СУЧАСНІ ВИМОГИ З БЕЗПЕКИ ФУНКЦІОНУВАННЯ СИСТЕМ УПРАВЛІННЯ МАШИНАМИ ТА МЕХАНІЗМАМИ

Левченко О. Г., д.т.н., проф., зав. каф. ОППЦБ КПІ ім. Ігоря Сікорського;
Каштанов С. Ф., к.т.н., доц. (каф. ОППЦБ КПІ ім. Ігоря Сікорського)

Анотація. Проаналізовано сучасні вимоги безпеки щодо проектування, розробки та функціонування систем управління машинами й механізмами. Визначено основні показники безпеки цих систем та надано відповідні рекомендації щодо їх реалізації.

Ключові слова: безпека, системи управління, машини та механізми.

Abstract. Modern safety requirements for the design, development and operation of control systems for machines and mechanisms are analyzed. The main safety indicators of these systems are determined. Relevant recommendations for their implementation are provided.

Keywords: safety, control systems, machines and mechanisms.

Вступ. Відповідно до існуючих вимог у сфері безпеки промислового обладнання, будь які системи управління машин та механізмів, у залежності від умов їх експлуатації, повинні гарантувати виконання необхідних функцій безпеки та контролю з метою забезпечення прийнятних рівнів ризиків щодо можливості негативного впливу на обслуговуючий персонал небезпечних та шкідливих виробничих факторів.

Аналіз стану питання. Процес розробки, проектування та експлуатації будь якого промислового обладнання передбачає обов'язкове виконання вимог Directive 2006/42/EC і діючих у цій сфері технічних регламентів та стандартів EN ISO 12100-1/2, ISO 14121, EN 954-1 (ДСТУ EN 954-1: 2003), EN ISO 13849-1 (ДСТУ EN ISO 13849-1- 2016) та IEC 62061 [1-6].

Необхідно зазначити, що застосування будь-яких захисних заходів, які використовуються для усунення існуючих небезпек та зниження рівнів можливих ризиків, повинно здійснюватися в певній послідовності у відповідності до вимог EN ISO 12100-1: 1 етап – запобігання небезпекам; 2 етап – захист від небезпек (безпечні небезпеки); 3 етап – визначення (виявлення) інших можливих джерел небезпек.

Ті частини систем управління машиною, які вирішують завдання безпеки, визначені в міжнародних стандартах, як "частини, що пов'язані з безпекою в системах управління" - "safety-related parts of control systems" (SRP/CS). Відповідно до вимог обох стандартів (ISO 13849-1 та IEC 62061) необхідні функції безпеки повинні бути забезпечені саме за рахунок SRP/CS.

Мета роботи: визначення основних особливостей застосування при проектуванні, розробці та експлуатації пов’язаних з безпекою систем управління (ПБСУ) машин та механізмів сучасних вимог безпеки з урахуванням вимог стандартів ISO 13849-1 та IEC 62061.

Методики, матеріали і результати досліджень. Для визначення

показників безпеки ПБСУ машин та механізмів у стандарті EN ISO 13849-1 використовується ймовірнісний підхід, що дозволяє реалізувати кількісний розгляд показників безпеки. Для того, щоб класифікувати рівні безпеки систем управління обладнанням використовується п'ять значень рівнів безпеки (РБ) – це рівні PL (a, b, c, d, e,), які залежать від здатності елементів систем управління, пов'язаних із забезпеченням безпеки, виконувати функції безпеки в передбачених обставинах і характеризуються відповідними значеннями середнього часу напрацювання до виникнення небезпечної відмови ($MTTF_d$) або ймовірністю небезпечної відмови за годину (PFH_d).

