УДК 621.39

СЕРЕДОВИЩЕ ПОТЕНЦІЙНИХ ПОРУШНИКІВ У СИСТЕМІ ТЕХНОЛОГІЧНОГО УПРАВЛІННЯ ТЕЛЕКОМУНІКАЦІЙНИМИ МЕРЕЖАМИ

Володимир Кононович, Андрій Севостьяненко
Українська Державна Академія Зв'язку, м. Одеса

Анотація: **доповідь стосується специфіки проблеми забезпечення технічного захисту інформації в системах технологічного управління електрозвєязком. Проводиться аналіз середовища потенційних порушників безпеки інформації в системах технологічного управління електрозв'язком. Доводиться необхідність розробки спеціального комплексу заходів, що найбільш повно враховував би особливості систем технологічного управління електрозвєязком.**

Abstract: **the report deals with problem peculiarities of information technical security providing in Telecommunications Technological Management Systems (TTMS). The TTMS information security potential intruders environment is analyzed. The importance of special arrangements plan, that fully takes into account the peculiarities of TTMS is proved.**

Ключові слова: **системи технічного управління, технічний захист інформації, несанкціонований доступ.**

Питання інформаційної безпеки набуло актуальності досить давно, але з розвитком телекомунікаційних технологій її значення неухильно зростає. Згідно проведених досліджень, міжнародних нормативних документів, що стосуються виключно систем технологічного управління електрозв'язком (далі СТУ) поки що не існує. Метою даної роботи є розгляд специфіки забезпечення технічного захисту інформації в системах технологічного управління електрозвєязком та аналіз середовища потенційних порушників безпеки інформації в системах технологічного управління електрозв'язком. Широко використовані нормативні документи, що визначають критерії безпеки для інформаційних систем, комп'ютерних мереж, автоматизованих систем тощо не можуть бути автоматично використані для систем технологічного управління. В Україні в даний час Державною Академією зв'язку поряд з іншими нормативними документами розроблюється галузевий Керівний Нормативний Документ (КНД), що має визначати моделі загроз та порушників в СТУ, на основі яких пізніше можуть бути визначені заходи, що спрямовані на забезпечення технічного захисту інформації (ТЗІ) в СТУ. В даній статті автори спробували проаналізувати особливості СТУ, як об'єкту ТЗІ.

Як відомо, інформація, що циркулює в інформаційних системах, може бути умовно поділена три рівні важливості, що співвідносяться на принципах ієрархії [4]. До першого, найнижчого рівня, можна віднести відкриту інформацію. Користувач сам має визначати ступінь важливості цієї інформації, рівень секретності даних та заходи, спрямовані на забезпечення захисту цієї інформації. До другого рівня може бути віднесена інформація комерційного характеру, тобто міжбанківська, внутрішньобанківська тощо. Звичайно таку інформацію не можна передавати, зберігати та обробляти у відкритому вигляді. Зловмисне використання, спотворення чи знищення її може завдати значних збитків. Рівень захисту такої інформації має бути вищим, ніж такий, що використовується для певної частини відкритої інформації. До третього, найвищого рівня, можна віднести конфіденційну інформацію, що належить не державним юридичним особам. Передавання конфіденційної інформації, що належить державі, по мережі загального користування без спеціальних засобів захисту не проводиться. Саме до такого типу можна віднести основну частину інформації, що циркулює в системі технологічного управління. Справді, інформація управління та сигналізації має виключно важливе значення для СТУ. Будь-яке, навіть незначне, видалення, спотворення чи модифікація такої інформації може призвести до некерованості СТУ та фатальних наслідків як для неї самої , так і для всіх систем, що взаємодіють з нею.

При створенні керівного нормативного документу, що визначає моделі загроз безпеці інформаційним ресурсам в системах технологічного управління (СТУ) можуть бути застосовані в обмеженому вигляді НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу" та НД ТЗІ2.5-005-99. "Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу". Обмеження на використання таких НД пов'язані в першу чергу з рівнем пріоритетності та важливості інформації, що циркулює в СТУ. Весь обсяг інформації, що пов'язаний з управлінням, має бути захищеним від ймовірних та суттєвих загроз безпеці інформації СТУ, що

можуть здійснюватись:

- технічними каналами, що включають канали побічних електромагнітних випромінювань і наводок, акустичними, оптичними, радіотехнічними, хімічними та іншими каналами;
- каналами спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації;
- несанкціонованим доступом шляхом підключення до апаратури та ліній зв'язку (слабкострумових технічних засобів) , подолання заходів захисту для використання інформації або нав'язування хибної інформації.

