УДК 681.3

DOI: 10.18664/ikszt.v0i4.53936

МІРОШНИК М.А., д.т.н. (Український державний університет залізничного транспорту)

# Розробка методів оцінки ефективності захисту інформації в розподілених комп'ютерних системах

*Запропоновано шляхи модернізації архітектури корпоративної комп'ютерної системи діагностики режимів систем залізниць, які дозволять підвищити надійність та ефективність системи і забезпечити передумови впровадження комплексного автоматизованого керування. При цьому запропоновано заходи, які включають обов'язкове впровадження систем інформаційної безпеки, організаційне зміщення навантаження обробки оперативної інформації на нижні рівні ієрархії, а також розширення набору протоколів передачі даних, що на сьогоднішній день стало можливим із розвитком мікропроцесорних та комп'ютерних технологій.*

***Ключові слова**: комп'ютерні системи, система захисту інформації, розподілені системи, інформаційний рівень, управління трафіком.*

**Аналіз останніх досліджень і публікацій, в яких започатковано розв'язання даної проблеми**

Основою інформатизації процесу оперативно-диспетчерського керування є інтегроване середовище первинних даних у взаємозв'язку з методами обробки даних. Отримання первинної інформації щодо штатних та аварійних режимів ґрунтується на технологіях розподілених синхронізованих вимірювань. Впроваджені комп'ютерні інформаційно-діагностичні систем залізничного транспорту забезпечують переважним чином функції моніторингу та комерційного обліку, проте через недостатнє теоретичне підґрунтя не реалізують вирішення задач діагностики та оперативного керування. Крім того, впровадження комп'ютерних методів, які забезпечують якісно новий рівень автоматизації процесів керування режимами енергопостачання, на сьогоднішній час, є можливим при дотриманні жорстких вимог безпеки, що в свою чергу потребує вирішення задач забезпечення інформаційного захисту від несанкціонованого доступу та підвищення надійності обладнання [1-5].

**Виділення невирішених раніше частин загальної проблеми, котрим присвячується означена стаття**

Для ефективного впровадження нових методів діагностики та забезпечення передумов реалізації комплексного автоматизованого керування режимами необхідним є проведення аналізу вимог та здійснення відповідних модернізаційних заходів щодо інфраструктурного забезпечення розподілених комп'ютерних інформаційно-діагностичних систем, що на сьогодні є актуальним науково-технічним завданням.



**Формулювання цілей статті (постановка завдання)**

Метою роботи є розробка модернізаційних заходів щодо архітектури розподілених комп'ютерних систем моніторингу, контролю і діагностики електроенергетичних мереж залізничного транспорту, спрямованих на підвищення ефективності функціонування систем, забезпечення можливостей впровадження повноцінних діагностичних функцій та комплексного автоматизованого керування режимами.

**Виклад основного матеріалу дослідження**

*Підвищення продуктивності нижнього вимірювального рівня.* Компоненти корпоративної комп'ютерної системи моніторингу та діагностики на кожному з рівнів ієрархії повинні забезпечуватись відповідними комплексами інформаційного захисту, або системи інформаційної безпеки (СІБ), що є передумовою подальшого використання інфраструктури системи для комплексного автоматизованого керування [3].

Мікропроцесорні пристрої і компоненти комп'ютерної мережі моніторингу та діагностики формують нижній рівень корпоративної комп'ютерної системи, на якому здійснюється формування первинної інформації. Первинна інформація підлягає інтелектуальній обробці та архівуванню, на її основі формуються системні керуючі дії на рівні дистанцій електропостачання або залізниці в цілому, а також організовано комерційний облік електроенергії. На нижньому рівні корпоративної системи в автоматичному режимі вирішується комплекс завдань, пов'язаних з реєстрацією режимних параметрів та забезпечується передача даних на вищі рівні управління [1].

Широко розповсюдженою на сьогоднішній день є базова конфігурація локальних підсистем моніторингу на ділянках електропостачання [4], що передбачає

покладання на розглядуваний рівень корпоративної мережі виключно завдань формування первинного інформаційного простору. При цьому, функції первинної обробки та керування, а також формування системних подій забезпечуються мікропроцесорними пристроями реєстрації, а на основі серверу ділянки електропостачання реалізовуються функції обробки та архівування даних. Повноцінна обробка інформації з метою діагностики стану або керування режимами покладається на верхні ієрархічні рівні [4, 5].