Рівень функціональної безпеки систем управління машинами та механізмами згідно IEC 62061 визначається трьома рівнями повноти безпеки (РПБ) SIL – «Safety Integrity» (1, 2, 3). РПБ встановлюють вимоги до повноти безпеки електричних, електронних і програмованих електронних систем управління, що пов'язані з безпекою (ПБЕСУ), а також вимоги щодо їх здатності виконувати функції безпеки в передбачених обставинах, і ці дискретні рівні, як показано на рис. 1, характеризуються відповідними значеннями ймовірності небезпечної відмови за годину (PFH_d).

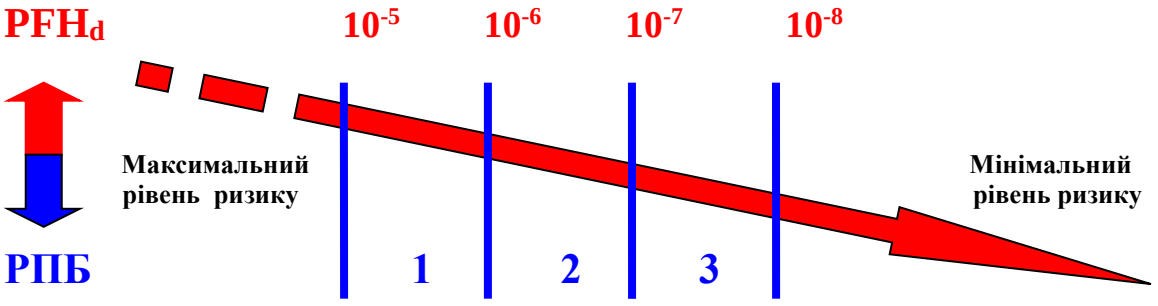

Рис.1. Взаємозв’язок ймовірності небезпечної відмови за годину (PFH_d) та рівня повноти безпеки (РПБ)

Зв'язок стандарту IEC 62061, який регламентує вимоги до функціональної безпеки електричних, електронних та програмованих електронних систем управління, з іншими відповідними стандартами та вся необхідна інформація щодо рекомендованого застосування цього стандарту та ISO 13849 при проведені оцінки ризику та проектуванні систем управління обладнанням [7-9] представлено на рис. 2.

Для будь якої ПБЕСУ повинні бути визначенні наступні показники (параметри): за стандартом EN ISO 13849 це: **Structure/category**; **$MTTF_d$** ; **$B10_d$** ; **n_{op}**; **CCF**; **DC_{avg}**; **PL**; **$T10_d$**, а за стандартом IEC 62061 це: **Structure/subsystem (SS) architecture**; **PFH_d**; **B10**; **λ_d/λ**; **C**; **β**; **DC**; **SIL**.

