Цивільна безпека

УДК 004.4 **doi: 10.26906/SUNZ.2023.3.155**

Б. Ю. Вінтенко[1], О. А. Смірнов[2], А. С. Коваленко[2], С. А. Смірнов[2], К. О. Буравченко[2]

[1] ПАТ "Науково-виробниче підприємство "Радій", Кропивницький, Україна
[2]Центральноукраїнський національний технічний університет, Кропивницький, Україна

ДОСЛІДЖЕННЯ ВИМОГ МІЖНАРОДНИХ СТАНДАРТІВ IEC 60880 ТА IEC 62138 З РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНО-КЕРУЮЧИХ СИСТЕМ АЕС, ВАЖЛИВИХ ДЛЯ БЕЗПЕКИ

Анотація. На сьогоднішній день значна частина електричної енергії виробляється атомними електростанціями. Атомна енергетика – це дешевий, економічно вигідний та екологічний спосіб забезпечення потреб людини електроенергією. Разом з тим, це виробництво пов'язане з необхідністю забезпечення захисту людини та навколишнього середовища від іонізуючого випромінювання ядерного палива під час нормальної експлуатації станції та при виникненні аварійних ситуацій. Атомні електростанції (АЕС) містять велику кількість обладнання для забезпечення технологічних процесів та виконання функцій безпеки. **Метою** роботи є дослідження вимог до формування життєвого циклу, основних етапів проектування і документуванням програмного забезпечення комп'ютерних систем управління атомних електростанцій (ПЗ КСУ АЕС), що виконують функції безпеки категорій «А», «В» та «С». Вимоги до ПЗ, що виконує функції безпеки категорії «А», наведені в міжнародному стандарті IEC 60880 «Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions», вимоги до ПЗ, що виконує функції безпеки категорії «В» і «С», наведені в міжнародному стандарті IEC 62138 «Nuclear power plants – Instrumentation and control important for safety – Software aspects for computer-based systems performing category B or C functions». **Об'єктом дослідження** є процес розробки програмного забезпечення для комп'ютерних систем управління АЕС. **Предметом** є дослідження вимог міжнародних стандартів IEC 60880 та IEC 62138 з розробки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки. **У результаті дослідження** розглянута загальна структура вимог стандартів IEC 60880 та IEC 62138, визначені групи учасників, які приймають участь в розробці ПЗ КСУ АЕС та розподілення видів діяльності з розробки ПЗ між цими групами, проведений аналіз вимог загальних вимог та вимог до етапу розробки специфікації ПЗ, вимог до етапу проектування та реалізації ПЗ, вимог до етапу верифікації, інтеграції та валідації та вимог до етапу встановлення, експлуатації та модифікації, сформована таблиця розподілення вимог до ПЗ, досліджені засоби імплементації вимог, визначена проблема оцінки відповідності стандарту. **Висновки.** Міжнародні стандарти IEC 60880 та IEC 62138 містять важливі вимоги до всіх етапів розробки ПЗ КСУ АЕС, важливого для безпеки. Вимоги стосуються як організаційних питань, так і технічних аспектів. Згідно з цими стандартами, кожне підприємство, що займається розробкою ПЗ КСУ АЕС, має визначити робочі групи, які будуть реалізовувати різні етапи ЖЦ (проектування, реалізація, верифікація тощо). Стандарти не містять вимог до інтерфейсів користувача ПЗ. Тому одним з напрямків наступних досліджень стануть вимоги інших міжнародних стандартів – IEC 61772 «Nuclear power plants – Control rooms – Application of visual display units (VDUs)» («Візуальні пристрої відображення») та IEC 62646 «Nuclear power plants – Control rooms – Computer-based procedures» («Комп'ютеризовані процедури»), а також вимоги галузевих нормативних документів, таких як NUREG-0700 «Human-System Interface Design Review Guidelines» – «Побудова інтерфейсів «людина-машина» (U.S. Nuclear Regulatory Commission, США). В стандартах не визначається загальноприйнятих метрик, що вказують ступінь відповідності ПЗ даним стандартам. Виходячи з цього, кожна організація, яка виконує оцінку відповідності ПЗ та КСУ в цілому вимогам стандартів, повинна створити власну методику такої оцінки. Тому метою наступних досліджень є вивчення засобів оцінки специфікацій вимог, метрик коду ПЗ, критеріїв повноти тестування ПЗ, які можуть бути використані для розробки формальних методик оцінювання ПЗ вимогам стандартів.

Ключові слова: програмне забезпечення, комп'ютерні системи управління, АЕС, IEC 60880, IEC 62138.

Вступ

Постановка проблеми. На сьогоднішній день значна частина електричної енергії виробляється атомними електростанціями [1]. Атомна енергетика – це дешевий, економічно вигідний та екологічний спосіб забезпечення потреб людини електроенергією. Разом з тим, це виробництво пов'язане з необхідністю забезпечення захисту людини та навколишнього середовища від іонізуючого випромінювання ядерного палива під час нормальної експлуатації станції та при виникненні аварійних ситуацій.

Атомні електростанції (АЕС) містять велику кількість обладнання для забезпечення технологічних процесів та виконання функцій безпеки.

Аналіз останніх досліджень і публікацій. Функції безпеки в залежності від наслідків відмови і хибного спрацювання класифікують за категоріями. У різних нормативних документах класифікація функцій безпеки може відрізнятися. У відповідності з міжнародним стандартом IEC 61226 («КСУ АЕС ВБ. Розподіл за категоріями ФБ») [4] виділяють 3 категорії функцій безпеки: «А», «В» та «С». У відповідності з нормативним документом МАГАТЕ «Safety Classification of Structures, Systems and Components in Nuclear Power Plants: Specific Safety Guide No. SSG-30» [5] виділяють 3 класи безпеки: «1», «2» та «3». З метою уникнення дублювання класифікації категорій в даній статті буде використовуватися позначення категорій за допомогою літер «А», «В» та «С», як

вказано в стандарті IEC 61226. Функції категорії «A» є найбільш важливими для попередження або захисту під час аварійних ситуацій, функції категорій «B» та «C» мають менший ступінь важливості.

Всі пристрої, системи і компоненти, включаючи програмне забезпечення (ПЗ) для контроля і управління, що являються елементами, важливими для безпеки, повинні бути визначені, а потім класифіковані на основі функції, що виконується, і важливості для безпеки. Огляд класифікації комп'ютерних систем управління (КСУ) і програмного забезпечення (ПЗ) у відповідності із стандартами і нормативними документами наведений у [12].

Постановка задач дослідження. Метою даної статті є дослідження вимог до формування життєвого циклу, основних етапів проектування і документуванням програмного забезпечення комп'ютерних систем управління атомних електростанцій (ПЗ КСУ АЕС), що виконують функції безпеки категорій «A», «B» та «C». Вимоги до ПЗ, що виконує функції безпеки категорії «A», наведені в міжнародному стандарті IEC 60880 «Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions» [6], вимоги до ПЗ, що виконує функції безпеки категорії «B» і «C», наведені в міжнародному стандарті IEC 62138 «Nuclear power plants – Instrumentation and control important for safety – Software aspects for computer-based systems performing category B or C functions» [7].

Загальна структура вимог стандартів IEC 60880 та IEC 62138

Область застосування. У розділі 1 обох стандартів областю застосування вказуються вимоги до ПЗ комп'ютерних систем управління, що виконують функції безпеки категорії «A» (IEC 60880) і «B» і «C» (IEC 62138). Мета цих вимог – створення ПЗ високого ступеню надійності, яке має мінімальну імовірність наявності прихованих програмних дефектів.

Нормативні посилання. У розділі 2 обох стандартів міститься перелік нормативів, що мають відношення до розробки ПЗ КСУ АЕС, важливих для безпеки. Це стандарти IEC 61508, IEC 61513, IEC 61226, нормативні документи МАГАТЕ тощо.