Разом з тим, розподіл функціональності по компонентах та рівнях ієрархії корпоративної системи моніторингу та діагностики на основі базової конфігурації можна переглянути, враховуючи істотне порівняне зростання продуктивності серверних рішень, що пропонуються на сучасному ринку [6, 7]. При цьому пропонується організаційне зміщення навантаження інформаційної обробки оперативної інформації на нижні рівні ієрархії.

На рис. 1 відображено модифіковану функціональну схему умовного інформаційного блока окремої ділянки електропостачання нижнього ієрархічного рівня корпоративної мережі моніторингу та діагностики.

Значний розвиток мікропроцесорних технологій на сьогоднішній день значною мірою дозволяє підвищити обчислювальну здатність пристроїв реєстрації з використанням цифрових сигнальних процесорів (DSPs-Digital Signal Processors), багатоядерних процесорів (MCPs-Multi-Core Processors), процесорів на ПЛІС (Dynamically Reconfigurable Processors based on PLD). Методика побудови мікропроцесорних пристроїв на основі DSPs на сьогоднішній час є найрозвиненішою, при цьому програмна частина реалізовується на основі операційних систем реального часу (RTOS, Real Time Operating System). Використання MCPs та паралельних обчислень в задачах обробки сигналів та обробки даних дозволяє отримувати істотний приріст продуктивності при ефективному розподілі задач між обчислювальними ядрами. Побудова процесорних пристрів на ПЛІС дозволяє створювати проблемно-орієнтовані високопродуктивні обчислювальні платформи. Зокрема запропоновано модель реалізації процесора з модифікованою RISC архітектурою (Reduced Instruction Set Computing - архітектура із скороченим набором команд). Метод організації швидкодійних контролерів паралельної архітектури із реконфігурованою структурою на базі ПЛІС, орієнтованих на рішення задач підвищеної інтелектуальної складності і розмірності запропонований в [8].