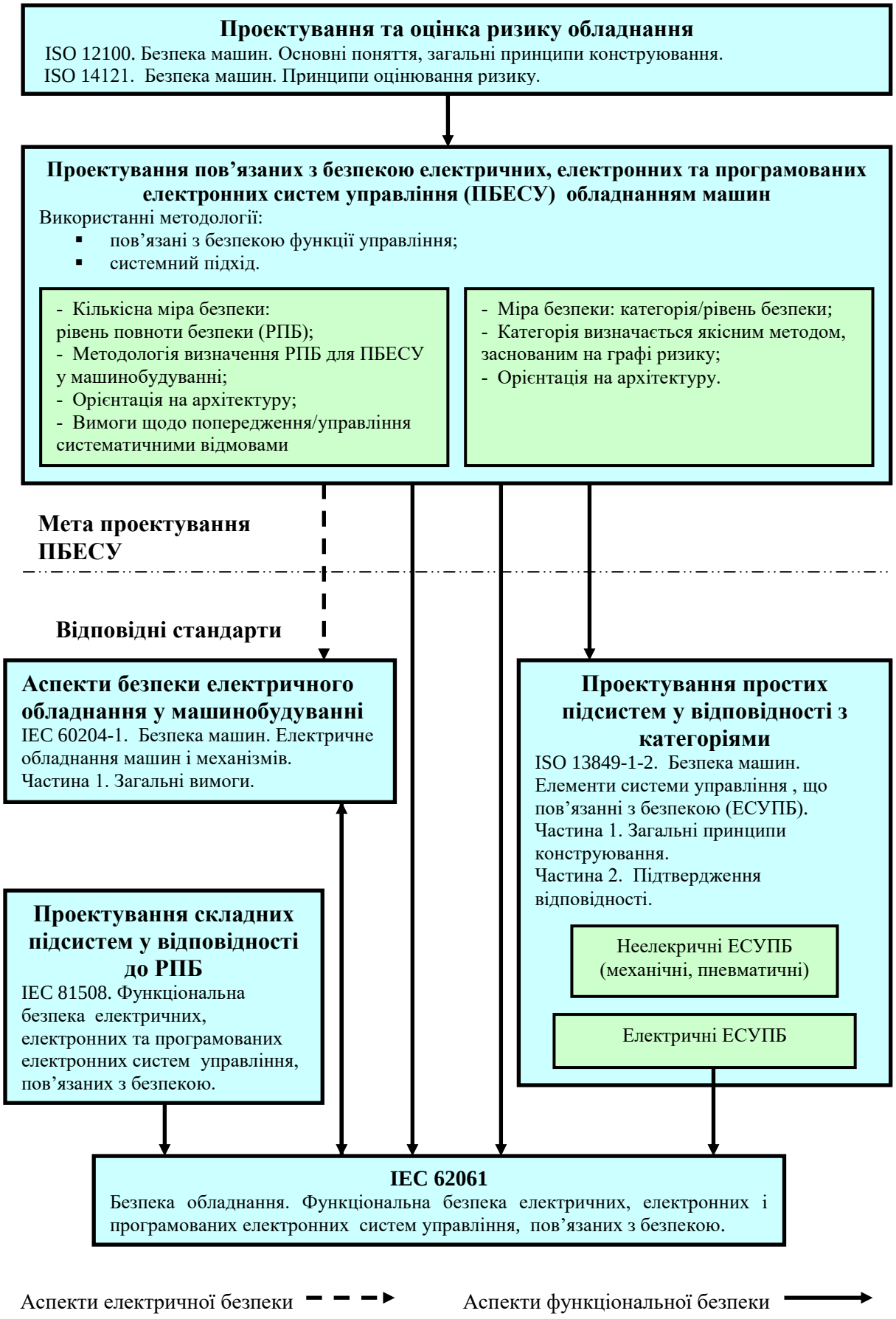

Рис. 2. Проектування та оцінка ризику обладнання

Застосування обох стандартів як EN ISO 13849-1, так і IEC 62061 передбачає виконання відповідних важливих вимог щодо забезпечення безпеки в залежності від технології, що використовується для реалізації пов'язаних з безпекою функцій управління обладнанням (таблиця 1).

Таблиця 1

Сфери застосування стандартів ISO 62061 и IEC 13849-1

Варіант	**Технологія реалізації зв'язаної (их) з безпекою функції (ій) управління**	**ISO 13849-1**	**IEC 62061**
A	Неелектрична, наприклад, гідравліка	«X»	Не охоплює
B	Електромеханічна, наприклад, реле або нескладні електронні пристрої	Обмежено встановленими архітектурами (див. Примітка 1) і до УБ = PLe	Усі архітектури і до УПБ = SIL 3
C	Складні електронні пристрої, наприклад, програмовані	Обмежено встановленими архітектурами (див. Примітка 1) і до УБ = PLd	Усі архітектури і до УПБ = SIL 3
D	A в поєднанні із B	Обмежено встановленими архітектурами (див. Примітка 1) і до УБ = PLe	«X» (див. Примітка 3)
E	C в поєднанні із B	Обмежено встановленими архітектурами (див. Примітка 1) і до УБ = PLd	Усі архітектури і до УПБ = SIL 3
F	C в поєднанні із A Або C в поєднанні із A і B	«X» (див. Примітка 2)	«X» (див. Примітка 3)

Позначка «X» - означає, що дану технологію регламентує стандарт, зазначений в заголовку колонки таблиці.

