УДК 004.94:351
DOI 10.17721/ISTS.2023.1.37-42

Сергій Толюпа, orcid.org/0000-0002-1919-9174,
tolupa@i.ua
Лада Сліпачук, orcid.org/0000-0001-9855-0729,
lada.knu@gmail.com
Київський національний університет імені Тараса Шевченка, Київ, Україна

ФОРМУВАННЯ СИСТЕМИ КІБЕРЗАХИСТУ ДЛЯ ІНТЕГРОВАНОЇ ГАЛУЗЕВОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ УКРАЇНИ СЕКТОРУ НАЦІОНАЛЬНОЇ КІБЕРБЕЗПЕКИ

Розкрито та висвітлено передбачений склад, структуру заходів і засобів, які увійдуть до комплексної системи захисту інтегрованої галузевої інформаційної системи України (ІГІСУ) сектору національної кібербезпеки. Описано специфіку і стратегічну цінність залучених ресурсів, якими оперуватиме створена система кіберзахисту. Зазначено, що система кіберзахисту ІГІСУ передбачає задіяти комплекс взаємопов'язаних засобів і заходів, виконання яких необхідне й достатнє для повноцінного захисту ІГІСУ, для протистояння зовнішнім несанкціонованим системам доступу (НСД) тощо. Акцентовано увагу на відповідності передбаченої системи кіберзахисту міжнародним критеріям і стандартам захисту подібних керівних систем для країн НАТО, зокрема і кібербезпековому стандарту міністерства оборони США (TCSEC – "Помаранчева книга"); міжнародним критеріям і стандартам захисту подібних керівних систем інших провідних країн світу, зокрема, міжнародному технічному стандарту ISO/IEC 15408 "Загальні критерії оцінювання безпеки ІТ", який ратифікувало багато країн; настановам і рекомендаціям міжнародної організації NCSS (National Cyber Security Strategies) для країн – партнерів НАТО, що передбачені Стратегією національної кібербезпеки та розроблені міжнародними експертами з питань національної кібербезпеки, науковцями та європейськими радниками з міжнародної кібербезпеки в контексті проєкту Програма НАТО SPS "Наука заради миру та безпеки"; національним технічним стандартам України. У межах цієї статті детально показано повний асортимент загальнообов'язкових ресурсів та інструментів, які передбачені для забезпечення кібербезпеки спроєктованої ІГІСУ сектору національної кібербезпеки, та які включають п'ять рівнів кіберзахисту (організаційний, програмний, апаратно-технічний, інженерно-технічний, додатковий фізичний).

Ключові слова: *система кіберзахисту ІГІСУ сектору національної кібербезпеки; особливість системи кіберзахисту; складові системи кіберзахисту; відповідність системи кіберзахисту.*

1. ВСТУП

Сучасний рівень розвитку технологічного прогресу вимагає від кожної держави, аби автоматизовані керівні системи були дієвими, максимально захищеними та відповідали не лише глобальним викликам, потенційним зовнішнім ризикам цифрового світу та сучасному рівню розвитку ІТ як предметної області, але й задовольняли нагальні потреби сектора національної кібербезпеки як проблемної галузі.

Адже нині сектор національної кібербезпеки являє собою стратегічно важливу для держави макрогалузь, проблематика якої полягає у тому, що назріла нагальна потреба держави у забезпеченні високого рівня керованості сектором національної кібербезпеки, особливо в екстремальних умовах наявності кіберінцидентів. Таку потребу задовольнить спроєктована ІГІСУ сектору національної кібербезпеки, яка, у свою чергу, для безпечного функціонування потребує створення комплексної системи кіберзахисту.

2. АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Проведений аналіз вітчизняних наукових публікацій, присвячених питанням створення систем захисту керівних систем засвідчив, що вказаний тематичний напрям перебуває у фокусі предмет-

ної уваги таких сучасних вчених: Ю. В. Землянко, О. А. Замула, О. О. Ткач, Н. І. Литвинова, Я. А. Пересічанська, В. В. Домарев, С. В. Ленков, Д. А. Перегудов, В. А. Хорошков, В. А. Герасименко, М. С. Вєртузаєв, О. М. Юрченко [1–5].

3. ПОСТАНОВКА ПРОБЛЕМИ В ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ АКТУАЛЬНІСТЬ

Для забезпечення високого рівня керованості стратегічно важливим для держави сектором національної кібербезпеки синтезовано ІГІСУ сектору національної кібербезпеки, котра, у свою чергу, згідно із чинними державними вимогами, потребує комплексної системи захисту.

