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].

Донедавна нормативною основою рішення задач захисту інформації були стандарти ISO 7498-2:1989 «Архітектура безпеки ВОС» і ISO/IEC 10181:1996 «Основні положення безпеки відкритих систем», що визначали теоретичні підходи до забезпечення захисту інформації [3–5].

У зв'язку з інтеграцією телекомунікаційних, мережних і комп'ютерних технологій, превалюванням у проектуванні телекомунікаційних і інформаційних систем ідеології єдиної інформаційної магістралі все більше практичне поширення одержує термін інформаційна технологія (ІТ) і його похідні: системи інформаційних технологій (ІТ-системи), продукти інформаційних технологій (ІТ-продукти), і, нарешті, безпека інформаційних технологій (ІТ-безпека). У міжнародному стандарті ІСО/МЕК 15408:2000 – "Критерії оцінки безпеки інформаційних технологій", більш відомому як "Загальні критерії" сформульовані нові підходи до забезпечення інформаційної безпеки. Під інформаційною технологією розуміють цілеспрямовану організовану сукупність інформаційних процесів, реалізованих з використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розподіл даних, доступ до джерел інформації незалежно від місця їх розташування.

Головна мета безпеки інформаційних технологій полягає в забезпеченні можливості будь-якої організації вирішувати (виконувати) свої функціональні задачі шляхом побудови ІТ-систем, де виключають або мінімізують ІТ-ризики організації, її партнерів і споживачів.

За типами основних класів загроз виділяють п'ять основних цільових задач безпеки.

1. Забезпечення доступності.
2. Забезпечення цілісності системи і даних.
3. Забезпечення конфіденційності даних і системної інформації.
4. Забезпечення спостереженості.
5. Забезпечення гарантій (гарантованість).

Система інформаційної безпеки телекомунікаційних мереж має бути реалізована як комплекс програмно-технічних засобів і організаційних (процедурних) рішень з захисту інформації від несанкціонованого доступу і складатися з функціональних підсистем:

керування доступом;
реєстрації й обліку;
криптозахисту;
забезпечення цілісності даних.

Комплексні системи захисту інформації (КСЗІ) призначені для захисту від несанкціонованого доступу і модифікації інформації, а також поновлення її після руйнування. КСЗІ характеризуються великою кількістю різнорідних параметрів, основне місце серед яких займають часові, що є наслідком об'єктивного процесу удосконалювання джерел загроз інформаційній безпеці в напрямку підвищення їх швидкодії. У цих умовах процеси захисту інформації є в максимальному ступені залежними саме від часових характеристик засобів протидії загрозам.

В даний час у структурі телекомунікаційних систем усе більший розвиток одержують широкосмугові радіосистеми. Вони застосовуються в структурах для забезпечення зв'язку рухомих абонентів як між собою, так і з стаціонарними системами та абонентами стаціонарної телефонної мережі (стандарт IEEE 802.11b).

Функціонування широкосмугових радіосистем (ШРС) спеціального призначення має забезпечувати повну інформаційну і технічну безпеку і конфіденційність інформаційних потоків.

Як правило, при розробці КСЗІ вважається, що середовище поширення є захищеним. Однак проведений аналіз загроз радіосистемам виявив певні особливості впливу загроз.

Типовим об'єктом нападу може служити інформаційний обмін між користувачами системи, між операторами мережі, між користувачем і постачальником обслуговування.

Загрозами для радіосистем є (рис. 1):

перехоплення;
маскування;
маніпуляції даними в радіоінтерфейсі;
радіоелектронне подавлення.

Визначено [6], що для ШРС із відкритим середовищем поширення найбільшою загрозою захищеності інформації є загроза радіоелектронного подавлення (РЕП). Ефект впливу на ШРС навмисних завад позначається в погіршенні якості оброблюваної інформації в результаті її руйнування або старіння, що збільшує ступінь невизначеності при прийнятті рішень. Таким чином, основною проблемою є забезпечення захисту повідомлень від несанкціонованої модифікації інформації, що міститься в них, при її передачі через незахищене середовище в умовах активної радіоелектронної протидії.