Терміни та визначення, скорочення. У розділі 3 обох стандартів визначаються поняття, які використовуються при формуванні вимог. Серед цих термінів та визначень необхідно відмітити найголовніші: універсальна мова, проблемно-орієнтована мова, раніше розроблене ПЗ, автоматизована генерація коду, ущільнення коду, самоконтроль, різноманітність тощо.

У розділі 4 обох стандартів наводиться список використовуваних скорочень та абревіатур.

Детальні вимоги. Починаючи з розділу 5, в обох стандартах наводиться основна частина вимог до розробки ПЗ.

Типи ПЗ та даних. Стандарти розробки ПЗ КСУ АЕС поділяють програмне забезпечення на типи: операційне ПЗ та прикладне ПЗ. Кожне ПЗ використовує конфігураційні дані, які також поділяються на категорії: незмінні (є частиною специфікації проекту) та змінні (можуть бути змінені оперативним персоналом в необхідних межах).

Етапи життєвого циклу ПЗ. Стандарт IEC 61513 описує життєвий цикл (ЖЦ) КСУ в цілому та визначає заходи, які мають відбуватися на всіх його етапах. Згідно концепцій цього стандарту, програмне забезпечення є невід'ємною частиною КСУ, ЖЦ ПЗ тісно пов'язаний з ЖЦ всієї системи. Стандарти КСУ IEC 60880 та IEC 62138 містять вимоги до ЖЦ ПЗ та конкретизують види діяльності, що відносяться до розробки ПЗ. Вони розглядають розробку апаратного та програмного забезпечення як паралельні процеси, які об'єднуються на етапі інтеграції.

В табл. 1 наведені етапи ЖЦ КСУ АЕС, види діяльності з розробки в межах цих етапів та номери підрозділів стандартів IEC 60880 та IEC 62138, що описують вимоги до відповідного виду діяльності.

Таблиця 1 – **Етапи ЖЦ та види діяльності з розробки ПЗ КСУ АЕС**

Етап ЖЦ	Вид діяльності	Підрозділ IEC 60880	Підрозділ IEC 62138
Всі етапи	Керування розробкою	5.4	6.2.1
	Виконання вимог плану забезпечення якості ПЗ	5.5	6.2.1
	Керування конфігурацією ПЗ	5.6	6.2.3
Розробка специфікації вимог до ПЗ	Планування захищеності ПЗ	5.7	6.4.4.4
	Планування захисту від відмов з загальної причини	13	6.12
	Вибір та аналіз придатності раніше розробленого ПЗ	15	6.3
	Розробка специфікації вимог до нового ПЗ	6.1-6.3, дод. «A»	6.4
Розробка проекту ПЗ та реалізація	Вибір інструментального ПЗ	14	6.2.4
	Вибір мов програмування	7.2, дод. «B»	6.2.5
	Створення проекту ПЗ	7, дод. «B»	6.5
	Реалізація нового ПЗ	7, дод. «B»	6.6
	Створення документації	7.4	6.5
Всі етапи	Верифікація	8	6.2.2
Інтеграція системи	Інтеграція ПЗ до КСУ	9	6.7
Валідація системи	Валідація ПЗ в складі КСУ	10	6.8
Встановлення системи	Встановлення ПЗ на місці експлуатації Навчання персоналу	12	6.9
Модифікація системи	Аналіз запитів на модифікацію, модифікація ПЗ	11	6.10, 6.11

Слід відмітити, що послідовність підрозділів, які описують види діяльності в межах кожного етапу, в стандартах IEC 60880 та IEC 62138 дещо відрізняються.

Висновки. Виходячи з структури вимог до розробки ПЗ КСУ АЕС, можна виділити окремі групи учасників цього процесу та побудувати схему взаємодії між ними. В наступному розділі наведено детальний розгляд цих груп.

Групи учасників, які приймають участь в розробці ПЗ КСУ АЕС

В розробці ПЗ КСУ АЕС можна виділити наступні групи учасників:

– група керування розробкою та контролю забезпечення якості (менеджмент) – учасники, що виконують керування проектом та контроль виконання плану забезпечення якості;

– група проектування ПЗ – учасники, що отримують специфікацію системи (технічне завдання) та формують специфікацію вимог до ПЗ;

– група розробки ПЗ – учасники, що розробляють проект ПЗ та виконують його реалізацію відповідно до специфікації вимог;

– група верифікації та валідації – учасники, що виконують перевірку ПЗ на всіх етапах ЖЦ;

– група інтеграції – учасники, які здійснюють об'єднання апаратного та програмного забезпечення в єдину систему;

– група впровадження та супроводу – учасники, що забезпечують контроль над встановленням КСУ на місці експлуатації, виконують функції супроводу (навчання персоналу, збір інформації про використання КСУ, обробка запитів на модифікацію).

Слід відмітити те, що менеджмент групи верифікації та валідації повинен бути незалежним від менеджменту інших груп у випадку розробки ПЗ категорій «А» та «В».

Схема взаємодії між цими групами та їх основні види діяльності наведені на рис. 1.

Висновок. Одним з результатів дослідження вимог стандартів до розробки ПЗ КСУ АЕС є розподілення учасників розробки на функціональні групи. Це дає можливість створити колектив учасників з відповідними компетенціями та спроектувати їх комунікацію між собою. Наступний розділ описує можливий варіант розподілу видів діяльності з розробки ПЗ між групами.