Тому така потреба у забезпеченні комплексного кіберзахисту ІГІСУ сектором національної кібербезпеки зумовила вибір теми статті. Саме сформована комплексна система кіберзахисту ІГІСУ сектором національної кібербезпеки і стала фундаментальним ядром і предметом цього дослідження.

4. МЕТА СТАТТІ

Окреслені вище проблеми обумовили мету нашої наукової розвідки, яка передбачає визначення та розроблення комплексної системи для забезпечення захисту ІГІСУ сектору національної кібербезпеки.

5. МЕТОДОЛОГІЧНИЙ АПАРАТ ДОСЛІДЖЕННЯ

Фундаментальним базисом цього дослідження стали структурно-функціональний і системний загальнонаукові підходи.

Додатково використано нормативно-правовий підхід.

6. КОРОТКИЙ ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

ІГІСУ, як і будь-яка вперше запроєктована керівна система державного значення, що містить ІзОД, в обов'язковому порядку, підлягає захисту.

Система кіберберзахисту ІГІСУ сектору національної кібербезпеки має носити комплексний характер.

Причому до складу комплексної системи захисту ІГІСУ сектору національної кібербезпеки передбачено задіяти таку кількість чітко впорядкованих, взаємопов'язаних, сучасних інструментів захисту, сукупність яких:

1) є необхідною та достатньою для повноцінного захисту ІГІСУ як керівної системи, а також для протистояння зовнішнім НСД.

2) дозволить забезпечити максимально високий рівень захисту цілісності, конфіденційності та доступності інформації, яка оброблятиметься в ІГІСУ сектору національної кібербезпеки.

Перелік таких засобів захисту визначався:

1) специфікою та цінністю для держави даних, якими оперує керівна система, що підлягає захисту;

2) відповідністю обраної системи кіберзахисту міжнародним критеріям і стандартам захисту подібних керівних систем для країн НАТО, зокрема, TCSEC ("Оранжева книга"). Це кібербезпековий стандарт США:

- у ньому прописано критерії, які в обов'язковому порядку використовує міністерство оборони США;
- він установлює базові вимоги щодо контролю комп'ютерної безпеки, убудованої в комп'ютерну систему;
- його використовують для класифікації та оцінювання керівних систем, у яких обробляється закрита інформація [6];

3) відповідністю обраної системи кіберзахисту міжнародним критеріям і стандартам захисту подібних керівних систем для інших провідних країн світу, зокрема і міжнародному технічному стандарту ISO/IEC 15408 "Загальні критерії оцінки безпеки ІТ", який ратифікувало більшість провідних країн [7];

4) відповідністю обраної системи кіберзахисту настановам і рекомендаціям міжнародної організації NCSS (National Cyber Security Strategies) для країн-партнерів НАТО, що розроблені міжнародними експертами з питань національної кібербезпеки, науковцями та європейськими радниками з міжнародної кібербезпеки в контексті проєкту Програма НАТО SPS "Наука заради миру та безпеки" [8, С. 51–58].

5) відповідністю обраної системи кіберзахисту Директивам NIS для країн ЄС, котрі:

- закладають єдині правила та вимоги у сфері кібербезпеки для всіх країн ЄС, але залишають за кожною країною-членом право вжити власних заходів щодо імплементації норм цієї Директиви;
- вимагають запровадити практику управління ризиками та зобов'язати сповіщення про кіберінциденти;
- рекомендують здійснювати аналіз проблем у сфері національної кібербезпеки та пошук шляхів їхнього вирішення;
- стверджують, що побудова ефективної державної політики щодо кібербезпеки можлива лише за наявності єдиного центру управління, за умови створення належної інфраструктури кібербезпеки, за умови розвитку індустрії кібербезпеки (шляхом забезпечення умов для плідної

співпраці всіх українських і міжнародних стейкхолдерів, а також чіткої узгодженої програми дій із стейкхолдерами з метою підвищення рівня довіри між основними стейкхолдерами з питань кібербезпеки) [9];

6) відповідністю обраної системи кіберзахисту національним технічним стандартам України, які вимагають наявності певних кібербезпекових складових, злагоджене функціонування яких підтримуватиме належний захист керівної системи від НСД [10–13].