Комплексна система захисту інформації має в максимальному ступені враховувати розмаїтість можливих завад і, зокрема, швидкість зміни параметрів завади а також стратегію постановника завад. У будь-яких

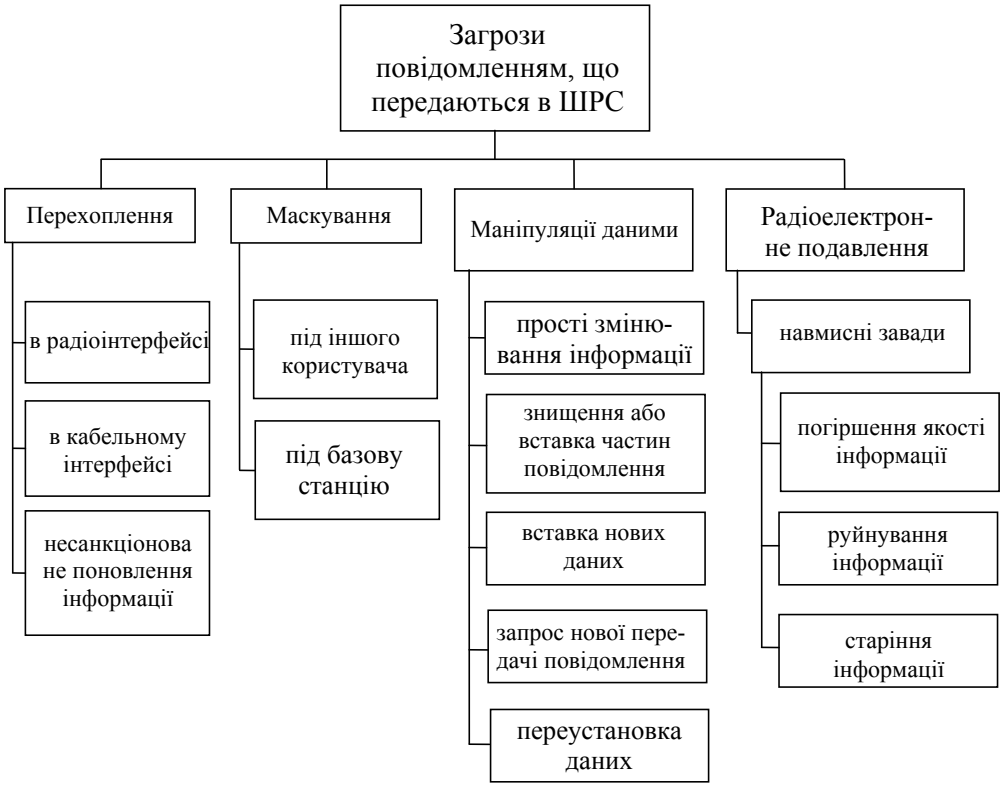

Рисунок 1 – Класифікація загроз повідомленням, що передаються в ШРС

стаціонарних каналах найбільшу захищеність забезпечують адаптивні системи зв'язку, що змінюють структуру сигналу і метод його обробки відповідно до стану каналу.

Найчастіше захист переданої інформації реалізується з використанням механізмів криптографічного захисту, таких як цифровий підпис і коди автентифікації повідомлень.

Однак використання криптографічних методів захисту інформації не завжди є ефективним, особливо для систем з відкритим середовищем поширення. Це пояснюється специфікою криптостійких кодів, що мають низку завадостійкість. Застосування некриптографічних методів не тільки підвищує захищеність інформації від несанкціонованої модифікації, але і підвищує стійкість до впливу завад природного і навмисного характеру, що дозволяє забезпечити захищеність інформації при прийманні. Тому для захисту інформації при передачі через відкрите середовище поширення крім криптографічних методів захисту необхідним застосування методів підвищення скритності і завадозахищеності (застосування шумоподібних сигналів (ШПС), сигналів з псевдовипадковим перестроюванням робочих частот (ППРЧ)).

Серед методів формування шумоподібних сигналів широке практичне застосування одержав метод ППРЧ, при якому розширення спектра в межах заданої полоси частот здійснюється за допомогою стрибкоподібної зміни частоти сигналу за псевдовипадковим законом, невідомим постановнику завад. В основі систем з ППРЧ лежить принцип перестроювання частот, на яких передають повідомлення, що дозволяє послабити або навіть цілком виключити вплив спектральної завади.

Стратегія постановки завад буде залежати від конкретних умов, можливостей постановника завад. Якщо постановник завад ставить загороджувальну заваду у визначеній ділянці полоси частот, виділеної для передачі повідомлень, то система ППРЧ перестроюється на роботу на вільній від впливів завади ділянці смуги частот.

При організації РЕП постановник завад має знати закон перестроювання частоти і, отже витрачати енергію і час на визначення цього закону.