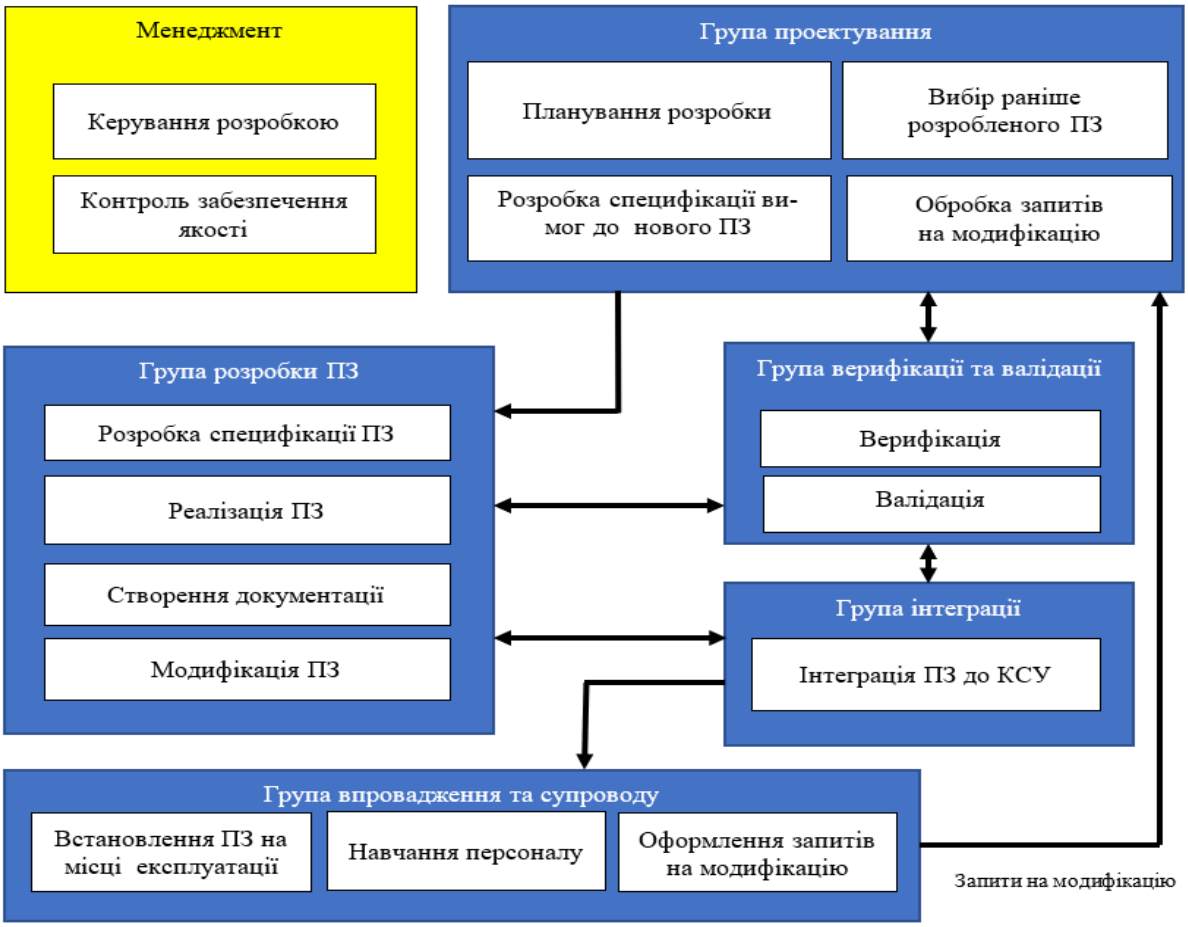

Рис. 1. Схема взаємодії між групами розробки ПЗ КСУ АЕС

Розподілення видів діяльності з розробки ПЗ між групами

Виходячи з того, що в розробці ПЗ КСУ АЕС беруть участь різні групи виконавців, очевидно, що різні етапи ЖЦ ПЗ, види діяльності з розробки ПЗ та вимоги стандартів IEC 60880 та IEC 62138 можуть в переважній мірі стосуватись окремих груп.

Орієнтовне відношення етапів ЖЦ, видів діяльності до окремих груп наведені в табл. 2.

Таблиця 2 – **Розподілення етапів ЖЦ та видів діяльності з розробки ПЗ між групами**

Етап ЖЦ ПЗ	Види діяльності в межах етапів ЖЦ ПЗ	Групи учасників
Всі етапи	Керування розробкою Контроль виконання вимог плану забезпечення якості ПЗ	Менеджмент
Розробка специфікації вимог до ПЗ	Вибір та аналіз придатності раніше розробленого ПЗ Планування захищеності ПЗ Планування захисту від відмов з загальної причини Розробка специфікації вимог до нового ПЗ	Група проектування ПЗ Група розробки ПЗ
Розробка проекту ПЗ та реалізація	Аналіз специфікації вимог до ПЗ Конфігурування раніше розробленого ПЗ Вибір інструментального ПЗ Вибір мов програмування Розробка специфікації нового ПЗ Реалізація нового ПЗ Створення документації Аналіз результатів верифікації, інтеграції та валідації	Група розробки ПЗ
Всі етапи	Верифікація результатів кожного етапу ЖЦ ПЗ Валідація ПЗ під час розробки	Група верифікації Група розробки ПЗ
Інтеграція системи	Інтеграція ПЗ до КСУ	Група інтеграції Група розробки ПЗ
Валідація системи	Валідація ПЗ в складі КСУ	Група верифікації
Встановлення системи	Встановлення ПЗ на місці експлуатації КСУ Навчання оперативного персоналу Оформлення запитів на модифікацію ПЗ	Група впровадження Група розробки ПЗ
Модифікація системи	Аналіз запитів на модифікацію ПЗ Модифікація ПЗ	Група проектування ПЗ Група розробки ПЗ

Слід зазначити, що розподілення вимог стандарту між учасниками не усуває необхідність знайомства окремих учасників з повним змістом всього стандарту. Проте головний **висновок** цього розподілення вказує на те, що при підготовці до розробки ПЗ з урахуванням вимог стандартів IEC 60880 та IEC 62138 учасники груп можуть визначити, які розділи та вимоги стандартів, види діяльності стосуються їх першочергово, а які – опосередковано.

В наступних розділах даної статті наводиться більш детальний аналіз вимог усіх розділів стандартів.

Аналіз вимог загальних вимог та вимог до етапу розробки специфікації ПЗ

В даному підрозділі проводиться дослідження основних вимог стандартів IEC 60880 та IEC 62138, які стосуються етапів діяльності, що є визначаючими та підготовчими до реалізації.

Керування розробкою. Процес розробки ПЗ має бути розділеним на декілька етапів. Етапи можуть або впливати на наступні, або залежати від попередніх. Всі етапи мають бути офіційно визначеними, жодний з них не може бути пропущений. Діяльність в межах етапів повинна співвідноситися з повним життєвим циклом ПЗ. Вимагається, щоб для кожного етапу було визначено та задокументовано:

– мета та виконавці;

– зміст та властивості вхідних та вихідних даних.

Документи, що описують кожний етап розробки, мають аналізуватися та перевірятися.

План забезпечення якості ПЗ. На ранніх етапах ЖЦ ПЗ має бути створений план забезпечення якості ПЗ, якого необхідно дотримуватися всім учасникам процесу розробки. В ньому має вимагатися:

– наявність опису всіх необхідних технічних процедур для кожного етапу;

– визначення всіх специфічних термінів та умовних позначень;

– визначення того, які методи, засоби, мови та правила застосовуються до яких видів діяльності;

– реалізація всіх етапів компетентними особами з наданням їм відповідних ресурсів;

– встановлення та обґрунтування відхилень від вимог стандарту;

– модифікація вже затверджених документів на основі чіткого визначення конкретних змін, їх аналізу та затвердження.

Згідно вимог стандарту, результати виконання плану забезпечення якості мають бути оформлені документально.

Керування конфігурацією. Стандарт IEC 60880 та IEC 62138 вимагають забезпечувати ідентифікацію всіх версій ПЗ, документації на нього, трансляторів та інших інструментальних програм. Має бути встановлений зв'язок між окремими версіями ПЗ та відповідними до них версіями документації. Повна версія програмного продукту повинна однозначно ідентифікуватися версіями повного набору компонентів ПЗ, що входять до нього. ПЗ, що знаходиться в розробці, має бути відділене від ПЗ, розробка та верифікація якого вже завершена.

Захищеність. Мета захищеності ПЗ та даних – унеможливити доступ до ПЗ та його функцій неуповноваженими особами. Згідно стандарту IEC 61513, забезпечення захищеності ПЗ є частиною забезпечення захищеності КСУ.

Згідно вимог стандарту IEC 60880, для ПЗ категорії «А» необхідне обов'язкове проведення аналізу потенційних загроз. На основі аналізу мають бути сформовані вимоги до проекту ПЗ з метою мінімізувати вразливості.

Зокрема, мають бути реалізовані:

– захист від змін ПЗ оператором;

– обмеження прав доступу користувачів до функціонально необхідних;

– встановлення безпечних діапазонів для даних, що змінюються оператором;

– відслідковування модифікацій ПЗ та його параметрів;

– заходи проти наявності прихованих функцій та засобів навмисного забезпечення несанкціонованого доступу.

Для ПЗ категорії «В», «С» в стандартах не вказуються конкретні вимоги до захищеності.

Самоконтроль. Згідно вимог стандартів IEC 60880 та IEC 62138, ПЗ категорії «А» та «В» повинно контролювати технічний стан КСУ та власну поведінку у визначені проміжки часу. Функції контролю повинні виявляти відмови апаратних засобів, помилкову поведінку ПЗ або порушення процесів передачі даних. В процесі самоконтролю має бути передбачений автоматичний збір діагностичної інформації для подальшого аналізу. При виявленні порушення має відбутися реакція у відповідності до проекту системи.

Періодичні тестування. ПЗ категорії «А» повинно мати здатність до проведення періодичних тестувань всіх функцій безпеки для виявлення будь-яких відмов. Має бути реалізований автоматичний збір діагностичної інформації про проведення та результати тестувань. ПЗ категорії «В» повинно мати таку здатність, якщо це не призводить до його надмірної складності.