Загалом, саме така сукупність обраних інструментів і процедур для захисту ІГІСУ сектору національної кібербезпеки:

1) має захищати керівну систему:

• від витікання даних технічними каналами, до яких належать канали побічних електромагнітних випромінювань і наведень, акустоелектричні й інші канали;

• від несанкціонованих дій та несанкціонованого доступу до інформації, що можуть здійснюватися шляхом підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм, використання комп'ютерних вірусів тощо;

• від спеціального впливу на інформацію, який може здійснюватися шляхом формування полів і сигналів із метою порушення цілісності інформації або руйнування системи захисту тощо.

2) має забезпечувати керівну систему:

• здатністю протистояти шкідливим зовнішнім впливам;

• здатністю адаптуватися до нових непередбачуваних ситуацій, виконуючи свою цільову функцію за рахунок відповідної зміни структури і поведінки системи;

• готовністю адаптуватися до нових непередбачуваних ситуацій (атак, ушкоджень, аварій), виконуючи свою цільову функцію за рахунок відповідної зміни поведінки системи;

• готовністю до технічних відмов системи в заданих межах;

• спроможністю швидко відновлюватися до штатного режиму роботи системи після збоїв;

• спроможністю протистояти зовнішнім деструктивним впливам;

• здатністю убезпечувати та захищати інформацію від несанкціонованого посягання.

У цьому випадку кібербезпека керівної системи:

1) не залежить від архітектурного чи її функціонального наповнення;

2) досягається стандартним шляхом, який є однаковим для всіх ІСУ, який є законодавчо врегульованим і чітко регламентованим, за рахунок обов'язкової наявності:

а) додаткових загальнообов'язкових зовнішніх стандартних модулів для захисту державних інформаційних ресурсів, таких як:

• додаткова система адміністрування кібербезпеки КСЗІ, за встановлення, сертифікацію та функціонування якої відповідає СБУ та ДССЗЗІ (згідно із чинним законодавством, оскільки сектор національної кібербезпеки належить до державних структур стратегічно важливого значення);

• додатковий зовнішній модуль адміністрування інтернет-безпеки ЗВІД (КУПОЛ) як додатковий зовнішній програмно-апаратний блок-модуль та частина зовнішньої державної системи кібербезпеки від інтернет-загроз;

б) додаткових зовнішніх стандартних модулів, що забезпечують готовність керівної системи до перевантаження напруги у мережах;

в) сформованих алгоритмів налаштувань параметрів автоматизованого регулятора залежно від;

• змін параметрів об'єкта управління;

• властивостей і готовності автоматизованого регулятора до можливих автоматичних збурень.

Розглянемо детальніше повний асортимент загальнообов'язкових ресурсів та інструментів, які включають п'ять рівнів кіберзахисту.

Перша група *передбачає застосування всіх можливих організаційних заходів кіберзахисту ІГІСУ сектору національної кібербезпеки та включає:*

1) наявність, знання та дотримання вимог нормативних документів, таких як:

• система забезпечення кібербезпеки;

• політика кібербезпеки у роботі з ІГІСУ сектору національної кібербезпеки;

• принципи кібербезпеки;

• настанови й інструктивні матеріали для адміністраторів і користувачів ІГІСУ сектору національної кібербезпеки;

• регламенти дій на випадок настання кіберінциденту;

2) застосування організаційних процедур розмежування (відповідно до законодавства щодо особливостей поводження з ІзОД), таких як:

• розмежування доступу користувачів та адміністраторів (згідно із законодавчо передбаченою ієрархією категорій і рівнів доступу);

• розмежування допуску користувачів та адміністраторів (згідно із законодавчо передбаченою ієрархією категорій і рівнів допуску);

• розподіл обов'язків адміністраторів;

3) дотримання встановлених рівнів конфіденційності:

• довірча конфіденційність (мінімальна, базова, повна, абсолютна);

• адміністративна конфіденційність (згідно з ієрархією апарату керування сектором національної кібербезпеки);

• аналіз наявності прихованих каналів (виявлення, контроль, перекриття);

• рівні конфіденційності під час трансакційного обміну (експорт-імпорт) інформацією, яка має критерії (мінімальна, базова, повна, абсолютна);

4) належна реєстрація та повноцінне документування будь-яких наглядових процедур:

• перевірки середовища функціонування на об'єкті автоматизації;

• випробувань (краш-тестів тощо);

• перевірок (планових, поточних, позапланових);

• виявлених порушень у паперовому журналі та вчасної сигналізації національної кібербезпеки;

5) забезпечення цілісності системи:

• адміністративної цілісності (мінімальна, базова, повна, абсолютна);

• довірчої цілісності (мінімальна, базова, повна, абсолютна);

• функціональної цілісності шляхом забезпечення належного технічного комплектування та можливості повернення до початкового рівня захисту (повні чи обмежені);