Оскільки інформація в СТУ має найбільший можливий пріоритет, то заходи, спрямовані на захист інформації в автоматизованих, комп'ютерних ситемах тощо є недостатніми для ефективного та надійного функціювання СТУ. Ці заходи можуть бути прийняті яка базові, але їх обов'язково треба доповнити додатковими, більш суворими технічними та організаційними мірорпиємствами.

В керівному нормативному документі "Технічний захист інформації в галузі зв′язку України. Моделі загроз безпеці інформаційним ресурсам в системах технологічного управління" буде проведена розробка вимог до взаємопов'язаного набору функціональних послуг захисту з необхідними рівнями ефективності і стійкості реалізацій цих послуг, при котрих забезпечується заданий рівень захищеності інформаційних ресурсів СТУ на основі виконання таких видів робіт:

- побудова моделі загроз для інформації системи технологічного управління, включаючи аналіз ризиків, що пов'язані з можливими реалізаціями загроз;
- визначення необхідного рівня довіри до коректності реалізації системі технологічного управління;
- визначення необхідного рівня захищеності інформаційних ресурсів системи технологічного управління.

Основні особливості функціонування СТУ:

- територіальна разнесеність компонентів системи і наявність інтенсивного обміну інформацією між ними;
- широкий спектр використовуваних засобів представлення, збереження і передачі інформації;
- інтеграція даних різноманітного призначення, що належать різним суб'єктам, у рамках єдиних баз даних і, навпаки, розміщення даних, необхідних деяким суб'єктам, у різноманітних віддалених вузлах мережі;
- абстрагування власників даних від фізичних структур і місця розміщення даних.

Спеціальні режими роботи:

- розподілене опрацювання даних;
- автоматизоване опрацювання інформації великої кількості користувачів і персоналу, що належать до різноманітних категорій.

Основні характеристики роботи СТУ:

- безпосередній і одночасний доступ до ресурсів (у тому числі й інформаційних) великого числа користувачів (суб'єктів) різноманітних категорій;
- високий ступінь неоднорідності використаних засобів зв'язку і обчислювальної техніки, а також їхнього програмного забезпечення;
- відсутність спеціальної апаратної підтримки засобів захисту в більшості типів технічних засобів, широко використовуваних у СТУ;
- наявність безпосередніх випадкових впливів персоналу і навмисних впливів зловмисників на виділені сервери і маршрутизатори можна вважати малоймовірними;
- ймовірність масованої атаки на сервери і маршрутизатори з використанням засобів віддаленого доступу, пошук порушниками можливості вплинути на роботу різноманітних підсистем серверів і маршрутизаторів, використовуючи хиби протоколів обміну і засобів розмежування віддаленого доступу до ресурсів і системних таблиць;
- використання усіх можливостей і засобів, від стандартних (без модифікації компонентів) до підключення спеціальних апаратних засобів (канали, як правило, слабко захищені від підключення), застосування досконалих програм для подолання системи захисту, встановлення апаратних і програмних закладок у самі маршрутизатори і сервери, внаслідок чого з'являються додаткові широкі можливості несанкціонованого віддаленого доступу. Закладки можуть бути встановлені як із віддалених станцій (за допомогою вірусів або іншого засобу), так і безпосередньо в апаратуру і програми серверів при їхньому ремонті, обслуговуванні, модернізації, переході на нові версії программного забезпечення, зміні устаткування;
- велика просторова протяжність ліній зв'язку через неконтрольовану або слабко контрольовану територію, що обумовлює можливість підключення до них, втручання в процес обробки та передачі даних.