Специфікація вимог до ПЗ. За результатами аналізу вимог до ПЗ повинна бути створена специфікація вимог. Це документ, який описує те, що повинна робити програма, а не те, як вона повинна це робити. Зокрема, в ньому повинні бути вказані:

– загальні характеристики (розрядність, типи обміну);

– вимоги до технічних засобів або посилання на відповідний документ;

– прикладні функції, що виконуються ПЗ;

– типи поведінки ПЗ, режими його роботи;

– інтерфейси ПЗ з користувачем та іншими системами;

– параметри ПЗ, що можуть бути змінені оператором;

– технологічні та функціональні обмеження;

– вимоги до самоконтролю та усунення наслідків відмов;

– вимоги до середовища роботи та стандартного ПЗ.

Внаслідок важливості даного етапу, процес встановлення специфікації вимог має бути строгим та оформленим документально. Специфікація вимог має бути однозначною, підлягати верифікації або тестуванню, а також досяжною для реалізації. Вона має бути доступною замовнику, клієнту, кінцевому користувачу, групі розробки, верифікації, оцінки та ліцензування.

Висновки. Керування проектуванням, планування та створення специфікації вимог до ПЗ є процесами, які є підготовчими до створення проекту та реалізації ПЗ розробниками.

Аналіз вимог до етапу проектування та реалізації ПЗ

Вимоги до раніше розробленого ПЗ. Для реалізації вимог до програмного забезпечення може бути використане раніше розроблене ПЗ (РПЗ), яке відповідає необхідним вимогам. Це може бути ПЗ різного розміру – від невеликих бібліотек до великих програмних продуктів. Використання РПЗ може бути більш вигідним, ніж розробка нового, особливо в тому випадку, якщо це РПЗ вже пройшло валідацію для використання в аналогічних системах.

РПЗ має відповідати всім вимогам стандартів розробки ПЗ КСУ АЕС відповідної категорії.

Для прийняття рішення про використання РПЗ потрібно визначити його придатність для виконання необхідних функцій. Потрібно відмітити, що для використання РПЗ може бути необхідно виконати його конфігурування або адаптацію. Інформацію для визначення придатності РПЗ необхідно отримати з його документації, в разі необхідності потрібно провести додатковий аналіз. В документації мають бути описані інтерфейси, функції, формати даних, обмеження тощо.

В разі прийняття позитивного рішення про використання РПЗ необхідне проведення оцінки його якості. Ця задача може бути розв’язана на основі вивчення документації з сертифікації та атестації. Має бути проаналізовано план забезпечення якості РПЗ, документи з специфікації, проекту, реалізації, результатів верифікації. Досвід з експлуатації РПЗ є доповненням до інформації, на основі якої приймається рішення про його застосування. Інформація про досвід експлуатації є більш вагомою, якщо накоплена за тривалий час, на великій кількості КСУ тощо.

В разі прийняття позитивного рішення про використання РПЗ, воно має бути введене під керування конфігурацією. Для використання повинна бути визначена та версія РПЗ, що була атестована. В плані забезпечення якості КСУ мають бути передбачені процедури оновлення РПЗ на більш нову версію при виникненні необхідності.

Таким чином, з досліджень вимог стандартів IEC 60880 та IEC 62138 можна зробити **висновок**, що для виконання функцій ПЗ всіх категорій безпеки КСУ АЕС можна використовувати РПЗ, але після проведення аналізу його придатності та оцінки якості. Підвищення категорії функцій безпеки збільшує жорсткість вимог до РПЗ, об’єму документації та процедур перевірок.

Загальні вимоги до інструментальних засобів. Використання інструментальних засобів зменшує кількість помилок в процесі розробки, підвищує надійність та скорочує час розробки. Такими засобами є засоби розробки програм, засоби конфігурування, транслятори, компілятори, засоби автоматизації тестувань, контролю версій, роботи з даними тощо.

Для інструментальних засобів розробки ПЗ функціональної безпеки «А»:

– повинна бути проведена верифікація та оцінка імовірності внесення ними дефектів;

– має бути розроблена та застосовуватися процедура атестації. Атестація маж визначити імовірність

того, що інструментальна програма внесе дефекти до ПЗ, а також наслідки внесення таких дефектів. Під час атестації має враховуватися інформація від розробника інструментального засобу, його документація, тестування та валідація, а також досвід використання.

Вибір інструментальних засобів розробки ПЗ функціональної безпеки «B» та «C» має ґрунтуватися на підтвердженні їх якості. Суворість вимог до якості залежить від важливості функцій і серйозності дефектів, які можуть бути внесені в ПЗ цим засобом.

Використання кожного інструментального засобу має бути документально оформлене. Мають бути чітко вказані процеси розробки за участю цього засобу, його вплив на генерований код та інші процеси розробки, його захищеність від помилок та несанкціонованих дій тощо.

Має бути чітко визначена версія та конфігурація кожного інструментального засобу. Для ПЗ категорії «A» та «B» перехід на використання нових версій має відбуватися після підтвердження того, що зміна версії не вносить дефекти в програму.

Для внесення різноманітності як засобу підвищення надійності ПЗ можуть використовуватися різні інструментальні засоби, що мають однакову функціональність. Їх різноманітність підтверджується отриманням їх від різних постачальників, різними процесами використання, різними мовами програмування тощо.

Транслятори та компілятори, що використовуються, не повинні без попередження видаляти захисні функції, що додаються програмістом. Оптимізація коду, що ґенерується компілятором, не повинна ускладнювати його. Для коду, який підлягав оптимізації, має бути передбачена верифікація та валідація.

Висновок. Інструментальні засоби – це необхідні компоненти в розробці ПЗ, кожен з яких згідно умов стандартів розробки ПЗ має бути обґрунтовано обраний, верифікований та атестований.

Вибір мов програмування. Для розробки ПЗ високої якості важливо обрати таку мову програмування, що дозволить реалізувати всі необхідні вимоги до ПЗ. Стандарти розробки ПЗ КСУ АЕС IEC 60880 та IEC 62138 містять рекомендації щодо вибору мов програмування. Вони поділяють мови програмування на два види: універсальні та проблемно-орієнтовані. Універсальні мови програмування є загальноприйнятими: C, C++, Асемблер, VHDL, Java, Python тощо. Код, написаний цими мовами, може бути безпосередньо завантажений до обчислювальних пристроїв та виконуватися ними.

Проблемно-орієнтовані мови програмування використовують методи формалізації для позначення операцій, такі як діаграми, блоки та зв'язки між ними. Це дає можливість створювати проекти фахівцям, що не мають навичок написання коду на універсальних мовах. Оформлення програми за допомогою проблемно-орієнтованих мов є більш наближеним до прикладної області. Генерація програмного коду для завантаження до обчислювальних пристроїв в цьому разі виконується автоматично.

Деякі рекомендації в стандартах наводяться для обох видів мов, деякі – тільки для одного виду.

Загальні вимоги стандарту **IEC 60880 щодо мов програмування для створення ПЗ категорії «A»** наступні:

– мова програмування повинна мати чітко визначений та документований синтаксис та правила написання коду;

– за можливості повинен використовуватися «скорочений», максимально «безпечний» варіант мови;

– мова програмування повинна мати перевірений транслятор.

Для універсальних мов програмування:

– пріоритет має віддаватися розповсюдженим та загальноприйнятим мовам програмування;

– пріоритет має віддаватися мовам програмування високого рівня;

– програма, написана обраною мовою, повинна бути легкою для читання;

Мова програмування повинна забезпечувати:

– можливість перевірки типів та меж значень змінних;

– можливість перевірки на вихід за межі масиву;

– можливість відслідковування помилок (наприклад, генерації виключень) при виході за межі масиву, використанні неініціалізованих змінних, відкиданні значущих розрядів чисел, неспівпадння типів даних. При цьому засоби мови не повинні намагатися автоматично «виправити» помилку;

– заборону використання неявних перетворень типів;

– явну декларацію змінних;

– використання довгих імен змінних та функцій;

– перевірку типів даних, межі масивів тощо на етапі компіляції програми, а не її виконання.

