

УДК 004.056

**С. Сербичанський**

(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

## **ДОСЛІДЖЕННЯ ВИМОГ ДО ФІЗИЧНОГО ТА ПРОГРАМНОГО ЗАХИСТУ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ЗАГРОЗ І ОБМЕЖЕНЬ**

UDC 004.056

**S. Serbychanskyi**

## **STUDY OF REQUIREMENTS FOR PHYSICAL AND SOFTWARE PROTECTION OF INFORMATION AT CRITICAL INFRASTRUCTURE OBJECTS UNDER THE CONDITIONS OF THREATS AND LIMITATIONS**

Електромережі є основою в сучасному світі, засоби зв'язку, банківська ж система, медична система та більшість інших важливих систем які не можна увити без систем електропостачання. Передбачається, що до 2050 року світове електроспоживання зросте втричі.

Переважно атомні електростанції покривають базову потребу використання (тобто використання електроенергії яке є постійним). Гідроелектростанції покривають в першу чергу перепади в потребах живлення до прикладу час пік.

Теплові електростанції покривають постійні та незначні перепади електроенергії. Звісно існують різні конфігурації мереж в залежності від потреб. Про те швидке інформування місць генерації електроенергії є досить складною задачею. Погіршує проблему саме використання зеленої електроенергетики. Таким чином ж інформування місць генерації та швидка взаємодія набуває основного значення.

Тому різними державами активно виділяється значна кількість коштів на розробку нової системи, що повинна пов'язати місця виробництва електроенергії та їх використання. Нові мережі мають децентралізовану цифрову інфраструктуру, що називаються smart grid.

Smart Grid об'єднує кілька добре відомих, але відмінних галузей, а саме електроенергетику, інформаційні технології та зв'язок.

Кожен пристрій у новій сітці, ймовірно, матиме власну IP-адресу та використовуватиме для зв'язку такі протоколи, як TCP/IP. Таким чином, вони будуть уразливі до подібних загроз безпеці, з якими стикаються сучасні комунікаційні мережі, однак ставки набагато вищі.

Для автентифікації пристрою використовуються алгоритми з відкритим ключем які не є досконалыми та мають ряд недоліків при використанні в мережах smart grid.

Альтернативою використанню ресурсоємної автентифікації відкритого ключа є система на основі дерев Меркла. Дерев Merkle пропонують недорогу автентифікацію для mesh-клієнтів. Порівняно з відкритим ключем, вони легкі та швидкі для генерації та пропонують такий самий, а у деяких випадках, кращий захист.