• цілісності інформації у разі обміну (мінімальна, базова, повна);

• цілісності з функціями диспетчера доступу;

6) застосування процедури профілактичного тестування засобів захисту ІГІСУ сектору національної кібербезпеки:

а) періодичне самотестування в реальних умовах функціонування (за потреби, при старті, у будь-який час);

б) тестування:

• на стійкість до відмов (з установленням обмежень);

• профілактичне чи поточне за запитом (із частковою заміною компонентів або повною модернізацією);

• на швидке відновлення після збоїв (ручне, автоматизоване, повне, часткове);

• доступність до необхідного державного ресурсного забезпечення за потреби (пріоритетність таких систем на використання ресурсів);

7) застосування процедур упереджувального технічного нагляду (моніторингу та контролю) рівня кіберзахисту керівної системи:

• перевірка вузлів і даних;

• перевірка достовірності каналу надходження поточних даних (одно- чи двонаправлений);

• перевірка цілісності комплексу засобів захисту;

• експертний нагляд за кібербезпекою та поточне супроводження кіберзахисту ІГІСУ сектору національної кібербезпеки;

• нагляд за дотриманням умов експлуатації;

• нагляд за використанням паролей безпеки.

Друга група *передбачає застосування всіх можливих програмних засобів забезпечення кібербезпеки ІГІСУ сектору національної кібербезпеки* – це спеціальні програмні засоби, що включаються до складу програмного забезпечення комплексних систем (КС) винятково для виконання захисних функцій керівної системи:

а) основні програмні засоби захисту:

• програми ідентифікації та аутентифікації користувачів КС;

• антивірусні програми;

• програми розмежування доступу користувачів до ресурсів КС;

• програми шифрування інформації (криптоключі, шифрувально-дешифрувальні програми, паролі, шифро-алгоритми);

• програми захисту інформаційних ресурсів (системного й прикладного програмного забезпечення, баз даних, комп'ютерних засобів навчання тощо) від несанкціонованої зміни, використання й копіювання.

б) допоміжні програмні засоби захисту:

• програми знищення залишкової інформації (у блоках оперативної пам'яті, тимчасових файлах тощо);

• програми аудиту з реєстрацією в журналі факту подій;

• програми тестового контролю рівня захищеності КС тощо.

Третя група *передбачає застосування всіх можливих апаратно-технічних засобів забезпечення захисту керівної системи* – це електронні й електронно-механічні апаратно-технічні пристрої, що включаються до складу технічних засобів КС та виконують (самостійно або в єдиному комплексі із іншими програмними засобами) деякі функції забезпечення інформаційної безпеки:

а) основні апаратні засоби:

• ключі доступу, системи сигналізації, засоби блокування;

• пристрої для ідентифікації користувача (магнітні та пластикові карти, відбитки пальців тощо);

• пристрої для шифрування інформації;

• пристрої для перешкоджання несанкціонованому включенню робочих станцій і серверів (електронні замки і блокатори);

б) допоміжні апаратні засоби:

• пристрої виявлення та знищення інформації на магнітних носіях;

• пристрої сигналізації про спроби несанкціонованих дій користувачів КС;

в) допоміжне апаратно-технічне обладнання, на зразок, апаратно-технічного комплексу КУПОЛ (ЗВІД), яке застосовується для захисту:

• комп'ютерної системи від несанкціонованих Інтернет втручань;

• зовнішніх мережевих каналів передачі інформації.

Четверта група *передбачає застосування усіх можливих додаткових засобів забезпечення кіберзахисту ІГІСУ сектору національної кібербезпеки та включає:*

а) застосування інженерно-технічних засобів зовнішнього поточного відеоконтролю (відеонагляду, відеоспостереження) таких як:

• інженерно-технічний відеозахист зовнішнього периметру території на якій знаходиться об'єкт автоматизації ІГІСУ;

• інженерно-технічний відеозахист зовнішнього інфраструктури об'єкта автоматизації ІГІСУ;

• інженерно-технічний відеозахист внутрішньо-будинкової інфраструктури об'єкта автоматизації ІГІСУ;

• інженерно-технічний захист (зсередини) конкретного приміщення об'єкту автоматизації, де знаходиться сама ІГІСУ сектору національної кібербезпеки;

б) застосування інженерно-технічних пристроїв:

• технічного обладнання;

• пристроїв зовнішнього екранування;

• захисних конструкцій (споруд).