**Примітки:*

1. *Встановлені архітектури визначені в EN ISO 13849-1, додаток B, де наданий спрощений підхід для квантифікації рівня безпеки (УБ) PL. УБ - рівень необхідного мінімального зниження ризику.*
2. *Для складних електронних пристроїв використовують встановлені архітектури до УБ = PLd згідно EN ISO 13849-1 або будь-які архітектури згідно IEC 62061.*

Елементи, що засновані на неелектричній технології, відповідно до EN ISO 13849-1 використовують в якості підсистем.

Згідно вимог EN ISO 13849-1 структури (архітектури) елементів системи управління, що пов'язані з безпекою, визначаються в залежності від вибраної категорії.

• Категорія B – базова категорія

Елементи системи управління, що пов'язані з безпекою, повинні бути, як мінімум, розроблені та сконструйовані відповідно до сучасного рівня техніки і повинні протистояти очікуваним зовнішнім впливам.

• Категорія 1

Елементи системи управління, що пов'язані з безпекою, повинні бути розроблені і сконструйовані з використанням перевірених компонентів і надійних принципів безпеки.

• Категорія 2

Функції елементів системи управління, які пов'язані з безпекою, повинні періодично контролюватися (тестування, діагностика) з відповідними часовими інтервалами. Як правило, тестування (діагностика) здійснюється періодично під час роботи з урахуванням аналізу існуючих ризиків. Тестування (діагностика)

може здійснюватися автоматично або вручну, але обов'язково при кожному запуску і, бажано, перед виникненням можливої небезпечної ситуації.

• Категорія 3

Одна відмова на елементах системи управління, що пов'язана з безпекою, не призводить до втрати функції безпеки всієї системи. В той же час, оскільки в системі управління не використовується функція самоконтролю і тому не всі несправності можуть бути виявлені, то накопичення таких невиявлених несправностей все ж таки може з часом викликати небезпечну ситуацію.

Згідно із стандартом IEC 62061 структури (архітектури) систем управління, що пов'язані з безпекою, визначаються базовими архітектурами підсистем, що входять до складу ПБЕСУ і можуть мати наступні типи: A, B, C і D.

Тип А - стійкість до відмов дорівнює нулю, без функції діагностики.

У даній архітектурі будь-яка небезпечна відмова елемента підсистеми викликає відмову ПБФУ.

Тип В - стійкість до відмов дорівнює одиниці, без функції діагностики.

У даній архітектурі одиночна небезпечна відмова елемента підсистеми не викликає відмови ПБФУ. Таким чином, повинна відбутися небезпечна відмова більш ніж одного елемента перш, ніж може відбутися відмова ПБФУ.

Тип С - стійкість до відмов дорівнює нулю, з функцією діагностики.

У даній архітектурі будь-який не виявлений небезпечний збій елемента підсистеми призводить до небезпечного відмови ПБФУ. Якщо виявлено збій елемента підсистеми, то діагностична (і) функція (ї) ініціює (ють) функцію реакції на збій.

Тип D - стійкість до відмов дорівнює одиниці, з функцією діагностики.

У даній архітектурі одиночна відмова будь-якого елемента підсистеми не викликає відмови ПБФУ.

Що стосується проектування структури ПБЕСУ, то кожна ПБФУ, як зазначено в специфікації вимог до безпеки ПБЕСУ, повинна бути структурно декомпозована до рівня функціональних блоків.

Обов’язково необхідно, щоб така структура була документально оформлена і включала:

- її опис;
- вимоги до безпеки (як функціональні вимоги, так і вимоги до повноти безпеки) для кожного функціонального блоку;
- визначення входів і виходів кожного блоку.