Для проблемно-орієнтованих мов програмування:

– використання стандартних позначень технологічних одиниць;

– можливість розбиття програми на модулі;

– невисока складність елементів, з яких складається програма;

– відсутність функціонально небезпечних елементів;

– проста структура коду, що генерується, наприклад переважно лінійна;

– формат програми має бути зрозумілий для технічних фахівців, які не є фахівцями в програмуванні.

Прикладом проблемно-орієнтованого засобу розробки ПЗ для КСУ АЕС є Radiy Platform Configuration Tool, розроблений ПАТ НВП «Радій» – https://radiy.com/radics/).

Загальні вимоги стандарту **IEC 62138 щодо мов програмування для створення ПЗ категорій «B» та «C»** наступні:

– мови програмування повинні мати чітко визначену лексику та семантику;

– перевага має надаватися проблемно-орієнтованим мовам.

Для категорії «B» вводиться ряд додаткових вимог:

– статична типізація;

– передбачувана поведінка програми.

Наприклад, недоцільним є переривання роботи програми для процедури «збирання сміття»;

– використання мов низького рівня (наприклад, асемблерів) має бути обґрунтованим.

Вимоги до реалізації ПЗ. Основним етапом діяльності при створенні програмного забезпечення є реалізація. Детальні вимоги до реалізації відрізняються в залежності від класу функціональної безпеки ПЗ і розглядаються в межах відповідного стандарту.

Загальні **вимоги стандарту IEC 60880 до реалізації ПЗ категорії функціональної безпеки «А»** наступні:

– структура програми повинна бути простою та зрозумілою;

– програма має бути побудована на модульному принципі;

– програма повинна реалізовувати функції самоконтролю;

– не рекомендується використовувати складні прийоми, рекурсію, стиснення коду;

– вихідний код програми повинен бути зрозумілий для кваліфікованих програмістів, які не беруть участь в розробці;

– будь-які відхилення від вимог стандарту мають бути обґрунтовані.

Детальні рекомендації стандарту IEC 60880 до розробки ПЗ містяться в додатку В. Цей додаток можна вважати головним компонентом стандарту IEC 60880, що стосується розробки ПЗ категорії «А». В табл. 3 згруповані та наведені категорії рекомендацій, перелік їх сфер застосування та кількість рекомендацій в кожній сфері (N – кількість рекомендацій в кожній сфері в стандарті).

Таблиця 3 – **Категорії та сфери застосування рекомендацій стандарту IEC 60880 до ПЗ КСУ АЕС**

Категорія рекомендацій	Сфери застосування	N
Загальний процес проектування	Можливість модифікації ПЗ	4
	Підхід до розробки «згори-донизу»	11
	Верифікація проміжних результатів	6
	Модифікація в процесі розробки	6
Структура ПЗ	Загальна структура програми	7
	Модульність	7
	Вимоги до операційного ПЗ	10
	Час виконання програми	9
	Використання переривань	6
	Побудова арифметичних виразів	4
Самоконтроль	Перевірки достовірності	4
	Безпечна вихідна інформація	4
	Аналіз змісту пам’яті	4
	Перевірка наявності, обробка помилок	6
Детальне проектування і кодування	Розгалуження і цикли	8
	Підпрограми	6
	Вкладені структури	4
	Адресація і масиви	5
	Структури даних	6
	Динамічна зміна коду	1
	Тестування	7
Рекомендації, що залежать від мови програмування	Послідовність описів, оформлення коду	5
	Наявність, дотримання правил кодуваннч	4
	Використання коментарів	4
	Мова асемблера	8
	Проблемно-орієнтовані мови	4
	Автоматична генерація коду	4

Вимоги **стандарту IEC 62138 до розробки ПЗ категорій «В» та «С»** є менш суворими та приведені в формі загальних рекомендацій.

Для ПЗ, що реалізоване з використанням універсальних мов програмування, вимагається використання правил кодування. Набір правил може бути специфічним в залежності від мови програмування. Структура програми повинна бути ясною та зрозумілою. Рекомендується дотримання модульного принципу структури ПЗ, використання принципів інкапсуляції. Вимагається уникати використання небезпечних особливостей мови програмування, на якій створюється ПЗ.

При використанні проблемно-орієнтованих мов програмування, використання документально оформлених правил кодування вимагається для ПЗ категорії функціональної безпеки «В».

Під час реалізації ПЗ стандартом вимагається проведення документально оформленої верифікації. Верифікація має стосуватися як дотримання правил кодування (для ПЗ категорії «В»), так і відповідності поведінки програми специфікації вимог до ПЗ.

Висновок. Вимоги стандартів до розробки ПЗ значно відрізняються в залежності від категорії. Стандарт IEC 60880 зобов'язує дотримуватися правил кодування та наводить велику кількість детальних рекомендацій. Стандарт IEC 62138 містить загальні вимоги з дотримання правил кодування без їх зазначення.

Аналіз вимог до етапу верифікації, інтеграції та валідації

В підрозділі проводиться дослідження основних вимог стандартів IEC 60880 та IEC 62138, які стосуються етапів верифікації, інтеграції та валідації ПЗ.

Верифікація ПЗ. З метою забезпечення впевненості у відповідності ПЗ необхідним показникам якості вимагається проведення процедур верифікації вхідних та вихідних даних та результатів виконання кожного етапу ЖЦ ПЗ.

Виконання верифікації має виконуватися незалежною групою – особами, які не брали участі в його реалізації. Для верифікації ПЗ категорії функціональної безпеки «А» та «В» особи, що проводять верифікацію, мають бути адміністративно незалежні від розробників (мати різне керівництво, працювати в різних підрозділах чи організаціях). Спілкування між групою верифікації та розробників повинно відбуватися в письмовому вигляді з забезпеченням можливості перевірки.

Дії з верифікації мають відбуватися відповідно до плану верифікації. Цей план створюється верифікаційною групою. В ньому мають бути документально оформлені всі використовувані критерії, методи та інструменти, а також всі дії, які виконуються для оцінки кожного об’єкту.

Верифікації підлягають:

– специфікація вимог до ПЗ;

– специфікація ПЗ;

– план валідації ПЗ;

– реалізація (для ПЗ категорії функціональної безпеки «А»).

Верифікація специфікації вимог до програмного забезпечення має встановити впевненість у повноті формування вимог до ПЗ відповідно до загальних вимог системи.

Верифікація специфікації програмного забезпечення має стосуватися:

– аналізу відповідності до специфікації вимог;

– зрозумілості для розробників;

– можливості технічної реалізації;

– розбиття на функціональні модулі (для категорії «А»).

Для ПЗ категорії «А» додатково вимагається верифікація його реалізації.

Верифікація ПЗ категорії «А», що реалізоване з використанням універсальних мов програмування, складається з наступних кроків:

– аналіз та тестування вихідного коду. Аналіз може відбуватися з використанням автоматизованих інструментів;

– функціональне тестування модулів. Цей крок має підтвердити, що модуль виконує всі необхідні функції та не виконує непередбачених;

– інтеграційне тестування модулів. Цей крок має продемонструвати, що модулі вірно взаємодіють один з одним.

Верифікація реалізації ПЗ категорії «А», що реалізоване з використанням проблемно-орієнтованих мов, повинна відбуватися за допомогою візуальної перевірки або за допомогою автоматичних інструментальних засобів. Ці засоби повинні мати можливість змоделювати роботу програмного забезпечення в режимі відлагодження. Процес верифікації має підтвердити, що всі елементи ПЗ реалізовані вірно та виконують необхідні функції відповідно до специфікації вимог до ПЗ.

Також верифікації підлягає конфігурація раніше розробленого ПЗ, що атестоване та використовується в проекті. Верифікація може відбуватися методами візуальної перевірки, за допомогою використання інструментальних засобів, або шляхом комбінування методик.

Результати верифікації мають оформлюватися документально та аналізуватися розробниками з метою усунення виявлених невідповідностей.

