управлять системой с любого из узлов с минимальным риском выполнения ошибочных действий; б) производит автоматический мониторинг состояния геокластера с немедленным уведомлением администратора о любых отклонениях от штатного режима работы; в) поддерживает постоянство внутренней среды системы (ротация системных журналов, удаление "забытых" временных файлов, и т. д.); г) предоставляет администратору средства автоматического и ручного резервного копирования/восстановления данных приложения. Следует отметить, что система резервного копирования является необходимым компонентом системы любого уровня надежности, поскольку является практически единственным средствам восстановления в случае человеческих ошибок.

Разработанные сценарии восстановления предоставлены заказчику в виде документа "План восстановления в аварийных ситуациях". Документ регламентирует необходимую реакцию персонала в случае возникновения аварийных ситуаций различного характера, в том числе отказа отдельных аппаратных компонент, обратимого и необратимого отказа узлов, ошибок оператора. Для каждого случая предусмотрены три этапа реагирования: идентификация проблемы на основе имеющихся симптомов, восстановление сервиса, восстановление штатного режима работы. Эффективность разработанных процедур была подтверждена в ходе проведенных со специалистами заказчика практических занятий по отработке сценариев восстановления в критических ситуациях.

V Выводы

Практический опыт, накопленный в процессе создания катастрофоустойчивой системы, позволяет нам сделать следующие выводы.

1. В настоящее время технология создания устойчивых к катастрофам систем в достаточной степени востребована и, что не менее важно, доступна на отечественном рынке.
2. Средства и технологии, используемые при создании географических кластеров, могут варьироваться в широких пределах и определяются, прежде всего, предъявляемыми к системе требованиями и особенностями целевого приложения.
3. Активация резервного центра является неэффективными методом восстановления в случае одиночных отказов аппаратных компонент. Устойчивость системы к подобным авариям должна достигаться в рамках каждого центра (площадки) резервированием оборудования или применением классических высокодоступных кластеров.
4. Вне зависимости от применяемого решения требуется существенная привязка конфигурации геокластерной системы к местным условиям, а также разработка специфических сценариев восстановления в критических ситуациях. Указанные сценарии в сочетании с дополнительным управляющим программным обеспечением, разработанным с учетом местных условий, позволяют добиться необходимой степени эффективности реакции обслуживающего персонала на аварийные ситуации.

Литература: 1. Geographic Remote Mirror for AIX V2R3.0: Concepts and Facilities – IBM, 2001-44 p. 2. К. Вахрамеев. Защита данных от катастроф // Открытые системы, №3 – 2000.

УДК 681.321;322:621.395

АНАЛІЗ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ УПРАВЛІННЯ ПРИ МОДЕРНІЗАЦІЇ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Микола Тардаскін, Володимир Кононович

Одеський регіональний центр технічного захисту інформації ВАТ "Укртелеком"

Анотація: **Аналізується проблема захисту інформації в автоматизованих систем управління, що впроваджуються при модернізації діючих систем телекомунікацій, Розглядається класифікація порушників та загроз інформації, порівнюються засоби захисту, рекомендується склад комплексу засобів захисту від несанкціонованого доступу.**

Summary: **An article the problem of security in automated management systems that are being incorporated in the acting systems of telecommunication in case of their enhancement is analyzed. Also, the classification of threats and users violator is considered. The protection facilities are compared and a list of such facilities from unauthorized access is recommended.**

Ключові слова: **Безпека інформації, автоматизована система управління, показники захищеності.**

І Вступ

В телекомунікаційних мережах загального користування інтенсивно проводиться модернізація обладнання, яке не виробило свій ресурс. Автоматизуються технологічні процеси, локальні системи управління, системи тарифікації, контролю тощо. При впровадженні систем автоматизації у телекомунікаціях першочергова увага приділялась технологічним вдосконаленням без достатньої уваги до вимог безпеки інформації. Недостатньо пророблені питання політики безпеки інформації у телекомунікаціях, де були б сформульовані вимоги до захисту інформації від загроз працездатності, підтримання режиму конфіденційності та відсутності несанкціонованого доступу [1]. Загрози захищеності розширюються при інтеграції у телекомунікаційні комплекси нових функцій, застосуванні мережевих обчислювань, програмно-апаратних комплексів, мереж автоматизованого управління електрозв'язком. Почастішали випадки несанкціонованого використання ресурсів операторів для нелегального надання послуг зв'язку, що знижує доходи та приводить до економічних втрат і перевантаження мережі загального користування. Тому аналіз захищеності інформації – складової частини проблеми пошуку шляхів вдосконалення телекомунікаційних систем, є актуальною задачею.

