and mechanisms of a control of integrity of information resources of the control systems are designed on the basis of the noise-resistant correcting code and technique of application of these methods. The estimate of resistance to cloning of the offered mechanism and possibilities on a control and restoration of integrity of information objects is realized.

Keywords: information security, safety threats, protection characteristics, residual risk, wholeness, availability, telecommunication nets.

***Будько Н.Н. Методы повышения защищенности информационных ресурсов автоматизированных систем специального назначения и оптимизации структур систем их технической защиты.*** – Рукопись.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.21 – Системы защиты информации. – Институт проблем моделирования в энергетике им. Г.Е. Пухова НАН Украины, Киев, 2002.

В диссертации рассмотрены вопросы выбора показателей эффективности систем защиты, оптимизации их параметров. Введены количественные характеристики защищенности информации в АСУ в виде вероятностных, стоимостных (экономических) и временных показателей обеспечения защищенности средствами системы ТЗИ соответствующих функциональных свойств защищенности информации (конфиденциальности, целостности, доступности). Введены модели процессов защиты информационных ресурсов АСУ в наиболее обобщенном виде и на их основе определена целевая функцию такого процесса. Сформулированы условия экономической целесообразности применения систем ТЗИ и ограничения на основные их характеристики. Получены выражения для определения оптимальных значений параметров системы ТЗИ. Обосновано и сформулировано требование минимизации продолжительности процедур выявления нарушений целостности информационных ресурсов АСУ и их устранения.

Произведена оценка множества возможных угроз, предложены модели процессов взаимодействия угроз и средств защиты, определены частные и обобщенные количественные оценки защищенности информационных объектов. Показана их существенная зависимость от защищенности информационных объектов в телекоммуникационных сетях. Определен возможный состав способов и средств обеспечения любого из свойств защищенности АСУ и разработана обобщенная модель взаимодействия атак и средств защиты ресурсов АСУ. Получены, кроме частных вероятностных и временных характеристик конфиденциальности, целостности и доступности, также обобщенные количественные характеристики системы защиты – вероятность нарушения функциональных свойств защищенной системы, время задержки доступа к ресурсам автоматизированной системы авторизованными пользователями при использование средств защиты по сравнению с ситуацией, когда такие средства отсутствуют.

Сделан вывод об актуальности и важности исследований и разработок относительно методов, способов, средств и методик обеспечения свойств защищенности информации в телекоммуникационных подсистемах (ТКПС), сетях, каналах обмена информацией и их элементах. Предложены модели воздействий угроз на элементы ТКПС и взаимодействия средств в процессе ТЗИ и на их основе сформулированные задачи обеспечения защищенности ресурсов в каналах (канальные целостность и доступность) и обеспечение защищенности ресурсов ТКПС в целом (абонентские целостность и доступность) – задачи обеспечения целостности и доступности информации (задачи обеспечение правильности и минимального времени задержки информации).

Осуществлена оценка влияния способов организации обмена на защищенность этих информационных объектов и оценка методов повышения их целостности и доступности. Разработана методика оценки возможных потерь из – за неэффективного обмена. Разработаны методы и механизмы контроля целостности информационных ресурсов автоматизированных систем на основе помехоустойчивого корректирующего кода и методики применения этих методов. Осуществлена оценка имитостойкости предложенного механизма и его возможностей по контролю и восстановлению целостности информационных объектов.

Ключевые слова: безопасность информации, угрозы безопасности, характеристики защищенности, остаточный риск, целостность, доступность, телекоммуникационные сети.

Підписано до друку 03.10.2002

Формат 60×90/.16. Папір друк № 2.

Умовн. друк. арк. 0,75. Обл.–вид. арк. 0,75.

Тираж 100 прим. Зам.

Відділ випуску документів ВАТ “КП ОТІ”

03115, м. Київ, вул. Ф. Пушіної, 30/32