Інтеграція ПЗ до КСУ. Етап інтеграції передбачає об'єднання верифікованих модулів апаратного забезпечення та ПЗ в єдину завершену систему. Він має відбуватися за попередньо розробленим планом. Процес інтеграції відбувається за наступними кроками:

– збирання та з'єднання модулів апаратного забезпечення у відповідності до проекту;

– збирання завершеного ПЗ з програмних модулів;

– завантаження ПЗ в технічні засоби, для яких воно розроблялося;

– перевірка відповідності ПЗ специфікації проекту;

– перевірка інтерфейсів між апаратним та програмним забезпеченням;

– перевірка функціонування ПЗ на конкретному апаратному забезпеченні.

Результати верифікації інтегрованої системи мають бути документально оформлені. У звіті мають бути вказаний перелік апаратного забезпечення та ПЗ, випробувального обладнання, параметри їх налаштувань, а також будь-які виявлені дефекти та невідповідності.

Валідація ПЗ. За результатами інтеграції системи вимагається проведення тестувань в її кінцевій конфігурації, включаючи кінцеву версію ПЗ. Перевірка має перевірятися за допомогою моделювання вхідних сигналів та даних, які існують під час експлуатації. Перевіркою має бути охоплені:

– всі функції, що реалізуються в ПЗ;

– всі діапазони сигналів та параметрів;

– логіка та алгоритми роботи;

– захист від помилок оператора та відмов інших систем.

За результатами валідації має бути створена документація, яка повинна включати в себе всі виявлені невідповідності та дефекти.

Висновки. Після завершення реалізації ПЗ розробниками мають відбутися етапи верифікації ПЗ, інтеграції ПЗ до КСУ та валідації ПЗ в складі КСУ. Мета цих етапів – перевірити якість розробленого ПЗ та відповідність його специфікації вимог. Будь-який етап може створити ітерацію в процесі розробки при виявлені дефекту. В цьому випадку інформація про винайдений дефект повинна бути передана розробникам ПЗ для аналізу та усунення, після чого має відбутися повторна перевірка.

Глибина верифікації та валідації залежить від категорії функціональної безпеки ПЗ. Наприклад, одна з основних особливостей верифікації ПЗ категорії «А» – необхідність верифікації його реалізації: архітектури та вихідного коду.

Аналіз вимог до етапу встановлення, експлуатації та модифікації

Встановлення та експлуатація. Після завершення етапів реалізації, інтеграції та валідації розпочинається етап встановлення КСУ та його експлуатації на АЕС. Стандарти IEC 60880 та IEC 62138 описують вимоги до встановлення, взаємодії між операторами та ПЗ КСУ, які стосуються установки, захищеності (для ПЗ категорії «А»), навчання операторів, а також дій у випадку виявлення аномалій.

Вимагається, щоб після встановлення ПЗ на місці експлуатації була передбачена процедура тестування його функціональності.

Важливою складовою забезпечення безпеки КСУ є дії оператора. Тому стандартами вимагається проведення навчання операторів АЕС та іншого персоналу з контролю та керування користуванню та обслуговуванню ПЗ в необхідних межах. План навчання має охоплювати як нормальні, так і аварійні умови експлуатації. Зокрема, оператор має вміти розпізнавати аномалії в роботі ПЗ. Для набуття оператором необхідних навичок навчальний план має включати як теоретичні знання, так і практичне оволодіння роботою з ПЗ на учбовій системі або тренажерах, які моделюють поведінку реального ПЗ та обладнання.

Якщо під час експлуатації ПЗ спостерігається відхилення його поведінки від очікуваної, вимагається складення протоколу про аномалію, що містить детальну інформацію про проведені дії та наслідки. Ці протоколи підлягають аналізу проектувальниками для модифікації ПЗ та усунення дефекту.

Стандарт IEC 60880 містить додаткові вимоги до захищеності ПЗ категорії «А» на місці експлуатації. Вони передбачають визначення заходів проти потенційних загроз виконанню функцій безпеки КСУ. Узагальнено ці вимоги можна звести до того, під час будь-яких дій з ПЗ має бути забезпечена функціональна безпека КСУ. Наприклад, такі дії як обслуговування, модифікація чи оновлення ПЗ можуть виконуватися при роботі АЕС на потужності. Через це повинні бути передбачені можливості блокування окремих функцій ПЗ, видачі аварійної сигналізації, заборона або використання окремих інтерфейсів під час обслуговування чи модифікації. Також дії, що впливають на захищеність, мають виконуватися оператором тільки з визначених місць (наприклад, не виконуватися з непередбачених робочих станцій з віддаленим керуванням).

Модифікація ПЗ. Протягом всього ЖЦ ПЗ може виникати необхідність модифікації ПЗ з причин зміни функціональних вимог, технічного забезпечення або виявлення аномалій під час тестування або експлуатації. Для виконання модифікації має бути розроблена документально оформлена процедура керування модифікацією.

В разі виявлення необхідності в модифікації ПЗ має бути створений запит на модифікацію. В ньому має вказуватися причина, область застосування та ініціатор запиту. Вимагається, щоб цей запит був проаналізований розробниками. Аналіз має включати в себе доцільність змін, можливий вплив на інші частини системи тощо.

В разі ухвалення рішення про проведення модифікації вона виконується з подальшим проведенням процедур верифікації та валідації всіх частин КСУ, на які має вплив. Якщо модифікація стосується ПЗ обладнання, що знаходиться в роботі, розробники та тестувальники програмного забезпечення мають мати доступ до аналогічної конфігурації обладнання для верифікації та валідації.

Всі документи, на які впливає модифікація, мають бути змінені та зареєстровані в архіві з управління модифікаціями проекту.

Висновки. Функціональна безпека КСУ забезпечується за умови вірного встановлення та кваліфікованої експлуатації її програмного забезпечення. Це можливо завдяки постійному контролю за станом ПЗ на місці експлуатації кваліфікованим персоналом. Персонал, що експлуатує КСУ, повинен мати зв’язок з представниками розробника для передачі інформації про виявлені аномалії в роботі та загальний досвід експлуатації системи.

Таблиця розподілення вимог до ПЗ

В результаті досліджень стандартів IEC 60880 та IEC 62138 до розробки ПЗ КСУ АЕС, важливих для безпеки, їх основні вимоги зведено до табл. 4.

Таблиця 4 – **Основні вимоги до розробки ПЗ КСУ АЕС**

Вимога	Категорія ПЗ		
	«А»	«В»	«С»
Керування розробкою			
Розподіл процесу розробки ПЗ на етапи та види діяльності	+	+	+
Документальне оформлення мети, зв’язків, вхідних та вихідних даних кожного етапу	+	+	+
Верифікація досягнення необхідної якості після виконання кожного етапу	+	+	+
Документування результатів виконання кожного етапу	+	+	+
План забезпечення якості			
Виконання всіх видів діяльності компетентними особами	+	+	+
Документальне визначення, оформлення та ідентифікація всіх інструментальних засобів та меж їх застосування	+	+	+
Чітке визначення специфічних термінів, скорочень та позначень	+	+	+
Необхідність відслідковування та вирішення всіх проблем забезпечення якості	+	+	+
Обґрунтування відхилень від умов та вимог стандартів	+	+	+
Звіт виконання кожного пункту плану забезпечення якості	+	-	-
Загальні вимоги до розробки ПЗ			
Розподілення ПЗ та конфігураційних даних на типи	+	+	+
Керування конфігурацією ПЗ	+	+	+
Захищеність ПЗ під час розробки	+	-	-
Реалізація допомогою універсальних мов	+	+	+
Реалізація допомогою проблемно-орієнтованих мов	+	+	+
Специфікація вимог до ПЗ			
Специфікація вимог має визначати, що робить програма, а не те, як вона це робить	+	+	+
Строгий опис вимог до ПЗ	+	-	-
Вимоги до захищеності ПЗ	+	-	-
Вимоги до самоконтролю ПЗ	+	+	-
Вимоги до періодичного тестування функцій ПЗ	+	-	-
Вимоги до захисту від відмови з спільної причини	+	+	+
Проектування та реалізація			
Модульний принцип, проектування «згори-вниз»	+	+	+
Код програми має бути простим і зрозумілим	+	-	-
Уникнення ускладнених прийомів кодування, рекурсії, «стиснення» коду	+	-	-
Код програми має відповідати документально оформленими правилам	+	+	-
Наявність повної документації зі створеного ПЗ	+	+	+
Інструментальні засоби			
Висока якість	+	+	+
Низький ризик внесення дефектів	+	+	+
Точна ідентифікація	+	+	-
Атестація та сертифікація	+	-	-