Впроваджувані системи автоматизації, як правило, є розподіленими системами збору та обробки інформації і виконують схожі функції. Типовим прикладом може бути система "Автоматизованого погодинного обліку розмов" (АПОР), яка стала невід'ємною частиною аналогових АТС (автоматичних телефонних станцій), або система контролю і управління таксофонами. Такі системи призначені для автоматичного обліку вартості місцевих, міжміських та міжнародних телефонних переговорів, формування сигналів для автоматичного визначення номера абонента, діагностики. База даних системи містить інформацію щодо: кількості та сумарної тривалості, часу та номеру набору переговорів; несправності розмовного тракту АТС (абонентських та шнурових комплектів) і таксофонів; даних навантаження абонентських комплектів; присвоєних категорій абонентів; технічного стану самої системи. Система АПОР дозволяє здійснювати з віддаленої центральної станції обмежене управління характеристиками АТС: пріоритетом доступу абонента до міжміської телефонної мережі, постановкою абонентської лінії під контроль, тарифікацією, обмеженням вихідного зв'язку.

Системи автоматизації побудовані за радіальним принципом. Так індивідуальні контролери системи АПОР встановлюються на штативах абонентських комплектів (АК) для контролю 160 каналів. Центральний контролер у комплекті з персональною обчислювальною машиною (ПЕОМ) проводить збір, накопичення, обробку, відображення інформації та забезпечує її передачу до центру тарифікації та аналізу. ПЕОМ встановлюється на робочому місці диспетчера. Індивідуальні контролери зв'язані радіальними лініями з центральним контролером. У свою чергу центральні контролери зв'язані міжстанційними лініями з центральною станцією, яка проводить аналіз, тарифікацію та видачу рахунків абонентам.

Пристроєм обробки інформації в системах автоматизації є ПЕОМ із стандартною архітектурою, для якої можливо створювати засоби нападу, віруси тощо. Така система вносить додаткові канали витоку інформації в мережі загального користування або АТС. У базі даних системи концентрується інформація з управління, абонентів, обладнання станцій та їх поточного стану. Порушник може аналізувати активність абонента, коло його респондентів, економічні інтереси, звички тощо.

Під загрози безпечного функціонування підпадає програмне забезпечення (ПЗ) автоматизованих робочих місць (АРМ), особливо якщо вони функціонують на базі ПЕОМ та використовують для роботи операційну систему Windows або MS-DOS. Функціональне та спеціалізоване ПЗ, як правило, зашите у постійні запам'ятовуючі пристрої, а проникнення у спеціалізовану операційну систему вважається практично неможливим.

Відповідно до задачі захисту інформації, за сукупністю характеристик (конфігурації апаратних засобів, операційним системам, їх фізичного розміщення, кількості різноманітних категорій інформації, що обробляється, кількості та категорій користувачів) система автоматизації класифікується згідно з [2] за класом "3" – розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності. Локальні частини систем автоматизації, що розташовані у межах станції і не мають з'єднань, що виходять за межі охороняємої території, класифікуються за класом "2" – локалізований багатомашинний багатокористувачевий комплекс, що обробляє інформацію різних категорій конфіденційності.

ІІ Класифікація порушників

Класифікація порушників для традиційної АТС наведена у [3]. Класифікація проводиться за рівнем можливостей, що надаються їм штатними засобами і може бути застосована до систем автоматизації, що

розглядаються. Для системи автоматизації виділяють чотири рівні можливих порушень (з найнижчого рівня до найвищого).