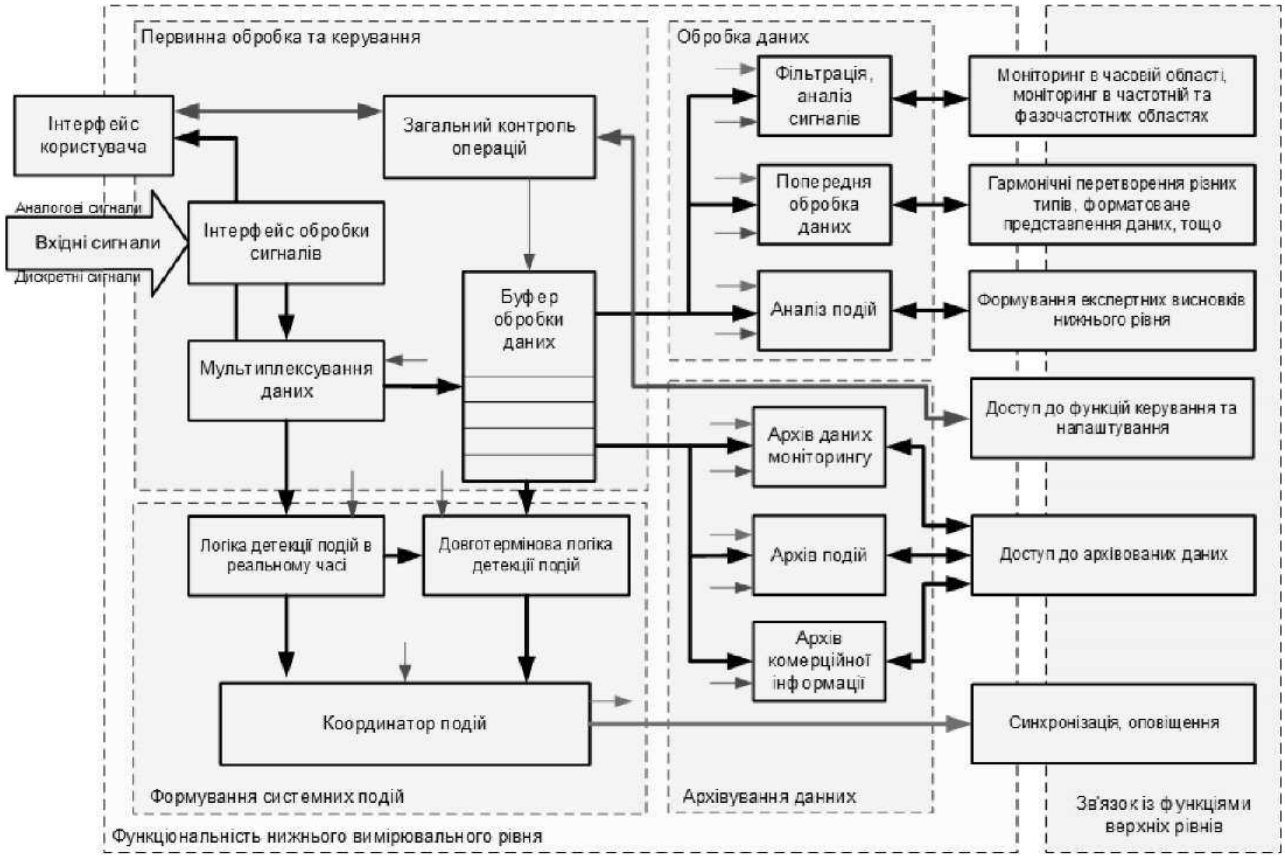


Рис. 1. Функціональна схема умовного інформаційного блока окремої ділянки електропостачання

У разі доповнення нижнього ієрархічного рівня корпоративної комп'ютерної системи повноцінною діагностичною функціональністю, інформаційно-діагностичні функції на ділянках електропостачання фактично реалізовуватимуться локальними підсистемами моніторингу та діагностики у складі корпоративної комп'ютерної системи. Такий розподіл, дозволить реалізацію локальних диспетчерських центрів та локального автоматизованого керування, на основі серверів дистанцій електропостачання. Ресурси серверу будуть задіяні як для реалізації локальних діагностичних процедур так і для необхідного формування вихідних даних для уніфікованих алгоритмів діагностики.

Зміщення навантаження на нижній рівень є виправданим з точки зору архітектури інформаційної мережі, зважаючи на те, що структура та склад локальних підсистем є детермінованими, а також зважаючи на практично незмінну інтенсивність інформаційних потоків, що на етапі проектування дозволяє визначити необхідні програмно-апаратні засоби з мінімальними ресурсними запасами. При цьому, порівняно із базовою конфігурацією, значна частина інформаційних потоків буде локалізуватися у відповідних підсистемах, що дозволить отримати резерв трафіку та обчислювальних потужностей на верхніх рівнях ієрархії.

Крім того, для підвищення ефективності процесів передачі інформації в діагностичних комп'ютерних мережах застосовуються методи прогнозування перевантажень і алгоритми управління чергами. Основною функцією управління трафіком є ефективне управління пропускною здатністю. Перевантаження зазвичай проявляються при недоліках мережних ресурсів або при їхньому неефективному розподілі, та усуваються за допомогою балансування навантаження в мережі. Управління трафіком зводиться до реалізації процедур керування пріоритетами й інтенсивністю переданих пакетів. Аналіз комунікаційних протоколів, які забезпечують управління мережним трафіком, показує, що вони орієнтовані на інтелектуальне обладнання, разом з тим як більша частина мереж використовує неінтелектуальні комутатори і концентратори. Відсутність засобів управління інформаційним трафіком на рівні мереж робочих груп призводить до їхнього перевантаження і, як наслідок, до блокувань переданих пакетів. Це знижує загальну пропускну здатність комп'ютерних мереж і робить малоефективним використання стандартних засобів мережних протоколів для вирішення задач наскрізного управління інформаційним трафіком у середовищі неінтелектуального комунікаційного обладнання автоматизованих керуючих систем.