Вимога	Категорія ПЗ		
	«A»	«B»	«C»
Мови програмування та транслятори			
Чіткі правила семантики та синтаксису	+	-	-
Використання «безпечного», скороченого варіанту мови	+	-	-
Наявність перевіреного транслятора	+	-	-
Використання інструментального ПЗ для автоматизованої перевірки	+	-	-
Універсальні мови програмування			
Правила програмування, які легко верифікувати	+	+	-
Верифікація дотримання правил та стандартів кодування	+	+	-
Забезпечення чітко детермінованої поведінки ПЗ	+	+	-
Статична типізація	+	+	-
Написання вихідного коду з дотриманням вимог додатку «B» (стандарту IEC 60880)	+	-	-
Проблемно-орієнтовані мови програмування			
Методи формалізації мови є простими, зрозумілими, стандартного представлення, без небезпечних елементів.	+	-	-
Формат представлення, зрозумілий для технологів-спеціалістів	+	-	-
Проста структура програмного коду, що генерується	+	-	-
Раніше розроблене ПЗ			
Оцінка функціональної придатності	+	+	+
Оцінка якості	+	+	+
Оцінка досвіду експлуатації	+	+	+
Наявність виявлення та стійкість до відмов	+	+	-
Стійкість до помилок операторів	+	+	-
Наявність документації з системних вимог, інтерфейсів, безпеки, самоконтролю	+	+	-
Верифікація			
Верифікаційна група не містить осіб, що брали участь в реалізації ПЗ	+	+	+
Верифікаційна група адміністративно незалежна від групи розробників ПЗ	+	+	-
Верифікація специфікації вимог до ПЗ	+	+	+
Верифікація правил реалізації ПЗ	+	+	-
Верифікація конфігурації раніше розробленого ПЗ	+	+	-
Верифікація вихідного коду нового ПЗ	+	-	-
Інтеграція			
Верифікація процесу інтеграції	+	-	-
Наявність процедури виправлення дефектів	+	-	-
Валідація			
Використання статичного та динамічного моделювання всіх вхідних сигналів	+	-	-
Повне тестування всіх функцій	+	-	-
Тестування відповідності функцій, характеристик та інтерфейсу ПЗ кожному пункту специфікації	-	+	-
Тестування відповідності функцій, характеристик та інтерфейсу ПЗ кожному пункту специфікації, важливому для безпеки	-	-	+
Оцінка результатів валідації особами, які не брали участі в реалізації	+	+	+
Модифікація			
Наявність процедури запиту на модифікацію	+	-	-
Незалежна оцінка запитів на модифікацію	+	-	-
Для випробування використовується конфігурація, ідентична реальній системі	+	-	-
Верифікація та валідація після проведених модифікацій	+	+	+
Корекція документів, на які впливає документація	+	+	+
Реєстрація документів з модифікації в архіві	+	-	-
Встановлення та експлуатація			
Захищеність ПЗ на місці експлуатації	-	-	-
Навчання операторів	-	-	-
Наявність процедури створення звіту про аномалію	+	+	+

Засоби імплементації вимог

Стандарти розробки ПЗ КСУ АЕС, важливих для безпеки – IEC 60880 та IEC 62138 – містять вимоги до всіх етапів ЖЦ ПЗ. Як вже зазначалося, дотримання вимог цих стандартів дозволяє створити ПЗ високого степеню надійності.

Для дотримання вимог стандартів під час розробки необхідно дотримуватися певних правил. Спираючись на дослідження цих вимог, а також на досвід автора під час розробки ПЗ КСУ АЕС науково-виробничим підприємством «Радій» (м. Кропивницький, Україна), можна сформувати основні правила, методики та заходи, які забезпечують створення ПЗ високої якості.

На етапі створення специфікації вимог до ПЗ важливі наступні фактори:

– отримання від замовника повної та всеосяжної специфікації вимог до КСУ;

– чітке визначення всіх функцій майбутнього продукту;

– детальний опис всіх вимог в специфікації апаратних засобів;

– детальний опис всіх вимог до ПЗ;

– чітке планування етапів розробки у відповідності до технологій, що використовуються;

– постійний зв’язок з представниками замовника для уточнення можливих запитань.

На етапі проектування та реалізації ПЗ важливі наступні фактори:

– наявність розробників-програмістів високої кваліфікації;

– наявність достатніх технічних засобів;

– обґрунтований та свідомий вибір мов програмування та інструментальних засобів;

– використання найкращих практик програмування: актуальних стандартів кодування, дотримання coding-guides для обраних мов, застосування безпечних прийомів програмування;

– постійне тестування коду;

– використання «гнучких» технологій програмування та взаємодії в команді, наприклад технології SCRUM [8];

– використання підходу CI/CD (Continuous Integration/Continuous Deployment);

– чітка ідентифікація версій ПЗ та документації до нього.

На етапі верифікації та валідації важливі наступні чинники:

– детальне вивчення специфікації вимог до КСУ та ПЗ;

– повнота тестувань;

– підтримка постійного зв'язку з розробниками;

– формування якісної документації за результатами перевірок.

На етапі впровадження та експлуатації важливі наступні чинники:

– якісне виконання монтажу системи та встановлення ПЗ;

– контроль за версіями та конфігурацією встановленого ПЗ;

– надання персоналу АЕС повної документації на всі компоненти КСУ;

– якісне навчання персоналу для роботи з КСУ;

– дотримання постійного зв'язку між персоналом АЕС та розробниками КСУ для збору інформації про досвід експлуатації, проблеми та запитання що виникають, а також оперативної обробки запитів на модифікацію.

Висновок. Як приклад, дотримання вимог стандартів розробки дозволило науково-виробничому підприємству «Радій», провідним інженером-програмістом якого є автор, розробити та поставити велику кількість КСУ на АЕС України, Болгарії, Канади, Аргентини та інших країн станом на 2023 рік. Ці КСУ успішно експлуатуються протягом багатьох років.

Проблема оцінки відповідності стандарту

Після розробки ПЗ КСУ АЕС відповідно до вимог стандартів IEC 60880 та IEC 62138 виникає необхідність оцінки відповідності процесу розробки та самого ПЗ цим стандартам. Оцінюванню може підлягати як будь-який окремий етап ЖЦ ПЗ, так і весь процес в цілому.

Згідно дослідження змісту стандартів, їх вимоги можна розподілити на «адміністративні» та «технічні». «Адміністративні» вимоги стосуються організації робочого процесу, змісту різноманітних документів, взаємодії між групами розробників тощо і стосуються переважно етапів створення специфікації вимог, верифікації, валідації, інтеграції та супроводу. «Технічні» вимоги стосуються етапів реалізації: вибору мови програмування, створення проекту та реалізації ПЗ конкретними мовами програмування, тобто переважно етапу проектування та реалізації ПЗ.

Оцінку відповідності «адміністративним» вимогам стандартів можна провести, вивчаючи якість виконання кожної вимоги.

Для цього потрібно проводити аналіз як самого робочого процесу, так і зміст документів за результатами відповідних етапів. Наприклад, в специфікації вимог до ПЗ мають бути вказані прикладні функції, що виконуються ПЗ, і наявність цього можна перевірити.