1 – запуск програм (задач) із фіксованого набору, що реалізує передбачені функції з обробки інформації. Це обслуговуючий персонал, що забезпечує експлуатацію обладнання системи. Інженери-електрики, користуючись АРМ, можуть мати доступ до інформації про абонента. Вони мають можливість підключати до системи автоматизації закладні пристрої.

2 – можливість створення та запуску власних програм з новими функціями з обробки інформації. Це оператори АРМ, центральної станції або інших вузлів комутації. Користуючись комплектом або модемом на з'єднувальній лінії, вони мають доступ до ПЗ АРМ, функціонального та спеціалізованого ПЗ та до баз даних, можуть використовувати можливості у передачі сигналів, передбачені та не передбачені у відповідних інтерфейсах.

3 – можливість управління роботою системи, тобто можливість впливу на базове ПЗ системи та на склад і конфігурацію обладнання. Це диспетчери системи автоматизації. Користуючись АРМ, вони мають доступ до баз даних, ПЗ АРМ, функціонального та спеціалізованого ПЗ та інформації про абонентів. Типові можливості такого порушника: формування штатних команд, запуск задач, не декларованих у технічній документації, несанкціоноване приєднання до інформаційних трактів.

4 – весь обсяг можливостей суб'єктів, що здійснюють проектування, реалізацію та ремонт технічних засобів, до включення у склад обладнання власних технічних засобів з новими функціями. Це програмісти, що приймають участь у розробці та виготовленні системи. Користуючись АРМ і пристроями управління, вони можуть впливати на функціональне та спеціалізоване ПЗ і на ПЗ АРМ. Типові можливості такі: впровадження програмних закладок, впровадження шкідливих кодів (вірусів), помилки у ПЗ та системі.

До потенційних порушників можна не відносити абонентів. Якщо на вузлі комутації та системі автоматизації нема програмних та апаратних закладок, то абонент практично не має можливості впливати на систему управління. Регламентовані для кінцевих терміналів користувачів основні та додаткові послуги не можуть впливати на роботу управляючого комплексу в цілому. Абонент може діяти тільки через абонентський комплекс. У нього можуть бути можливості активізувати програмну закладку, отримати інформацію інших абонентів при несправності обладнання системи.

Можливості здійснення загроз залежать від місцезнаходження порушника. Якщо порушник знаходиться поза межами станції, то його можливості залежать від того, чи є засоби захисту при модемному підключенні до мережі, засоби безпеки при реалізації систем тарифікації (допускається чи не допускається віддалене підключення легальних користувачів до системи тарифікації), засоби безпеки при виході до системи управління.

Якщо таких засобів захисту немає, то можливі впливи порушника через зовнішні інтерфейси системи автоматизації, системи сигналізації на абонентських та з'єднувальних лініях. Системи сигналізації забезпечують передачу різноманітних сигналів управління, у тому числі цифр номера, які через функціональні елементи комутаційної системи поступають для аналізу в систему автоматизації. При цьому для активізації програмних закладок можливі різні варіанти використання сигналів управління, наприклад, такі: режиму типу "додаткова послуга", що не декларується в документації; абонентського номера або коду для активізації програмної закладки.

З розширенням цифрової частини мережі загального користування буде створюватись мережа спільно-канальної сигналізації № 7 (СКС-7), яка буде використовуватись на напрямках між цифровими АТС, опорно-транзитними станціями, міжнародними центрами комутації. Система сигналізації СКС-7, крім вище названих можливостей, потенційно надає додаткові можливості організації несанкціонованого доступу (НСД). У складі СКС-7 є підсистеми забезпечення можливостей транзакцій (TCAP) та прикладних підсистем, що організуються на них, таких, як підсистема рухомого зв'язку GSM (MAP), підсистема інтелектуальних мереж (INAP), підсистема експлуатації, техобслуговування і адміністративного управління (OMAP) та інші. Інтерфейси, спеціалізовані для нетелефонних функцій (TCAP, OMAP та інші) системи СКС-7, можуть бути використані для прихованого вводу команди, що реалізує несанкціонований вплив на АТС. У СКС-7 організується доступ до мережевих баз даних. Виникає загроза їх навмисного спотворення, що може викликати порушення в роботі мережі.