Найефективніші засоби управління перевантаженням базуються на управлінні буферами/чергами серверів. Якість функціонування системи передачі залежить від величини затримки при передачі пакетів і наявності каналу підтвердження. В модель системи потрібно додати механізм управління у вигляді контуру зворотного зв'язку. При підтвердженні кожного окремого пакета процес формування сигналу зворотного зв'язку можна пов'язати зі зміною стану мережного з'єднання, яке характеризується номером очікуваного до прийому пакета. Бажані властивості алгоритмів керування трафіком містять мінімальну затримку, при заданій продуктивності, або найбільшу продуктивність при заданому значенні затримки.

Таким чином, запропонований розподіл функціональності дозволяє підвищити ефективність використання мережевих каналів зв'язку та загальну ефективність реалізації інформаційно-діагностичних функцій корпоративною комп'ютерною системою.

*Модернізація рішень для інформаційного обміну.* Для застосування у Wide Area Measurement System (WAMS), стандартом C37.118 визначено чотири типи повідомлень, до яких належать дані, заголовки, конфігурації та команди. На рис. 2 приведено схему потоків даних у корпоративних комп'ютерних системах моніторингу та діагностики. Повідомлення що надсилаються від Phasor Measurement Units (PMUs) та локальних концентраторів на верхні рівні ієрархії, найчастіше містять дані щодо режимних параметрів, або можуть містити заголовки подій із описовою інформацією, чи конфігураційні дані. В зворотному напрямку від вузлів доступу можуть надходити повідомлення із передбаченими командами керування та налаштування. При цьому, для використання інфраструктури WAMS в задачах керування режимами енергопостачання необхідним є забезпечення відповідної уніфікованої системи командних повідомлень із керуючих рівнів їх надійної доставки та арбітрування на рівні PMUs.

Регламентовані протоколи обміну передбачають багатопотокову передачу від окремого джерела. Критичні аспекти інформаційної безпеки в частині протоколу обміну включають необхідність обміну в реальному часі, необхідність збереження цілісності та, в деяких випадках, забезпечення конфіденційності. Робота в реальному часі зумовлює критичність корпоративних систем діагностики до термінів доставки повідомлень, і необхідність відповідної швидкодії СІБ. В свою чергу, при контролі цілісності та конфіденційності засобами СІБ, повинна зберігатись обов'язковість доставки повідомлень.

