УДК 004.4

АНАЛІЗ КІБЕРБЕЗПЕКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ КОМП'ЮТЕРНОЇ СИСТЕМИ УПРАВЛІННЯ АЕС

CYBER SECURITY ANALYSIS OF THE SOFTWARE OF THE COMPUTER SYSTEM OF NPP MANAGEMENT

Борис Вінтенко, Олексій Смірнов, Тетяна Смірнова

Центральноукраїнський національний технічний університет, пр. Університетський, 8, Кропивницький, 25006, Україна

Abstract. *This work is devoted to the detailing of measures to ensure the investigated aspects of cyber security, as well as the description of the sequence of actions that are proposed to ensure the cyber security of new software of a computer control system during the development and assessment of the compliance of the software of existing computer control systems with the requirements of cyber security.*

Виходячи з досліджених вимог стандартів з кібербезпеки, можуть бути виділені критерії, які доцільно враховувати під час проектування та оцінки захищеності програмного забезпечення (ПЗ) комп'ютерної системи управління **(**КСУ): фізичний захист технічних засобів; управління конфігурацією ПЗ; контроль за відсутністю прихованих функцій в ПЗ; захищеність доступу до ПЗ; автентифікація при доступі до функцій ПЗ; напрямки прийому та/або передачі даних; захищеність від некоректності прийнятих даних; контроль параметрів, що вводяться оператором. Нижче наводиться опис дослідження ПЗ за даними критеріями.

Для дослідження базових критеріїв необхідним етапом є складання переліку технічних засобів КСУ та ПЗ, що входить до його складу. На цьому етапі можливий розгляд ПЗ з точки зору наступних критеріїв: фізичний захист технічних засобів; управління конфігурацією ПЗ; контроль за відсутністю прихованих функцій в ПЗ; захищеність доступу до ПЗ; автентифікація для доступу до функцій ПЗ.

Базові фактори впливу на кібербезпеку. Для будь-якого ПЗ проводяться наступні дотримання та перевірки: фізична захищеність; контроль конфігурації; відсутність прихованих функцій. На всіх етапах життєвого циклу (ЖЦ) ПЗ, від розробки до інтеграції та встановлення, необхідне використання ліцензованих та верифікованих інструментів, бібліотек мов програмування. Це унеможливлює внесення прихованого коду або функцій під час редагування коду розробником або компіляції;

Доступ до ПЗ як фактор, що впливає на кібербезпеку. При забезпеченні кібербезпеки КСУ АЕС доступ до ПЗ може розглядатися в двох аспектах: доступ до функцій ПЗ та доступ до складових частин ПЗ. Доступ до функцій ПЗ відбувається через інтерфейс користувача ПЗ та необхідний оперативному персоналу під час регламентних операцій, корекції параметрів, отримання інформації, перевірок та технічного обслуговування КСУ. Під доступом до складових частин ПЗ мається на увазі доступ до файлів програм ПЗ, файлів конфігурації, баз даних, змісту енергонезалежної пам'яті тощо, а також доступ до конфігурації середовища функціонування ПЗ, наприклад IP-адреси мережевих карт або портів введення-виведення.

Висновок: проведені основні рекомендації з реалізації вимог кібербезпеки в ПЗ. Необхідно зазначити, що для контролю виконання даних вимог зручно створити кількісний показник. Для розв'язання даної задачі може бути складений звіт, в якому для кожного компонента ПЗ КСУ зазначається застосовність певних вимог кібербезпеки та відповідність даним вимогам. Інформація з даного звіту може бути використана для розрахунку числового показника кібербезпеки ПЗ.