З погляду витрат енергії важко визначити, якою має бути оптимальна стратегія постановника завад:

ставити заваду, що стежить за перестроюванням, або випадкову (загороджувальну);

формувати заваду як набір вузькосмугових сигналів або як обмежений по частоті шум;

модулювати вузькосмугову заваду для розширення її спектра або робити заваду синусоїдальною;

зосередити всю енергію завади на даному частотному інтервалі або роззосередити її на декількох вузькосмугових ділянках.

Структура сигналів у системі з ППРЧ організується різними методами.

1. Стрибок частоти відповідає символу зовнішнього коду в каскадній конструкції.
2. Стрибок частоти відповідає символу багаторазової модуляції.
3. Стрибок частоти відповідає кожному із символів кодової послідовності на вході багаторазового модулятора, що утворює символ модульованого сигналу.

За інших рівних умов чим частіше стрибки, тим ефективніше ППРЧ. Однак підвищенню швидкості перебудови заважає обмежена швидкодія синтезаторів частоти. У деяких випадках введення пристрою стрибкоподібної зміни частоти з відносно повільною швидкістю є більш простим, ніж реалізація складних адаптивних коректорів, що необхідні для вирівнювання великих затримок поширення. Зокрема, для некогерентної системи демодуляції створення адаптивних коректорів є досить складною задачею.

Система захисту інформації має в максимальному ступені враховувати розмаїтість можливих завад і, зокрема, швидкість зміни параметрів завади. Якщо швидкість зміни параметрів завади низька, можливе застосування повільного ППРЧ, при високій швидкості зміни параметрів завад – швидкого ППРЧ.

Архітектура ШРС є відкритою і має три рівні (рис. 2):

фізичний (L1),
канальний (L2),
мережний (L3).

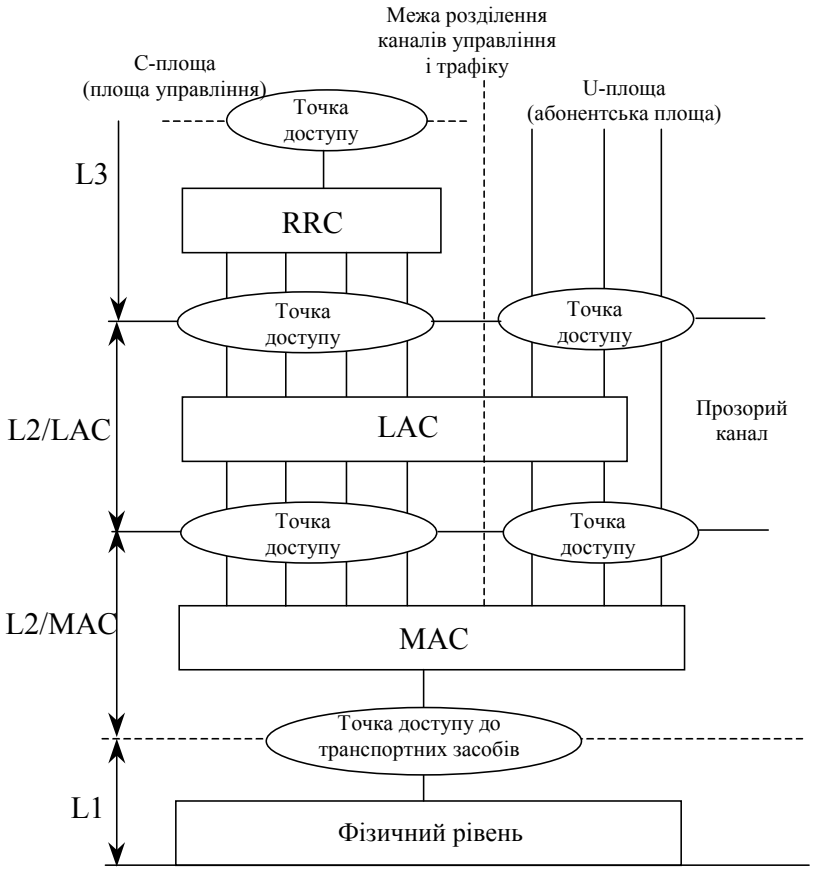

Рисунок 2 – Архітектура ШРС

Використання 3-рівневої моделі замість 7-рівневої дозволяє не тільки спростити опис взаємозв'язків між об'єктами різних рівнів, але і більш ефективно використовувати модульний принцип при проектуванні радіосистем.