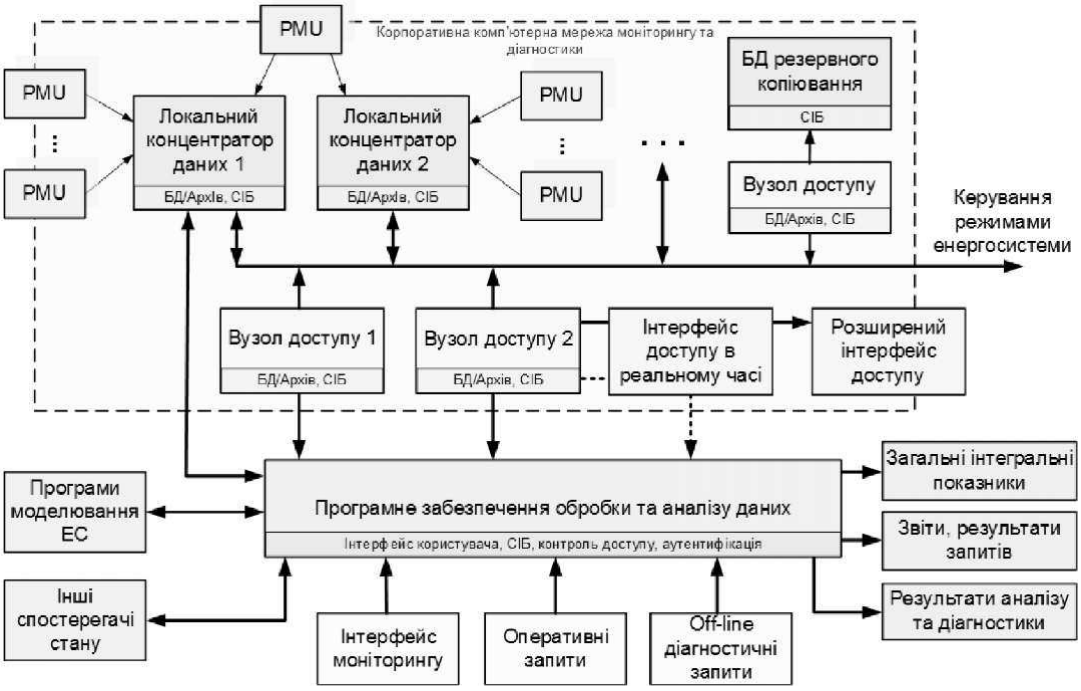


Рис. 2. Потоки даних у корпоративних комп'ютерних системах моніторингу та діагностики

Протоколи передачі даних потокових векторів, реалізовані на прикладному рівні (рівень 7) OSI (Open Systems Interconnection Basic Reference Model, базова модель взаємодії відкритих систем). Оскільки жоден із сучасних стандартів потокової передачі даних від PMUs не вимагає механізмів захисту в своїй структурі, механізми безпеки повинні включатися на нижніх рівнях моделі OSI.

Для запобігання несанкціонованих команд, дані можуть супроводжуватись відповідними підписами, або кодом аутентифікації повідомлення, із використанням в при передачі механізму криптографічного хешування із ключем (HMAC, Hash-based Message Authentication Code). Характер потокових даних в розглядуваних системах, вимагає «швидкої і легкої» методології шифрування для забезпечення цілісності та конфіденційність даних, що може бути реалізовано на основі симетричних алгоритмів типу AES (Advanced Encryption Standard). При цьому основним питанням залишається розподіл ключів, для чого можуть використовуватися інфраструктура відкритих ключів (PKI, Public Key Infrastructure), обмін ключами Діффі-Хеллмана або загальні ключі, якщо кількість пристроїв досить мала.

Доступні рішення для шифрування і аутентифікації протоколів потокових даних в комп'ютерних системах діагностики реалізуються на основі захищених каналів зв'язку в мережах на основі інтернет протоколів типу IPSEC (IP security) та VPNs, а також DTLS (Datagram Transport Layer Security), в той же час, найбільш надійним є використання виділених мереж.

Мережеві протоколи обміну призначені для аналізу і архівування та не підтримують високі швидкості. Використання цих протоколів обмежено внутрішньою мережею. Специфікація формату файлів COMTRADE (C37.111), дозволяє простий розбір, читання та обробку даних від багатьох джерел що генерують, зберігають та передають інформацію. проте не є оптимізованою для передачі по мережах зв'язку. Внаслідок цього, даний формат використовується переважно для архівування та довготривалих операцій в «off-line».

Стандарт OPC UA (Object Linking and Embedding (OLE) for Process Control (OPC) Unified Architecture) адаптовано для забезпечення контролю тривог і подій, пакетної передачі, комунікації сервер-сервер, доступу до архівованих даних, доступу до об'єктів (SOAP, Simple Object Access Protocol) і веб-служб, реалізації механізмів захисту.

Розширення набору протоколів передачі даних, може відбуватися із використанням сучасних протоколів обміну для інтернет-мереж загального використання із врахуванням специфіки корпоративних діагностичних та керуючих комп'ютерних системи. Зокрема пропонується застосування перспективної технології веб-сокетів (WebSocket), орієнтованої на потокову інформацію в реальному часі, що дозволить істотно розширити діагностичні та керуючі можливості верхніх рівнів відносно локальної ділянки спостереження.

**Виводи**

Запропоновано шляхи модернізації архітектури корпоративної комп'ютерної системи діагностики режимів систем залізниць, які дозволять підвищити надійність та ефективність системи і забезпечити передумови впровадження комплексного автоматизованого керування. При цьому запропоновано заходи, які включають обов'язкове впровадження систем інформаційної безпеки, організаційне зміщення навантаження обробки оперативної інформації на нижні рівні ієрархії, а також розширення набору протоколів передачі даних, що на сьогоднішній день стало можливим із розвитком мікропроцесорних та комп'ютерних технологій.