Якщо порушник розташований всередині станції, то у нього багато можливостей здійснення загроз, навіть за наявності засобів захисту при підключенні до мережі, засобів безпеки при реалізації систем автоматизації, засобів безпеки при виході на мережу управління. Порушник з правами диспетчера системи автоматизації може здійснювати НСД шляхом формування штатних команд, запускати програми, не регламентовані в технічній документації. Порушення доступу може полягати в:

- модифікації баз даних (установка несанкціонованих режимів технічної експлуатації та видів обслуговування);

- ознайомленні з конфіденційною інформацією баз даних (номеронаборами вхідних та вихідних з'єднань, часом встановлення з'єднання, додатковими видами обслуговування, що використовуються);

- зупинці та перезапуску системи автоматизації, що може спричинити втрату процесу тарифікації та управління;

- заміні ПЗ (нове інстальоване ПЗ може мати програмні закладки та "люки").

III Склад комплексу засобів захисту від НСД

У комплексах систем автоматизації реалізовано обмежений захист даних від НСД. Основними засобами захисту інформації є розмежування доступу до АРМ та система ідентифікації при обміні каналами зв'язку.

На АРМ при роботі з конфіденційною інформацією передбачено дві ролі: адміністратора та користувача. Адміністратор має доступ до всіх даних. Користувач при звертанні до закритої інформації вводить ідентифікатор і пароль.

Якщо пароль складається із p символів з алфавіту (множини) потужністю P, а кожна спроба розкрити пароль шляхом звертання до системи вимагає часу t, то ймовірність розкриття паролю за час T при умові, що він не змінюється за цей час [4]

$$1 - k_{зр} = T / tP^p . \tag{1}$$

Розрахунки показують, що довжину пароля необхідно вибирати не менше 7 – 8 символів, а період його зміни не більше 90 діб.

Ідентифікація користувача при віддаленому доступі та ідентифікація обладнання при обміні каналами зв'язку між центральною станцією та центральними контролерами також виконується за допомогою паролю. При мережевому обміні передбачено посилку спеціальної кодової комбінації центральному контролеру у пакеті запиту на видачу інформації. Ця кодова комбінація грає роль паролю. Якщо пароль не вірний, то обмін забороняється. Паролі абонентів мають довжину 2 байти. Масиви цих паролів передаються каналами міжпроцесорного зв'язку у складі інформаційних блоків із побайтовим захистом на парність. Застосований захист від НСД до абонентських ліній дозволяє на 5 – 10% зменшити втрати від сторонніх підключень.

Для аналізу ефективності ідентифікації при обміні на міжстанційних лініях розглянемо математичне очікування часу розкриття паролю [4]

$$M[T] = 0.5 A^s l / c \tag{2}$$

Якщо порушник підключається до мережевої лінії, якою передаються дані зі швидкістю c = 9,6 Кбіт/с, а довжина файлу (пакету) l = 57 Кбайт, то середній час розкриття при довжині паролю s = 16 біт становить приблизно 60 годин, що явно недостатньо. Розкривши пароль, порушник може перехопити канал зв'язку та отримати всі файли. Доцільно розглянути використання криптографічного захисту цифрової інформації за умови витрати невеликої частки ресурсів системи автоматизації. Інформацію практично неможливо розшифрувати, якщо порушнику недоступні декілька копій одного і того ж зашифрованого повідомлення або початкового та зашифрованого повідомлення. Тому шифрування поєднують із організаційними та фізичними заходами захисту та застосовують комплексні підходи до створення системи захисту інформації від НСД.

В Україні започатковано власне виробництво захищених від витоку каналами побічних електромагнітних випромінювань і наводок (ПЕМВН) засобів обчислювальної техніки, програмно-апаратних засобів захисту, активних засобів захисту інформації, пристроїв захисту інформації в телефонних лініях та ін. Є можливості реалізувати функціональний профіль захищеності, що задовольняє задані вимоги щодо захищеності інформації.