Розглянемо середовище потенційних порушників в СТУ. Нагадаємо, що порушник - особа, що намагається виконати заборонені операції (дії) помилково, по незнанню, або свідомо з лихими намірами (з корисливих інтересів) або без таких (заради гри або задоволення, із метою самоствердження і т.п.) та використовує для цього різні методи, можливості та засоби. Зловмисником будемо називати порушника, що навмисно виконує порушення з корисливих спонукань. Практичні та теоретичні можливості, апріорні знання, час і місце дії і т.п. можуть бути відображені за допомогою неформальної моделі порушника СТУ.

У кожному конкретному випадку, виходячи з певної технології обробки інформації, може бути визначена модель порушника, що має бути адекватною реальному порушнику для даної СТУ.

При розробці моделі порушника визначаються:

- припущення про категорії осіб, до яких може належати порушник; припущення про мотиви дій порушника (мету порушника);
- припущення про кваліфікацію порушника і його технічне оснащення (про методи та засоби, що використані для вчинення порушення);
- обмеження і припущення про характер можливих дій порушників.

Стосовно досліджуваної СТУ порушники можуть бути внутрішніми (із числа персоналу системи) або зовнішніми (сторонніми особами).

Внутрішнім порушником може бути особа, що належить до таких категорій персоналу:

- користувачі (оператори) системи;
- персонал, що обслуговує технічні засоби (інженери, техніки);
- співробітники відділів розробки і супроводу програмного забезпечення (ПЗ) (прикладні і системні програмісти);
- технічний персонал, що обслуговує приміщення (прибиральники, електрики, сантехники й інші співробітники, що мають доступ до приміщень і помешкань, де розміщені компоненти системи технологічного управління);
- співробітники служби безпеки системи технологічного управління;
- керівники різних рівнів посадової ієрархії.

Сторонні особи, що можуть бути порушниками:

- клієнти (представники організацій, громадяни);
- відвідувачі (запрошені з будь-якого приводу);
- представники організацій, що взаємодіють із питань забезпечення життєдіяльності організації (енерго-, водо-, теплопостачання і т.п.);
- представники конкуруючих організацій (іноземних спецслужб) або особи, що діють за їхнім завданням;
- особи, що випадково або навмисно порушили пропускний режим (не маючи мету порушити безпеку сту);
- будь-які особи за межами контрольованої території.

Всіх порушників можна класифікувати за такими характеристиками (рисунок 1).

За рівнем знань про СТУ :

- порушник знає функціональні особливості СТУ, основні закономірності формування в ній масивів даних і потоків запитів до них,
- уміє користуватися штатними засобами;
- порушник має високий рівень знань і досвід роботи з технічними засобами системи і їхнього обслуговування;
- порушник має високий рівень знань в області програмування й обчислювальної техніки, проектування й експлуатації СТУ;
- порушник знає структуру, функції і механізм дії засобів захисту СТУ, їх сильні і слабкі сторони.

За рівнем можливостей (використовуваним методам і засобам):

- порушник, що використовує чисто агентурні методи одержання даних;
- що використовує пасивні засоби (технічні засоби перехоплення без модифікації компонентів системи);
- порушник, що використовує тільки штатні засоби та недоліки систем захисту для їх подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні магнітні носії інформації, що можуть бути приховано винесені через пости охорони;
- порушник, що використовує методи і засоби активного впливу (модифікація і підключення додаткових технічних засобів, підключення до каналів передачі даних,
- введення програмних закладок і використання спеціальних інструментальних і технологічних програм).

За часом дії:

- у процесі функціонування СТУ (під час роботи компонентів системи);

- у період неактивності компонентів СТУ (у неробочий час, під час планових перерв у її роботі, перерв для обслуговування і ремонту і т.п.);
- як у процесі функціонування СТУ, так і в період неактивності компонентів системи.