**Література**


1. Никонов В.И. Методы защиты информации в распределенных компьютерных сетях./ Управление, ВТ и информатика Доклады ТУСУРа, № 1 (21), часть 2, июнь, 2010 – с. 219-224.
2. Мирошник М.А. Применение сетей клеточных автоматов в криптографических системах. / М.А. Мирошник, Я.Ю. Королева, И.В. Гормакова // Тези доповідей другої міжнародної науково-практичної конференції «Методи та засоби кодування» 22-24 квітня, Вінниця. – 2009.
3. Мирошник М.А. Диагностические эксперименты в системах защиты информации на сетях клеточных автоматов. / М.А. Мирошник, Я.Ю. Королева // Інформаційно-керуючі системи на залізничному транспорті. – 2009. – №4.
4. Мирошник М.А. Методы эффективного кодирования внутренних состояний микропрограммных автоматов. / М.А. Мирошник, Я.Ю. Королева, // Технология приборостроения. – 2011. – №1.
5. Miroshnik M. Uses of programmable logic integrated circuits for implementations of data encryption standard and its experimental linear cryptanalysis. / Miroshnik M., Kovalenko M. // Інформаційно-керуючі системи на залізничному транспорті. – 2013. – №6, с.36-45.
6. Мирошник М.А. Методы защиты информации в распределенных компьютерных сетях. / М.А. Мирошник // Інформаційно-керуючі системи на залізничному транспорті. – 2014. – №5, с.66-70.
7. Мирошник М.А. Разработка средств защиты информации от в распределенных компьютерных системах и сетях. / М.А. Мирошник // Інформаційно-керуючі системи на залізничному транспорті. – 2015. – №1, с.18-25.
8. Miroshnik M. Implementation of cryptographic algorithms on FPGA-based digital distributed systems. / Miroshnik M. // Інформаційно-керуючі системи на залізничному транспорті. – 2015. – №2, с. 25-36.



**Мирошник М.А. Разработка методов оценки эффективности защиты информации в распределенных компьютерных системах.** Предложены пути модернизации архитектуры корпоративной компьютерной системы диагностики режимов систем железных дорог, которые позволят повысить надежность и эффективность системы и обеспечить предпосылки внедрения комплексного автоматизированного управления. При этом предложены меры, которые включают обязательное внедрение систем информационной безопасности, организационное смещение нагрузки обработки оперативной информации на нижние уровни иерархии, а также расширение набора протоколов передачи данных, что на сегодняшний день стало возможным с развитием микропроцессорных и компьютерных технологий.



**Ключевые слова:** компьютерные системы, система защиты информации, распределенные системы, информационный уровень, управление трафиком.


---


**Miroshnik M.A. Development of effectiveness evaluating methods for distributed computer systems information security.** For effective implementation of new methods of diagnosis and ensuring background for implementation of integrated automated regimes control is necessary to analyze the requirements and implementation of relevant modernization measures of infrastructure supplementation for distributed computer information and diagnostic systems that today are important scientific and technical challenge.

The purpose of the research is to develop measures for modernization of architecture of distributed computer systems for monitoring, control and diagnostics of electric power networks in railway transport, aimed at improving of the systems performance efficiency, ensuring the ability of full implementation of diagnostic functions and integrated automated modes control.

The ways of upgrading the architecture of corporate computer system diagnostics modes of railways that will improve the reliability and efficiency of the system and provide the preconditions implementation of integrated automated control. This proposed measures include mandatory implementation of information security, organizational bias operative information processing load on the lower level of the hierarchy, and expanding set of data transfer protocols, which today became possible with the development of microprocessor and computer technology.



**Key words**: computer systems, information security, distributed systems, information level traffic management.

Рецензент Лістровий С.В., д.т.н., професор, професор кафедри СКС (УкрДУЗТ)

*Поступила 02.06.2015г.*



***Мірошник М.А.,*** *д.т.н., професор кафедри СКС, Український державний університет залізничного транспорту, Харків, Україна.*

***Miroshnik M.A.,*** *Dr. of tech. science, Ukrainian State University of Railway Transport, Kharkiv, Ukraine.*