склалася, як телекомунікаційних систем, комп'ютерних мереж, мережних інформаційних ресурсів, так і аудиторії користувачів, якій ця інформація адресована, ускладнює об'єктивний аналіз і моніторинг телекомунікаційних архітектур і ресурсів. Тому безумовно актуально, що при експлуатації телекомунікаційних систем і комп'ютерних мереж повинен бути використаний досить широкий спектр сучасних і науково обгрунтованих технічних і технологічних розв'язань їх аналізу та моніторингу. Розв'язання задач моніторингу розподілених телекомунікаційних систем є важливим з точки зору забезпечення необхідної при обробці потоків завдань продуктивності і пропускної здатності. Впровадження систем моніторингу дозволяє вирішити безліч завдань, в числі яких: скорочення термінів і витрат на виконання поточних завдань, включаючи активацію послуг; підвищення віддачі від існуючих ресурсів мережі і поліпшення якості планування їх майбутнього розвитку; зниження потреби в персоналі і, як наслідок, скорочення поточних витрат; повніша реалізація потенціалу сучасного мережного обладнання за рахунок розробки та реалізації нових послуг; зведення до мінімуму ризиків втрат доходів; скорочення термінів реагування, що відбуваються в мережі події; залучення високоприбуткових клієнтів за рахунок надання додаткових послуг на основі гарантованої якості; скорочення термінів введення в експлуатацію нових послуг; підвищення якості та оперативності обслуговування користувачів мережі за рахунок чіткої координації та інформаційної підтримки робіт; забезпечення координації взаємодії численного персоналу віддалених підрозділів у режимі реального часу.

УДК 656.254.5

В.І. Мойсеєнко, Г.Є. Григор'янц

СИСТЕМА ДИСПЕТЧЕРСЬКОЇ ІНДИВІДУАЛЬНОЇ ІНФОРМАТИЗАЦІЇ

V.I. Moyseenko, G.E. Grygoryants

THE SYSTEM OF INDIVIDUAL INFORMATIZATION OF TRAFFIC CONTROL OFFICER

Системи управління і контролю на залізничному транспорті за своєю сутністю були, є і в майбутньому будуть людино-машини. У зв'язку з специфікою роботи людина глибоко інтегрована у систему управління, виконуючи відповідальні функції.

Впровадження мікропроцесорних систем управління дозволило істотно розширити коло виконуваних системою управління функцій, проте процес взаємодії з людиною-оператором найчастіше будувався за старими процедурами.

Для вирішення завдань оперативності в організації безпеки праці на залізничному транспорті та підвищення контролю за дотриманням вимог охорони праці розробляється система диспетчерської індивідуальної інформатизації (СДІІ) на базі сучасних інформаційних і телекомунікаційних мобільних технологій. Основні можливості системи та сфери дії і операції:

- автоматичне попередження персоналу про небезпеку, що виникає для їхнього життя і здоров'я;
- ідентифікація персоналу при виконанні відповідальних, критичних щодо безпеки функцій, наприклад окремі операції чергового по станції (увімкнення запрошувального вогню на світлофорі,

аварійне переведення стрілки і т. п.), поїзної бригади та ін.

• ідентифікація місцезнаходження персоналу при виконанні регламентних робіт, пов'язаних з технічним обслуговуванням;

• забезпечення ефективного контролю фактичного виконання персоналом робіт.

Вирішення цих проблем вимагає проведення таких наукових досліджень:

• ідентифікація розташування суб'єкта. Необхідно розробити модель зони можливого знаходження суб'єкта, визначити розміри зони в різних умовах;

• розробка моделі зон взаємодії для різних систем і різних видів діяльності;

• розробка нечітких моделей з нечіткими функціями належності людини до контрольованої зони.

Необхідно розробити модель взаємодії людини-оператора з робочою небезпечною зоною та модель взаємодії з неробочої небезпечною зоною в різних умовах, в режимі реального часу. На базі цієї моделі буде побудована система диспетчерської індивідуальної інформатизації, яка зможе ідентифікувати людину-оператора в тій чи іншій зоні. Це дозволить значно покращити оперативність роботи диспетчерів, розширити можливості контролю перевезень, підвищити безпеку руху поїздів, удосконалити контроль виконання робіт.

УДК 004.56.5 (043.2)

О.І. Демічев

АНАЛІЗ КРИПТОГРАФІЧНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В СПЕЦІАЛЬНИХ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

O.I. Demichev

ANALYSIS CRYPTOGRAPHIC SOFTWARE IN A SPECIAL INFORMATION AND TELECOMMUNICATION SYSTEMS

В даний час для захисту інформації потрібна не просто розробка приватних механізмів захисту, а реалізація системного підходу, що включає комплекс взаємопов'язаних заходів (використання спеціальних технічних і програмних засобів, організаційних заходів, нормативно-правових актів та іншого).

PGP (Pretty Good Privacy) — комп'ютерна програма, також бібліотека функцій, що дозволяє виконувати операції шифрування і цифрового підпису повідомлень, файлів і іншої інформації, поданої в електронному вигляді, у тому числі прозоре шифрування даних на пристроях, що запам'ятовують, наприклад, на жорсткому диску.

На теперішній час в програмному пакеті PGP використовуються вісім алгоритмів шифрування, з яких два асиметричні (RSA і Elgamal) та шість симетричних (AES, 3DES, Blowfish, IDEA, Twofish, Camellia).

TrueCrypt - комп'ютерна програма для шифрування "на льоту" для 32- і 64-розрядних операційних систем сімейств Microsoft Windows NT 5 і новіше (GUI -интерфейс), Linux і Mac OS X. За допомогою TrueCrypt можна повністю шифрувати розділ жорсткого диска або іншого носія інформації, такий як флоппі-диск або USB флеш-пам'ять. Усі збережені дані в томі TrueCrypt повністю шифруються, включаючи імена файлів і каталогів. Змонтований том TrueCrypt подібний до звичайного логічного диска. У список підтримуваних TrueCrypt 6.2 алгоритмів шифрування входять AES, Serpent і Twofish. Попередні версії програми також підтримували алгоритми з