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

розміром блоку 64 біти (включаючи версії 5.x, яка могла відкривати, але не створювати розділи, захищені цими алгоритмами). Крім того, можливе використання каскадного шифрування різними шифрами, приміром: AES+Twofish+Serpent.

BitLocker Drive Encryption – пропріетарна технологія, що є частиною операційних систем Microsoft Windows. BitLocker дозволяє захищати дані шляхом повного шифрування диска (у термінології Microsoft - томи). Підтримуються такі алгоритми шифрування: AES 128; AES 128 с Elephant diffuser; AES 256; AES 256 с Elephant diffuser.

Використання іноземного програмного забезпечення, навіть після його аналізу, не бажано у спеціальних інформаційно-телекомунікаційних системах, так як воно не є досить надійним та безпечним. Інформаційна безпека держави залежить від власних сучасних розробок програмного забезпечення та операційних систем.

*М.О. Котов*

## АНАЛІЗ СУЧАСНИХ МЕТОДІВ ТА МОДЕЛЕЙ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ МІКРОПРОЦЕСОРНИХ СИСТЕМ ЗАЛІЗНИЧНОЇ АВТОМАТИКИ

*M.O. Kotov*

## ANALYSIS OF MODERN METHODS AND SOFTWARE MODELS OF MICROPROCESSOR SYSTEMS OF RAILWAY AUTOMATICS

Сучасний стан розвитку науки транспорту та технологій визначається широким застосуванням комп'ютерно-інтегрованих інформаційних технологій та керуючих систем. На сьогоднішній день процес практичного впровадження комп'ютерної техніки та технологій відбувається дуже інтенсивно практично у всіх галузях народного господарства, у тому числі на залізничному транспорті. Внаслідок цього виникає розрив між теорією та практикою. Особливої уваги заслуговують системи керування рухом поїздів на залізничному транспорті, де питання теоретичного обґрунтування побудови прикладного програмного забезпечення досліджені не достатньо. Переважна більшість розробників використовують експериментальні методи без проведення їх серйозного теоретичного обґрунтування. Таким чином, можна зробити висновок, що наукова проблематика, пов'язана з дослідженням інформаційно керуючих систем на залізничному транспорті, є актуальною як в науковому, так і в практичному плані.

**УДК 656.259.12:656.256.3**

*І.О. Саяпіна*

## ПІДВИЩЕННЯ ЗАВАДОСТІЙКОСТІ ТОНАЛЬНИХ РЕЙКОВИХ КІЛ З ВИКОРИСТАННЯМ НЕЙРОННИХ МЕРЕЖ

*I.O. Saiapina*

## TONAL TRACK CIRCUITS NOISE IMMUNITY IMPROVEMENT USING NEURAL NETWORKS

Відомий пристрій підвищення завадостійкості тонального рейкового кола (ТРК) з централізованим розміщенням обладнання, який дозволяє виключити дію завад на