РПБ, який досягається ПБЕСУ у відповідності з архітектурними обмеженнями, повинен бути менше або дорівнювати найменшому значенню граничної вимоги до РПБ будь-якої з підсистем, що беруть участь у виконанні ПБФУ.

Таким чином, показники безпеки підсистеми характеризуються граничними вимогами до РПБ, що визначаються її архітектурними обмеженнями, граничною вимогою до РПБ для систематичної повноти безпеки і ймовірністю випадкових небезпечних відмов апаратних засобів.

Найбільш високий рівень повноти безпеки апаратних засобів, який може знадобитися для виконання функції безпеки, обмежується стійкістю до відмов апаратних засобів і часткою безпечних відмов підсистем, які виконують цю пов'язану з безпекою функцію управління.

Найбільший рівень повноти безпеки, який може знадобитися для ПБФУ, яку реалізує підсистема з урахуванням стійкості до відмов апаратних засобів і частки безпечних відмов цієї підсистеми, визначається за допомогою таблиці 2.

Обмеження архітектури, наведені у таблиці 2, повинні застосовуватися в кожній підсистемі відповідно до наступних вимог:

- стійкість до відмов апаратних засобів N означає, що відмова N + 1 може привести до втрати ПБФУ (при визначенні стійкості до відмов не повинні враховуватися засоби, які могли б керувати впливом помилок, наприклад, засоби діагностики);
- якщо одна помилка безпосередньо призводить до однієї або більше наступних помилок, то її розглядають як одиничну помилку;
- у визначенні стійкості до відмов апаратних засобів деякі помилки можуть бути виключені за умови, що імовірність їх виникнення дуже мала по відношенню до вимог повноти безпеки підсистеми (будь-які винятки помилок повинні бути обгрунтовані і документально оформлені).

Таблиця 2

Архітектурні обмеження підсистеми. Максимальне значення РПБ, яке може бути досягнуто цією підсистемою

Частка безпечних відмов	**Відмовостійкість апаратних засобів**		
	N=0	*N*=1	*N*=2
< 60 %	Не обмовляється	РПБ 1	РПБ 2
60 % - 90 %	РПБ 1	РПБ 2	РПБ 3
90 % – 99 %	РПБ 2	РПБ 3	РПБ 3
≥ 99 %	РПБ 3	РПБ 3	РПБ 3
** Примітки:* *1. Відмовостійкість апаратних засобів N означає, що N + 1 відмова призведе до втрати пов'язаної з безпекою функції управління.* *2. Вийняток: для підсистеми зі стійкістю до збоїв апаратних засобів, що дорівнює нулю, в якій виключення збою може привести до небезпечної відмови, граничне вимога до РПБ через обмеження щодо архітектури такої підсистеми обмежена максимальним значенням РПБ 2.*			

Якщо підсистема відноситься до простих підсистем і розроблена відповідно до ISO 13849-1, а її підтвердження відповідності виконано згідно з ISO 13849-2, то в контексті архітектурних обмежень можуть бути застосовані тільки співвідношення обрані відповідно до таблиці 3.

Таблиця 3

Архітектурні обмеження простих підсистем. Зв'язок категорій з граничними вимогами за РПБ.

Категорія	**Стійкість до відмов апаратних засобів**	**Частка безпечних відмов (ЧБВ)**	**Максимальне значення граничної вимоги до РПБ, що відповідає обмеженням архітектури**
	Передбачається, що підсистеми з вказаною категорією мають характеристики, наведені нижче		
1	0	< 60 %	див. Примітку 1
2	0	60 % - 90 %	РПБ 1
3	1	< 60 %	РПБ 1
	1	60 % - 90 %	РПБ 2
4	>1	60 % - 90 %	РПБ 3 (див. Примітку 3)
	1	>90 %	РПБ 3 (див. Примітку 4)

* Примітки:

1. Вважається, що підсистеми категорій 1 і 2, у яких ЧБВ <60%, не задовольняють вимогам ISO 13849-1, тому підсистеми, розроблені відповідно до ISO 13849-1, на практиці будуть досягати значень ЧБВ більше 60%.