Головна задача мережного рівня – формування потоків даних від кінцевого користувача, а також службових повідомлень і сигналізації.

Канальний рівень є транспортним середовищем між верхніми і фізичними рівнями. Це механізми керування мережними ресурсами і підтримки протоколів з урахуванням різних вимог до вірогідності, якості обслуговування і часу очікування.

У КСЗІ можуть бути реалізовані три режими передачі, засновані на застосуванні протоколу керування радіоканалом, що дозволяє абоненту взаємодіяти з мережею.

Прозорий – потік даних проходить без обробки і додавання службових символів. Якщо користувач забезпечує цілісність і вірогідність пакетів даних, то запропонована система може надавати «прозорий» канал зв'язку, не вносячи додаткових символів коректувального коду.

Достовірний – у ньому використовуються спеціальні протоколи з захистом від помилок в умовах РЕП. Якщо користувач не забезпечує вірогідність інформації власними засобами, то використовується система завадостійкого кодування і структурної адаптації.

Захищений – у випадку впливу загроз у радіоінтерфейсі (перехоплення даних, вставка, маскування) припускає використання достовірного режиму, доповненого криптографічними методами захисту.

На фізичному рівні реалізуються всі функції, пов'язані з безпосереднім доступом до радіоканалу, обробкою символів модулюючої і демодулюючої послідовностей, із синхронізацією, переключенням режимів прийом/передача.

У будь-якій реальній мережі взаємодія рівнів реалізується відповідно до визначеного набору конкретних протоколів роботи, причому в різних мережах набори функцій різних рівнів можуть відрізнятися або деякі рівні можуть бути відсутніми.

Може забезпечуватися два рівні безпеки переданої інформації:

стандартний, який використовує шифрування радіоінтерфейса;

високий, який використовує наскрізне шифрування (від джерела до одержувача).

Багаторівнева організація керування процесами в мережі породжує необхідність модифікувати на кожному рівні передані повідомлення стосовно до функцій, реалізованих на цьому рівні. Транспортний рівень забезпечує інтерфейс між мережею передачі даних і верхніми трьома рівнями еталонної моделі взаємодії відкритих мереж. Саме цей рівень надає користувачу факультативні можливості одержання сервісу визначеної якості від самої мережі (тобто мережного рівня).

Усі відомі системи передачі дискретних повідомлень можна поділити на системи без зворотного зв'язку і системи зі зворотним зв'язком.

У системах передачі без зворотного зв'язку повідомлення передаються в одному напрямку: від відправника до одержувача. При цьому можливо застосування як простих, так і коректувальних кодів. При простому (безнадлишковому) кодуванні вірність передачі визначається тільки якістю каналу зв'язку.

Усі системи передачі без зворотного зв'язку характеризуються тим, що відправник не одержує підтвердження про правильність прийому повідомлення одержувачем. В даний час набули широке поширення ШРС із змінною надмірністю. Особливістю систем зі змінною надмірністю є те, що надмірність, необхідна для виправлення помилок, вводиться автоматично в міру виникнення помилок. Реалізація систем зі змінною надмірністю можлива тільки при наявності зворотного зв'язку, тобто каналу, яким відправник одержує підтвердження про правильність прийнятого повідомлення одержувачем. У системах передачі зі зворотним зв'язком одержувач і відправник з'єднані каналами зв'язку в двох напрямках і на передавальній стороні використовується інформація про стан прямого каналу, що надходить із приймальної сторони каналом зворотного зв'язку [7].

Отже, захищена ШРС має складатися з прямого і зворотного каналів, призначених для передачі як основних повідомлень, так і вимірювальної інформації та команд (рис. 3). ШРС із структурою, що перебудовується, буде системою автоматичного регулювання. Така система повинна мати в своєму складі пристрій обробки вимірювальної інформації, який формує сигнали керування, що оптимізують структуру сигналу (коду), тобто бути адаптивною. Відомо, що в будь-яких стаціонарних каналах найбільшу завадозахищеність забезпечують адаптивні системи зв'язку, що змінюють структуру сигналу і метод його обробки відповідно до стану каналу.

При зниженні показників захищеності нижче припустимого рівня необхідно застосовувати структурну адаптацію, що дозволяє істотно підвищити захищеність переданої інформації. При цьому в умовах РЕП захищена ШРС повинна мати у своєму складі засоби визначення параметрів загроз переданої інформації (рис. 3).