Комплекс заходів захисту (КЗЗ) системи автоматизації, крім вимог щодо блокування технічних каналів витоку, має відповідати вимогам, сформульованим в [2], а саме вимогам до конфіденційності, доступності та спостереженості.

КЗЗ системи автоматизації вибраного функціонального профілю захищеності має реалізувати такі послуги з захисту інформації:

1) надавати послуги з захисту об'єктів від несанкціонованого ознайомлення з їх змістом (компрометації) (конфіденційність забезпечується такими послугами: КА-1 – мінімальна адміністративна конфіденційність, КО-1 – повторне використання об'єктів);

2) надавати послуги з захисту оброблюваної інформації від несанкціонованої модифікації (цілісність може забезпечуватись послугою ЦА-1 – мінімальна адміністративна цілісність);

3) надавати послуги щодо забезпечення можливості використання системи автоматизації в цілому, окремих функцій або оброблюваної інформації на певному проміжку часу і гарантувати спроможність системи автоматизації функціонувати у випадку відмови її компонентів (доступність може забезпечуватися в КС послугою ДВ-1 – ручне відновлення після збоїв);

4) надавати послуги з забезпечення відповідальності користувача за свої дії і з підтримки спроможності КЗЗ виконувати свої функції (спостереженість забезпечується в системі автоматизації такими послугами: НР-2 – реєстрація (аудит), (захищений журнал), НИ-2 – одиночна ідентифікація і автентифікація, НК-1 – однонаправлений достовірний канал, НО-1 – розподіл обов'язків, а саме виділення адміністратора, НЦ-1 – КЗЗ з контролем цілісності, НТ-2 – самотестування при старті).

Інтерпретація послуг комплексу засобів захисту від НСД в системі автоматизації може бути така.

1. Система захисту інформації АРМ. Призначена для попередження НСД з робочих місць операторів системи. Використовується система перевірки повноважень користувача та системи захисту операційної системи, абонентської, тарифної та технологічної інформації. Як системи захисту інформації АРМ рекомендується використовувати програмні чи апаратно-програмні комплекси захисту, що пройшли сертифікацію уповноважених органів. Порівняльні дані щодо реалізації послуг захисту об’єктів у поширених операційних системах та засобах забезпечення технічного захисту інформації, а також вимоги до рівня гарантій наведені в табл. 1. Порівняльна таблиця дає можливість вибрати номенклатуру КЗЗ, що забезпечує захист у повному обсязі за рахунок ідентифікації і автентифікації, управління потоками інформації, реєстрації в журналі, розмежування доступу, маскування інформації, блокування каналів ПЕМВН, захисту від НСД жорстких магнітних дисків (ЖМД) тощо.

2. Додаткові засоби захисту, необхідність та склад яких визначається за результатами аналізу вразливості АТС. Сюди можуть входити різноманітні системи перевірки коректності даних.

3. Засоби дублювання, резервування, реагування, схемно реалізовані у системі. Призначені для забезпечення необхідної надійності системи, зниження ймовірності виникнення загрозливих ситуацій до припустимого рівня.

4. Контроль сигналізації відкриття обладнання системи та станції. Призначені для контролю фізичного доступу до вузлів системи, а також до інформаційних магістралей.

5. Для виключення втрати інформації, що зберігається на магнітних носіях, при короткочасному зникненні напруги у мережі електроживлення, як незалежне джерело має бути передбачена система безперебійного живлення (UPS). Необхідно також використовувати завадопоглинаючі пристрої, що забезпечують захист від навмисного несанкціонованого силового впливу (НСВ) на мережу живлення, яке призводить до виходу обладнання із ладу.

6. Усі зовнішні лінії мають бути захищені від витоку технічними каналами і від атаки технічними засобами НСВ. Має бути виключено доступ до інформаційних кабелів з метою провокування збоїв та пошкоджень системи автоматизації контактними та безконтактними технічними засобами НСВ та НСД.

7. Необхідно передбачити засоби контролю за роботою зовнішніх підсистем.