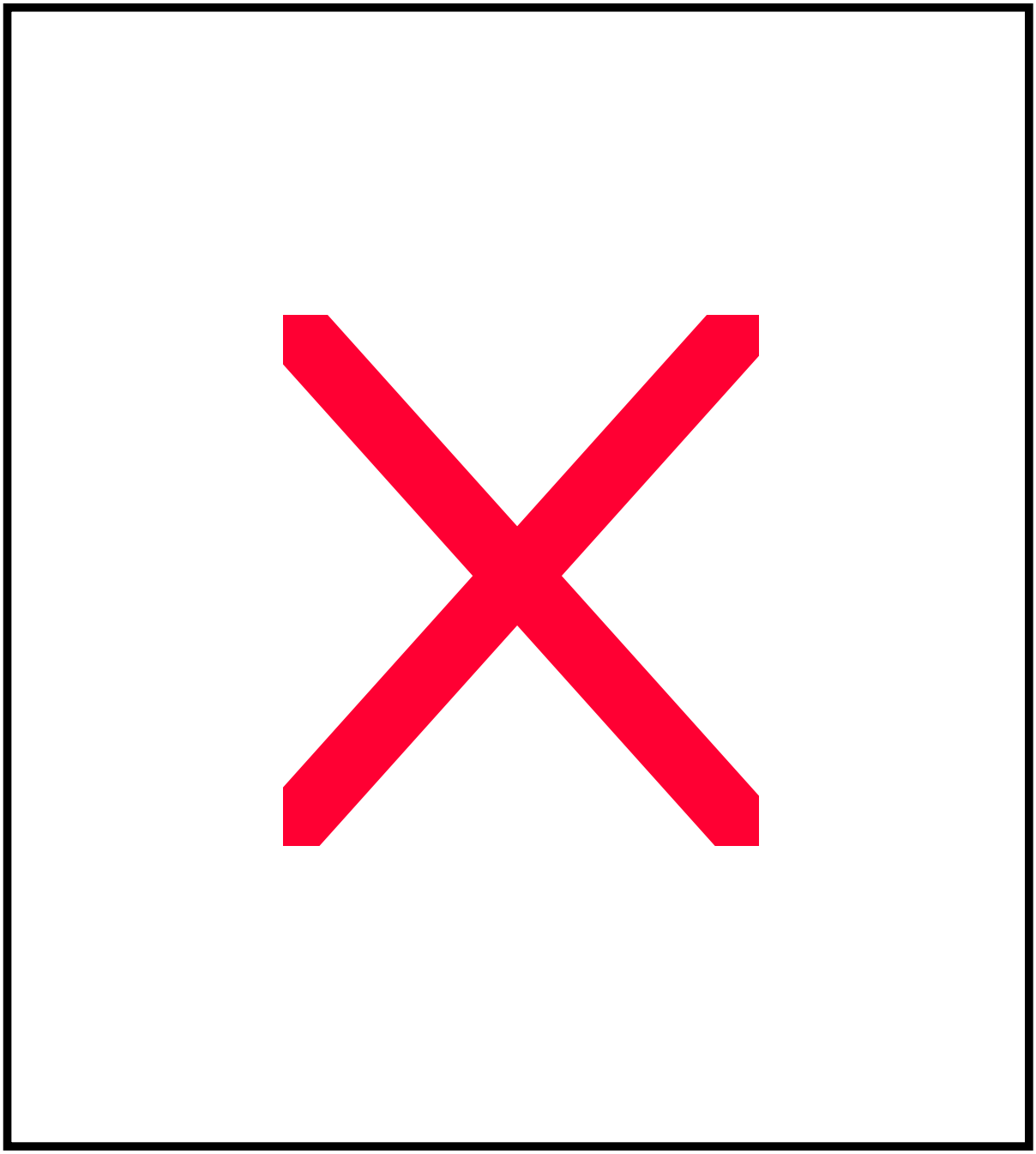
За місцем дії:
- без доступу на контрольовану територію організації;
- з контрольованої території без доступу до приміщень та споруд;
- всередині помешкань, але без доступу до СТУ;
- з робочих місць прикінцевих користувачів (операторів) СТУ;
- з доступом у зону даних (баз даних, архівів і т.п.):
- з доступом до зони керування засобами забезпечення безпеки СТУ.

Можуть враховуватися такі обмеження і припущення про характер дій можливих порушників:
- робота з добору кадрів і спеціальні заходи можуть ускладнити можливість створення коаліцій порушників, тобто об'єднання (змови) і цілеспрямованих дій для подолання підсистеми захисту двома і більше порушниками;
- порушник, що планує спроби несанкціонованого доступу (НСД), приховує свої несанкціоновані дії від інших співробітників;
- НСД може бути наслідком помилок користувачів, адміністраторів, персоналу що експлуатує й обслуговує, а також хиб використовуваної технології обробки інформації і т.д.