Наявність зворотного зв'язку при передачі повідомлень дозволяє здійснити послідовну процедуру аналізу стану каналу, аналізу наявності загроз, що дає можливість одержати на передавальній стороні дані про стан захищеності інформації. Використовуючі ці дані можна побудувати різні адаптивні системи передачі інформації зі структурною адаптацією.

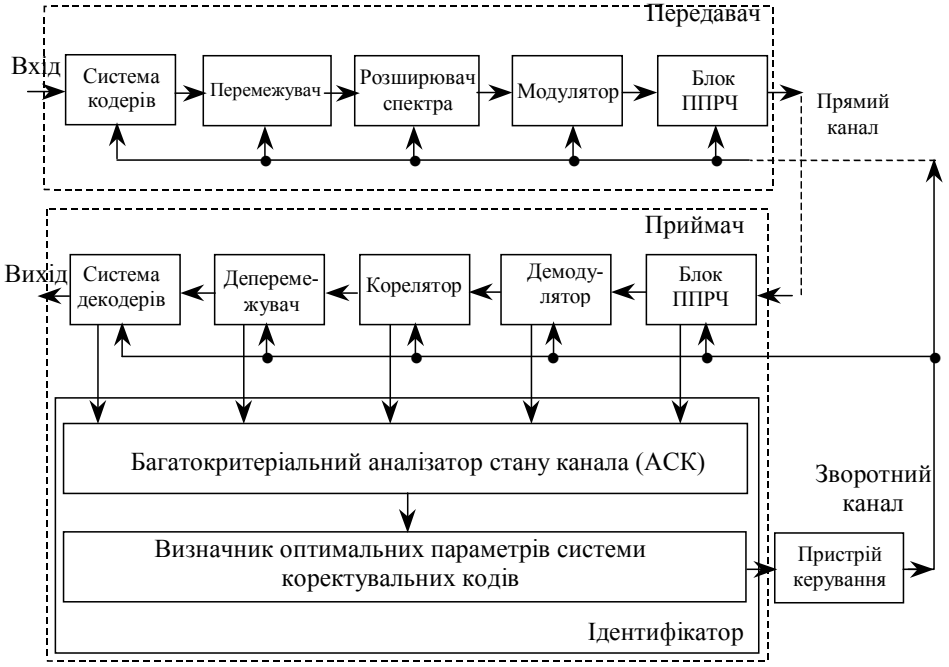

Рисунок 3 – Структурна схема ШРС зі структурною адаптацією

При адаптації за структурою сигналів важливу роль набувають адаптивні (змінювані) параметри: надмірність коду, глибина перемеження, кількість використовуваних частот, затримка, рівні і розташування порогів м'якого декодера, потужність ансамблю сигналів. У залежності від стану захищеності інформації в ШРС з ППРЧ може бути змінений метод кодування і декодування, вид сигналу (вид модуляції) або порядок чергування частот.

Найбільш перспективним є комбінований метод адаптації, при якому змінюється одночасно вид сигналу і спосіб кодування (оптимальна сигнально-кодова конструкція) [8, 9]. Це не тільки підвищує захищеність інформації від несанкціонованого доступу, але і робить її менш сприйнятливою до завад природного і навмисного характеру.

Висновки.

1. У ШРС має забезпечуватися комплексний захист інформації (інформаційна безпека).
2. Для ШРС із відкритим середовищем поширення найбільшою загрозою захищеності інформації є загроза радіоелектронного подавлення.
3. У ШРС для забезпечення інформаційної безпеки доцільно застосувати поряд із криптографічними методами і некриптографічні, що підвищує не тільки захищеність інформації від несанкціонованої модифікації, але і стійкість до впливу завад природного і навмисного характеру та дозволяє забезпечити захищеність інформації при прийомі.
4. З метою оптимізації пропускної здатності в ШРС необхідно передбачити кілька режимів забезпечення захищеності інформації (прозорий, достовірний, захищений).
5. Захищена радіосистема повинна мати в своєму складі засіб визначення параметрів загроз переданої інформації.
6. Найбільшу захищеність забезпечують адаптивні системи зв'язку. При цьому найбільш перспективним є комбінований метод адаптації оптимального виду, що використовує спільно вид сигналу і спосіб кодування (оптимальну сигнально-кодову конструкцію).