Для задоволення вимог до рівня гарантій мають враховуватись: порядок проектування засобів захисту інформації; комплект документації комплексної системи захисту інформації (КСЗІ) та інтерфейсів захисту; керівництво з КСЗІ для адміністратора захисту; правила безпеки, яких необхідно дотримуватись при розробці ПЗ; результати аналізу “слабких місць” у захисті; можливості внесення “закладок” тощо.

Порядок проектування засобів захисту інформації на кожному етапі життєвого циклу передбачає формування цілей та прийняття рішень щодо захисту системи. У тому числі, аналізуються суб’єкти доступу та їх потенційні можливості здійснення НСД, розробляються сценарії впливу на ПЗ, якщо у ньому існують закладки. На кожному етапі проводиться оцінка безпеки системи. Вона супроводжується гарантіями, що мають базуватись на формальних доказах достатності функцій безпеки. Проте на практиці поки що приймаються рішення, адекватність яких заявленим цілям формально не може бути доведена [5].

В склад документації входять: опис принципів побудови та функціонування КСЗІ, модель захисту, опис механізмів захисту, експлуатаційні документи.

Керівництво з КСЗІ для адміністратора захисту повинно мати опис функцій, що контролюються, інструкцію з експлуатації КСЗІ, опис старту, тестування, відновлення КСЗІ та роботу із засобами регістрації.

При розробці ПЗ необхідно дотримуватись таких правил безпеки:

- розробка процедури модифікації коду, що передбачає обов’язкове тестування кожної версії ПЗ;
- супроводження початкового коду на сервері та захищена пересилка тільки об’єктного коду;
- ідентифікація резервних копій тощо.

У ПЗ можуть бути внесені “закладки”, тому необхідна розробка стратегії захисту при активації таких закладок. При цьому такий захист не блокує саму загрозу, а лише дає рекомендації з усунення наслідків при реалізації програмної закладки.

Система захисту інформації має пройти сертифікаційні випробування та мати формальні гарантії забезпечення необхідного рівня захисту УК від НСД.

Таблиця 1 – Порівняльні характеристики засобів забезпечення ТЗІ

№ п\п	Послуги захисту	Windows 9X, 2000, DOS	Windows-NT	Linux, Unix	Windows 9X, 2000 з системою реєстрації “Інспектор”	Програмно-апаратний засіб “Захисник”	Засіб ТЗІ від НСД “Гриф”	ЕОМ-П	Мікро-ЕОМ PLUTON + “Гриф”	Комплекс “Плазма 3В”	ПК “EXPERT”
1	КА-1 – мінім. адмін. конфіденційність	-	-	-	-	-	+ (КА-2)	-	+ (КА-2)	-	-
2	КО-1 – повторне використання об’єктів	-	-	-	-	-	+ (КО-0)	-	+	-	-
3	ЦА-1 – мінім. адміністративна цілісність	-	-	-	-	-	+	-	-	-	-
4	ДВ-1 – ручне відновлення після збоїв;	+	+	+	+ (ДС-1)	-	+	-	+	-	-
5	НР-2 – аудит, захищений журнал	-	+	+	+ (НР-5)	-	+	-	+	-	-
6	НІ-2 – одиночна ідентифікація і автентифікація,	-	+	+	- (НІ-1)	-	+ (НИ-3)	-	+ (НИ-3)	-	-
7	НК-1 – однонапр. достовірний канал	-	-	-	+ (НК-2)	-	+	-	+	-	-
8	НО-1 – розподіл обов'язків	-	+	+	+ (НО-3)	-	+ (НО-2)	-	+ (НО-2)	-	-
9	НЦ-1 – КЗЗ з контр. цілісності.	-	-	-	+	-	+	-	+	-	-
10	НТ-2 – само-тестування	-	-	-	+ НТ-3	-	+	-	-	-	-
11	Вимоги до рівня гарантій		Не вище Г1	Не вище Г2	Г3	-	Г3	-	Г3	-	-
12	Захист від ПЕМВН	-	-	-	-	-	-	+	+	+	+
13	Захист від НСД ЖМД	-	-	-	-	+	-	-	+	-	-
14	Блокування акусто-електрич. каналів	-	-	-	-	-	-	-	-	+	+

Захист інформації вимагає витрат додаткових ресурсів. Із введенням системи захисту експлуатаційні витрати можуть вирости до 60%. Раціональною системою захисту можна вважати ту, для реалізації якої треба найменші витрати ресурсів. При цьому враховується вартість апаратних та апаратно-програмних засобів захисту. В цілому, в проблематиці проектування комплексної системи захисту інформації намітилась тенденція переходу до нових технологій проектування безпечних інформаційних технологій [6], що ставить нові задачі перед практиками.