2. Передбачається, що для підсистем категорії 2 значення ЧБВ > 90% не буде досягнуто застосуванням вимог до її розробки, представлених в ISO 13849-1.

3.. Передбачається, що для підсистем категорії 4 охоплення діагностики буде <90%, якщо стійкість до відмов апаратних засобів (накопиченим відмовам) більше одиниці.

4. Підсистема категорії 4 вимагає значення ЧБВ більше 90%, якщо стійкість до відмов апаратних засобів такої підсистеми дорівнює одиниці.

5. Вважається, що підсистема категорії В, яка задовольняє вимогам ISO 13849-1, не досягає РПБ 1.

Обмеження архітектури згідно з таблицею 3 повинні застосовуватися до кожної підсистемі, що реалізує функціональний блок ПБФУ.

Для визначення граничних вимог до РПБ з урахуванням архітектурних обмежень, де це необхідно, повинна бути виконана оцінка ЧБВ.

При оцінці ЧБВ для кожної підсистеми повинен бути проведений аналіз (наприклад, аналіз дерева відмов, видів і наслідків відмов), щоб визначити всі відповідні відмови і їх види. Чи є відмова безпечною або небезпечною, залежить від ПБЕСУ і виконуваних ПБФУ, включаючи функцію реакції на відмову.

Ймовірність кожного виду відмови повинна бути визначена на підставі ймовірності виникнення пов'язаного (их) з нею збою (їв) з урахуванням заданого застосування підсистеми і може бути отримано з таких джерел, як:

- надійні дані про інтенсивність відмов, що зібрані з урахуванням практичного досвіду виробника і пов'язані з заданим застосуванням;
- дані про відмову компонента з визнаних галузевих джерел і пов'язані з заданим застосуванням;

• дані про інтенсивність відмов, що отримані за результатами тестування і аналізу.

Висновки. Результати проведеного в даній роботі аналізу свідчать, що ретельне виконання вимог діючих стандартів EN ISO 12100-1/2, ISO 13849-1 та IEC 62061 щодо врахування можливих ризиків та небезпек і дотримання приведених у них вимог безпеки при проектуванні, розробленні та функціонуванні систем управління машинами та механізмами дає можливість гарантовано забезпечити мінімально можливі рівні ризиків щодо отримання виробничих травм та професійних захворювань обслуговуючим персоналом та максимально високі показники безпеки експлуатації спроектованих машин та механізмів при їх експлуатації.

Література

1. Machinery Directive: Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006. / Official Journal of the European Union — 09.06.2006. – L157. – pp. 24-86.
2. Постанова КМ України від 30 січня 2013 р. № 62 про затвердження Технічного регламенту безпеки машин (із змінами, внесеними згідно з Постановою КМ № 632 віл 28.08. 2013 року).
3. EN ISO 12100-1/2 «Safety of machinery General principles for design and risk evaluation. Basic concepts».
4. EN 954-1 «Safety of machinery SRP/CS. General principles for design».
5. EN ISO 13849-1/-2 «Safety of machinery - Safety-related parts of control systems».
6. IEC 62061 «Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems».
7. Каштанов С.Ф., Полукаров Ю.О., Митюк Л.О. // Сучасні вимоги з безпеки при проектуванні електричних та електронних систем управління / журнал «Вісник КрНУ імені Михайла Остроградського». – Випуск № 6 (119). – 2019. – С. 161-165.
8. Левченко О. Г., Каштанов С. Ф. Современные требования безопасности к системам управления машин и механизмов (Часть 1) // Сварщик. – 2020. – № 1. – С.28-33.
9. Левченко О. Г., Каштанов С. Ф. Современные требования безопасности к системам управления машин и механизмов (Часть 2) // Сварщик. – 2020. – № 2. – С.28-31.