Для більш точного опису віддалених атак в СТУ пропонується така класифікація згідно ознак:
За характером впливу – пасивний і активний., та їх комбінація
Пасивний вплив не порушує безпосередньо роботу системи, але може порушувати її політику безпеки. Саме відсутність безпосереднього впливу на функціонування СТУ призводить до того, що пасивний віддалений вплив практично неможливо виявити. Прикладом типового пасивного віддаленого впливу є прослуховування каналу зв'язку в мережі.
Під *активним впливом* на розподілену обчислювальну мережу будемо розуміти безпосередній вплив на роботу системи (зміна конфігурації мережі, порушення працездатності і т.д.) і що порушують політику безпеки. Практично всі типи віддалених атак є активними впливами. Це пов'язано з тим, що в самій природі руйнуючого впливу є активна складова. Очевидною особливістю активного впливу в порівнянні з пасивним є принципова можливість його виявлення (природно, із більшим або меншим ступенем складності), тому що в результаті його здійснення в системі відбуваються визначені зміни. На відміну від активного, при пасивному впливі не залишається ніяких слідів (від того, що атакуюча особа перегляне чуже повідомлення в системі, у той же момент нічого не зміниться).
За метою впливу:
- порушення конфіденційності інформації або ресурсів системи;
- порушення цілісності інформації СТУ
- порушення працездатності (доступності) СТУ.

Ця класифікаційна ознака є прямою проекцією трьох основних типів погроз - розкриття, цілісності і відмови в обслуговуванні.
Основна мета практично будь-якої атаки на СТУ- одержати несанкціонований доступ до інформації СТУ. Існують дві принципові можливості доступу до інформації: перехоплення і спотворення. Можливість перехоплення інформації означає одержання до неї доступу, але неможливість її модифікації. Отже, перехоплення інформації веде до порушення її конфіденціальності. Прикладом перехоплення інформації є прослуховування каналу мережі. У цьому випадку є несанкціонований доступ до інформації без можливості її спотворення. Очевидно також, що порушення конфіденціальності інформації є пасивним впливом.
Можливість спотворення інформації означає або повний контроль над інформаційним потоком між об'єктами системи, або можливість передачі повідомлень від імені іншого об'єкта. Таким чином, очевидно, що перекручування інформації веде до порушення її цілісності. Даний інформаційний руйнуючий вплив являє собою яскравий приклад активного впливу. Прикладом віддаленої атаки, мета якої порушення цілісності інформації, може служити типова віддалена атака. Принципово іншою метою атаки є порушення працездатності СТУ. У цьому випадку не передбачається одержання атакуючою особою несанкціонованого доступу до інформації. Основна мета порушника - домогтися, щоб операційна система атакованого об'єкту вийшла з ладу і для всіх інших об'єктів системи доступ до ресурсів атакованого об'єкта був би неможливий. Прикладом віддаленої атаки, метою якої є порушення працездатності системи, є типова віддалена атака "Відмова в обслуговуванні". Віддалений вплив, як і будь-яке інше, може почати здійснюватися тільки за певних умов.

У просторово розподілених СТУ існують три види умов початку здійснення віддаленої атаки:
Атака за запитом від атакованого об'єкта



У цьому випадку порушник очікує передачу запиту визначеного типу для початку атаки, що і буде умовою початку здійснення впливу. Важливо відзначити, що даний тип віддалених атак найбільш характерний для розподілених СТУ.

Атака після настання очікуваної події на атакованому об'єкті

У цьому випадку порушник здійснює постійне спостереження за станом операційної системи віддаленого об’єкту атаки і починає вплив при виникненні попередньо визначеної події в СТУ. Як і в попередньому випадку, ініціатором здійснення початку атаки виступає самий атакований объект

Безумовна атака

У цьому випадку початок здійснення атаки є безумовним стосовно об’єкту атаки, тобто атака здійснюється негайно і незважаючи на стан системи і атакованого об'єкта. Отже, у цьому випадку порушник є ініціатором початку здійснення атаки.