IV Висновки

Створення ефективної КСЗІ є досить складною задачею. На діючих аналогових системах інформація захищалась, в основному, від витоку каналами ПЕМВН за рахунок акустоелектричних перетворень, паразитної високочастотної генерації та модуляції, впливу зовнішніх електромагнітних полів. Блокування технічних каналів витоку складає деяку долю серед заходів ТЗІ. Основні загрози НСД до інформації у автоматизованих системах виходять від програмного забезпечення та внутрішніх і зовнішніх користувачів.

При практичному проектуванні комплексної системи захисту інформації від НСД важко застосовувати формальні процедури доказу достатності функцій безпеки.

Розглянута процедура дозволяє реалізувати комплексний підхід до захисту інформації у системах автоматизації при модернізації діючого обладнання телекомунікаційних систем. На основі моделі порушників, аналізу загроз, аналізу вразливостей, оцінки ресурсів можна обґрунтувати множину задач захисту і перейти до розробки профілю захисту та проекту безпеки інформації. При цьому постає задача вибору і оцінки різних методів та засобів захисту, розробки суб'єктивних та об'єктивних показників складності захисту і ймовірності реалізації даного рівня захищеності, розробки методики аналізу ризиків. Вирішення цих питань можуть бути предметом наступної роботи.

Література: 1. Тардаскін М. Ф., Кононович В. Г. Аспекти політики безпеки системи управління телекомунікаційними мережами. "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", № 2, 2001. С. 234–239. 2. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. – ДСТСЗІ СБ України, К. 1999. С. 16. 3. НД ТЗІ 1.1-001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення. – ДСТСЗІ СБ України, К. 1999. С. 16. 4. Хетагуров Я. А., Древс Ю. Г. Проектирование информационно-вычислительных комплексов. – М.: Высш. шк., 1987. – 280 с. 5. Голубев А. Н. Информационная безопасность узлов коммутации российских сетей связи. – Вестник связи, № 7, 2001. С. 37–40. 6. Потий А. Технология проектирования систем обеспечения ИТ-безопасности. Служба безопасности, 2 (68), 2002. С. 24– 25.

УДК 621.395, 621.391.82

АНАЛІЗ ОСОБЛИВОСТЕЙ ПОБУДОВИ КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ ДЛЯ ШИРОКОСМУГОВИХ РАДІОСИСТЕМ

Олександр Корнейко, Олексій Кувшинов, Сергій Лівенцев

Військовий інститут телекомунікацій та інформатизації НТУУ "КПІ"

Анотація: **Проведено аналіз сучасного стану забезпечення безпеки інформаційних технологій. Запропоновано підхід до вирішення задачі побудови комплексних систем захисту інформації для широкосмугових радіосистем.**

Summary: **The analysis of a modern status of safety of information technologies is carried out. The approach to the decision of a task of construction of complex systems of protection of the information for broadband radiosystems is offered.**

Ключові слова: **Інформація, захист інформації, комплексна система захисту інформації, широкосмугова радіосистема.**

Аналіз розвитку інформаційних технологій в Україні і перспектив їх подальшого удосконалення дозволяє виявити стійку тенденцію розширення як функцій відповідних інформаційно-телекомунікаційних систем, так і сфер їх застосування. Це, у свою чергу, породило безліч загроз інформаційним процесам в інформаційно-телекомунікаційних системах і, як наслідок, необхідність розробки адекватних засобів і систем забезпечення інформаційної безпеки і методів оцінки їх захищеності [1, 2].