Література: 1. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. –НД ТЗІ 1.1-002-98, ДСТЗІ СБ України, Київ, 1998. 2. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. – НД ТЗІ 1.1-001-98, ДСТЗІ СБ України, Київ, 1998. 3. ISO/IEC 15408:2000 – Information technology – Security techniques – Evaluation criteria for IT security. – Part 1: Introduction and general model. 4. ISO/IEC 15408:2000 – Information technology – Security techniques – Evaluation criteria for IT security. – Part 2: Security functional requirements. 5. Перспективы применения международного стандарта ISO/IEC 15408 в Украине. Бондаренко М., Скрыпник Л., Горбенко И., Потий А. // Збірник „Правове, нормативне та метрологічне забезпечення систем

захисту інформації в Україні. НТУУ „КПІ”. – 2002. – №. 3. – С. 10-24. 6. Антонюк А. Жора В. Загрози інформації і канали витоку. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, науково-технічний збірник, вип. 2, НТУУ „КПІ”. К. 2001 р. 7. Метод захисту цілісності інформації, яка передається в системах абонентського радіодоступу спеціального призначення / Корнейко О. В., Кувшинов О. В., Лівенцев С. П. // Збірник „Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. НТУУ „КПІ”. – 2002. – №. 4. – С. 60-66. 8. Банкет В. Л., Дорофеев В. М. Цифровые методы в спутниковой связи. – М.: Радио и связь, 1988. – 240 с. 9. Зяблов В. В., Коробков Д. Л., Портной С. Л. Высокоскоростная передача сообщений в реальных каналах. – М.: Радио и связь, 1991. – 288 с.

УДК 621.96

ОСОБЕННОСТИ ХРАНЕНИЯ, ВОССТАНОВЛЕНИЯ И УНИЧТОЖЕНИЯ ИНФОРМАЦИИ НА ЖЕСТКИХ ДИСКАХ

Сергей Коженевский
ООО «ЭПОС»

Аннотация: **Обобщается опыт фирмы ЕПОС по ремонту жестких дисков и восстановлению информации, приводятся специфические каналы утечки информации, хранящейся на жестких дисках, описывается принцип построения стенда технического обслуживания жестких дисков с возможностью гарантированного уничтожения информации.**

Summary: **In this paper the experience of EPOS company in hard drives repair and data recovery is summarized. The specific channels of leakage of data stored on hard drives are considered. In this paper also are described the structure of hard drives maintenance test bench with provision of secure data erasure.**

Ключевые слова: **Информация, информационная безопасность, техническая защита информации.**

В информационных системах, базовым элементом которых является компьютер, основные объёмы информации хранятся на жёстких магнитных дисках.

Именно в накопителе на жестких магнитных дисках (НЖМД) хранится и с него загружается в оперативную память компьютера его операционная система, информация, обрабатываемая в процессе использования, а также использованная и удаляемая информация.

Широкому применению НЖМД способствует ряд их положительных эксплуатационных качеств: надежность, быстрота доступа и дешевизна (в расчёте на единицу хранения информации). Кроме того, один из самых важных показателей – энергонезависимость – делает НЖМД практически незаменимым для оперативного и долговременного хранения больших массивов информации.

В то же время размещение и хранение информации в устройствах долговременной энергонезависимой памяти создаёт предпосылки как для утраты важной информации, так и для несанкционированного доступа к ней.

В последнее время значительно увеличился объем информации, хранимой на жестких дисках. В основном увеличение объема достигнуто за счет увеличения плотности записи. Увеличение плотности записи привело к необходимости применения специальных мер, направленных на увеличение надежности жестких дисков. Несмотря на принимаемые производителями жестких дисков меры по обеспечению надежности, жесткий диск остается самым ненадежным элементом компьютера. Ежегодно в сервисный центр «ЕПОС» поступает для ремонта более полутора – двух тысяч жестких дисков. Примерно треть из них имели неисправности, обусловленные естественными причинами. Но две трети всех поломок обусловлены небрежным обращением с дисками. Поломка винчестера может привести к утрате важной информации. Для уменьшения риска утраты информации в серверах необходимо применять отказоустойчивые дисковые системы – RAID. Однако, применение таких систем может быть неприемлемо, например, по экономическим соображениям. Более того, утрата информации возможна и на исправном жестком диске, например, вследствие случайного ее уничтожения или вследствие вирусной атаки. К счастью в большинстве случаев информация теряется не безвозвратно. Ее можно восстановить.

В простейших случаях случайно уничтоженную информацию можно восстановить с помощью стандартных, широко распространенных утилит. Разработанные фирмой ЕПОС технологическая оснастка и специальные утилиты восстановления позволяют восстановить информацию в большинстве случаев и при поломке диска (в том числе, например, даже при обрыве головок).