По наявності зворотнього зв'язку з щойно атакованим об'єктом

Розрізняють:

- атаку зі зворотним зв'язком;
- атаку без зворотнього зв'язку (однонаправлена атака).

Віддалена атака, що здійснюється при наявності зворотного зв'язку з атакованим об'єктом, що входить до складу СТУ, характеризується тим, що на деякі запити, передані на атакований об'єкт, нападнику потрібно одержати відповідь, отже, між нападником і метою атаки існує зворотній зв'язок, що дозволяє нападнику адекватно

реагувати на всі зміни, що відбуваються на атакованому об'єкті. Подібні віддалені атаки найбільше характерні для розподілених обчислювальних мереж.
На відміну від атак із зворотнім зв'язком, віддаленим атакам без зворотнього зв'язку не потрібно реагувати на будь- які зміни, що відбуваються на атакованому об'єкті. Атаки даного виду звичайно здійснюються шляхом передачі на атакований об'єкт одиночних запитів, відповіді на які нападнику не потрібні. Подібну віддалену атаку можна називати однонаправленою віддаленої атакою. Прикладом однонаправленої атаки є типова віддалена атака "Відмова в обслуговуванні".

По розташуванню суб'єкта атаки щодо атакованого об'єкта:
- внутрішньосегментне;
- міжсегментне.
Суб'єкт атаки (або джерело атаки) - програма-нападник, або оператор, що безпосередньо здійснює вплив, комп'ютер мережі (робоча станція) тощо.
Сегмент мережі - фізичне об'єднання комп'ютерів мережі. Наприклад, сегмент мережі утворять сукупність комп'ютерів мережі, під'єднаних до сервера за схемою "загальна шина" . При такій схемі підключення кожний комп'ютер мережі має можливість піддавати аналізу будь-який пакет у своєму сегменті.

Отже, при організації технічного захисту інформації, що циркулює в системі технологічного управління, не можна копіювати заходи забезпечення безпеки, що були розроблені для менш пріоритетних автоматизованих та комп'ютерних систем; навпаки, має бути визначений індивідуальний комплекс заходів, що найбільш повно враховував би особливості СТУ. Саме така робота проводиться при розробці керівних нормативних документів, що стосуються СТУ.

Література: 1. Trusted Computer System Evaluation Criteria (TCSEC), US DoD 5200.28-STD, 1993.. 2. Information Technology Security Evaluation Criteria (ITSEC). Harmonised Criteria of France - Germany - the Netherlands - the United Kingdom.- Department of Trade and Industry, London, 1991. 3. Canadian Trusted Computer Product Evaluation Criteria (CTCPEC), Version 3.0, Canadian System Security Centre, Communications Security Establishment, Government of Canada, 1993.. 4. В. Г. Кононович, А. О. Севостьяненко. Основи організації служби ТЗІ в галузі телекомунікацій. Тези доповіді на конференції "Современные и будущие информационные технологии Украины", К.: УДЭНТЗ, 2000, с. 3.. 5. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. 6. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. 7. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем та стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

УДК 621.391.052

ВОСП И ЗАЩИТА ИНФОРМАЦИИ

Сергей Авдеев, Андрей Свинцов, Анатолий Свинцов
г. Королев, РКК «Энергия», г. Москва, МГТУ им. Баумана, г. Москва, ТОО «Прогноз+»

Анотация: ***Рассматриваются особенности и основные пути обеспечения защиты информации от НСИ в ВОСП***
Ключевые слова: ***ВОСП, системы диагностики состояния, ЧМЗ, рефлектометрия***

Волоконно-оптические системы передачи (ВОСП) благодаря уникальной пропускной способности, малому затуханию волоконных световодов (ВС) и успехам в технологии элементов ВОСП являются наиболее перспективными информационными системами. В области стационарных систем передачи информации с большой информационной емкостью и высокой надежностью ВОСП не имеют конкурентов. Радио системы, в том числе для подвижной связи, и спутниковые системы связи имеют свои преимущества, но по комплексу параметров (скорость передачи, помехоустойчивость, защищенность информации) ВОСП являются наилучшими информационными системами.