Оцінку відповідності «технічним» вимогам, зокрема правильності вибору мови програмування та реалізації ПЗ, можна виконати шляхом аналізу вихідного коду програми та його функціональному тестуванню. При цьому відповідність ПЗ вимогам специфікації можна перевірити, послідовно перевіряючи всі наявні функції ПЗ, а відповідність коду програми правилам кодування можна оцінити, тільки детально аналізуючи код програми. Для проведення аналізу коду програми (нагадаємо, це стосується ПЗ категорії «А») кваліфікація фахівця, який виконує перевірку, в конкретній мові програмування має бути співставною з кваліфікацією програмістів, що реалізували ПЗ.

Як **висновок**, можна відмітити, що в стандартах розробки ПЗ КСУ АЕС не наводиться конкретних методик оцінки та метрик відповідності ПЗ цим стандартам. Виходячи з цього, оцінка відповідності ПЗ вимогам стандартів включає суб'єктивну складову і залежить від методів перевірки, що використовуються в конкретній організації.

Висновки

Міжнародні стандарти IEC 60880 та IEC 62138 містять важливі вимоги до всіх етапів розробки ПЗ КСУ АЕС, важливого для безпеки. Вимоги стосуються як організаційних питань, так і технічних аспектів. Згідно з цими стандартами, кожне підприємство, що займається розробкою ПЗ КСУ АЕС, має визначити робочі групи, які будуть реалізовувати різні етапи ЖЦ (проектування, реалізація, верифікація тощо).

Інтерфейси користувача. Стандарти не містять вимог до інтерфейсів користувача ПЗ. Тому одним з напрямків наступних досліджень стануть вимоги інших міжнародних стандартів – IEC 61772 «Nuclear power plants – Control rooms – Application of visual display units (VDUs)» («Візуальні пристрої відображення») [9] та IEC 62646 «Nuclear power plants – Control rooms – Computer-based procedures» («Комп'ютеризовані процедури») [10], а також вимоги галузевих нормативних документів, таких як NUREG-0700 «Human-System Interface Design Review Guidelines» – «Побудова інтерфейсів «людина-машина» (U.S. Nuclear Regulatory Commission, США) [11].

Оцінка відповідності ПЗ стандартам. В стандартах не визначається загальноприйнятих метрик, що вказують ступінь відповідності ПЗ даним стандартам. Виходячи з цього, кожна організація, яка виконує оцінку відповідності ПЗ та КСУ в цілому вимогам стандартів, повинна створити власну методику такої оцінки.

Тому метою наступних досліджень є вивчення засобів оцінки специфікацій вимог, метрик коду ПЗ, критеріїв повноти тестування ПЗ, які можуть бути використані для розробки формальних методик оцінювання ПЗ вимогам стандартів.

СПИСОК ЛІТЕРАТУРИ

1. Nuclear power by country. [Електронний ресурс] – Режим доступу: https://en.wikipedia.org/wiki/Nuclear_power_by_country.
2. IEC61508-2010: Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements. Geneva, International Electrotechnical Commission (IEC), 2010.
3. IEC61513-2011: Nuclear power plants – Instrumentation and control important to safety – General requirements for systems requirements. Geneva, International Electrotechnical Commission (IEC), 2011.
4. IEC61226-2009: Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions. Geneva, International Electrotechnical Commission (IEC), 2009.
5. Safety Classification of Structures, Systems and Components in Nuclear Power Plants: Specific Safety Guide No. SSG-30. Vienna, IAEA, 2014.
6. IEC60880-2006: Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions. Geneva, International Electrotechnical Commission (IEC), 2006.
7. IEC62138-2004: Nuclear power plants – Instrumentation and control important for safety – Software aspects for computer-based systems performing category B or C functions. Geneva, International Electrotechnical Commission (IEC), 2004.
8. Tor Stålhane, Vikash Katta, Thor Myklebust. Scrum and IEC 60880. Norwegian University of Science and Technology, 2013.
9. IEC61772:2009: Nuclear power plants — Control rooms — Application of visual display units (VDUs). Geneva, International Electrotechnical Commission (IEC), 2009.
10. IEC62646-2019: Nuclear power plants – Control rooms – Computer based procedures. Geneva, International Electrotechnical Commission (IEC), 2012.
11. NUREG-0700 Revision 3. Human-System Interface Design Review Guidelines. U.S. Nuclear Regulatory Commission, 2020.
12. Вінтенко Б.Ю., Смірнов О.А., Коваленко О.В., Смірнов С.А., Коваленко А.С. «Дослідження нормативних документів та галузевих стандартів розробки програмного забезпечення комп'ютерних систем управління АЕС, важливих для безпеки». *Системи управління, навігації та зв'язку*, 2023, вип. 2(72), С. 161-180.

Received (Надійшла) 30.05.2023
Accepted for publication (Прийнята до друку) 02.08.2023

Study of the requirements of international standards IEC60880 and IEC62138 for the development of software for information and control systems of NPPs important for safety

Boris Vintenko, Oleksii Smirnov, Anna Kovalenko, Serhii Smirnov, Kostiantyn Buravchenko

Abstract. Today, a significant part of electrical energy is produced by nuclear power plants. Atomic energy is a cheap, economically beneficial and ecological way of meeting people's needs with electricity. At the same time, this production is connected with the need to ensure the protection of people and the environment from ionizing radiation of nuclear fuel during normal operation of the plant and in case of emergency situations. Nuclear power plants (NPP) contain a large amount of equipment to ensure technological processes and perform safety functions. **The purpose** of the work is to study the requirements for the formation of the life cycle, the main stages of design and documentation of the software of the computer control systems of nuclear power plants (software CCS NPP), which perform safety functions of categories "A", "B" and "C". Requirements for software performing category A functions are given in the international standard IEC 60880 "Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions", software requirements , performing category "B" and "C" safety functions, specified in the international standard IEC 62138 "Nuclear power plants – Instrumentation and control important for safety – Software aspects for computer-based systems performing category B or C functions". **The object of research** is the process of developing software for computer control systems of nuclear power plants. **The subject is a study** of the requirements of international standards IEC 60880 and IEC 62138 for the development of software for information and control systems of NPPs, important for safety. **As a result of the study**, the general structure of the requirements of the IEC 60880 and IEC 62138 standards was considered, the groups of participants who participate in the development of the software of the NPP CCS and the distribution of software development activities among these groups were determined, the analysis of the requirements of the general requirements and the requirements for the stage was carried out development of the software specification, requirements for the stage of design and implementation of software, requirements for the stage of verification, integration and validation and requirements for the stage of installation, operation and modification, a table of distribution of requirements for software was formed, means of implementation of requirements were studied, the problem of assessment of compliance with the standard was determined. **Conclusions**. The international standards IEC 60880 and IEC 62138 contain important requirements for all stages of the development of the safety-critical NPP control system software. The requirements concern both organizational issues and technical aspects. According to these standards, each enterprise engaged in the development of NPP CCS software must define working groups that will implement various stages of the NPP (design, implementation, verification, etc.). The standards do not contain requirements for software user interfaces. Therefore, one of the directions of further research will be the requirements of other international standards – IEC 61772 "Nuclear power plants – Control rooms – Application of visual display units (VDUs)" ("Visual display units") and IEC 62646 "Nuclear power plants – Control rooms – Computer -based procedures" ("Computerized procedures"), as well as the requirements of industry regulatory documents, such as NUREG-0700 "Human-System Interface Design Review Guidelines" – "Construction of human-machine interfaces" (U.S. Nuclear Regulatory Commission, USA). The standards do not define generally accepted metrics that indicate the degree of compliance of the software with these standards. Based on this, each organization that performs an assessment of the compliance of software and CSU as a whole with the requirements of the standards must create its own methodology for such an assessment. Therefore, the goal of the following research is to study the means of evaluating requirements specifications, software code metrics, completeness criteria of software testing, which can be used for the development of formal software evaluation methods for the requirements of standards.

Keywords: software, computer control systems, nuclear power plants, IEC 60880, IEC 62138.