П'ята група *передбачає застосування всіх можливих додаткових засобів, таких як фізична охорона підрозділами безпеки середовища функціонування ІГІСУ сектору національної кібербезпеки:*

• фізична охорона (по периметру) зовнішньої прибудинкової території навколо об'єкта автоматизації ІГІСУ;

• фізична охорона входів-виходів та внутрішньобудинкової інфраструктури, обладнання, систем об'єкта автоматизації ІГІСУ.

7. ОТРИМАНИЙ НАУКОВИЙ РЕЗУЛЬТАТ І ЙОГО ПРИКЛАДНА ЦІННІСТЬ

Результатом дослідження стало представлення ключових аспектів і специфічних особливостей комплексної системи:

• яка спеціально створена для забезпечення кіберзахисту ІГІСУ сектору національної кібербезпеки;

• яка виступає фундаментальним ядром і предметом цього дослідження;

• структурні складові та прикладна цінність якої глибоко пояснюються у межах цього дослідження.

8. ВИСНОВКИ

Із усього вище зазначеного випливає логічний висновок стосовно того, що, найбільшої уваги з-поміж інших заслуговує:

• не лише розроблення сучасної автоматизованої ІГІСУ сектору національної кібербезпеки;

• але й система її кіберзахисту, яка забезпечить безперебійну роботу зазначеної керівної системи в умовах сучасних потенційних ризиків і зовнішніх кіберзагроз.

9. ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Подальші дослідження доцільно присвятити питанням розроблення, упровадження, а також процедурі ліцензування описаної вище системи кіберзахисту ІГІСУ сектору національної кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Землянко, Ю. В., Замула, О. А., Ткач, О. О., Литвинова, Н. І., & Пересічанська, Я. А. (2010). Принципи та порядок розробки комплексних систем захисту інформації в інформаційно-телекомунікаційних системах. *Прикладная радиоэлектроника*, т. 9, № 3. 460–469.

[2] Лєнков, С. В., Перегудов, Д. А., & Хорошко В. О. (2008). Методи та засоби захисту інформації. *Несанкціоноване отримання інформації* (Т. 1). К., 464.

[3] Вєртузаєв М. С., Юрченко О. М. (2001). Захист інформації в комп'ютерних системах від несанкціонованого доступу, К., 201 с.

[4] Міжнародний стандарт ISO/IEC 15408. Загальні критерії оцінки безпеки ІТ (Міжнародний стандарт Міністерства оборони США TCSEC – "Помаранчева книга").

[5] A. Klimburg (Ed.) (2012, January 10), National Cyber Security Framework Manual, NATO CCD COE Publication, Tallinn, 253. https://www.ccdcoe.org/uploads/2018/10/NCSFM_0.pdf.

[6] Кольцов, М., Приходько, О., & Аушев, Є. Пропозиції до політики щодо реформування сфери кібербезпеки в Україні (Директиви NIS для ЄС). https://pdf.usaid.gov/pdf_docs/PA00XC84.pdf

[7] НД ТЗІ 2.5.004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затв. нак. № 806 ДСТСЗІ СБУ від 28.12.2012.

[8] НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від НСД. Затв. нак. № 22 ДСТСЗІ СБУ від 28.04.1999.

[9] Дежстандарт України. Інформаційні технології. Настанови з керування безпекою інформаційних технологій (Ч. 4). Вибір засобів захисту: ДСТУ ISO/IEC TR 133354:2005 (ISO/IEC TR 13335-4:2000, IDT), [Чинний від 2006-01-07]. К., 2005, 30 с.

[10] НД ТЗІ 3.7-003-2005. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. Затв. нак. № 806 ДСТСЗІ СБУ від 28.12.2012.

REFERENCES

[1] Zemlyanko, Y. V., Zamula, O. A., Tkach, O. O., Lytvynova, N. I., & Ya. A. Peresichanska (2010). Principles and order of development of complex information protection systems in information and telecommunication systems. *Applied radio electronics*, vol. 9, no. 3, p. 460–469 [in Ukrainian].

[2] Lenkov, S. V., Peregudov, D. A., & Khoroshko V. O. (2008). Methods and means of information protection, vol. I. *Unauthorized obtaining of information*, K., 464 [in Ukrainian].

[3] Vertuzaev, M. S., Yurchenko, M. S. (2001). Protection of information in computer systems against unauthorized access, K., 201 [in Ukrainian].

[4] International standard ISO/IEC 15408. General criteria for evaluating IT security (International standard of the US Department of Defense TCSEC – "Orange Book") [in Ukrainian].

[5] A. Klimburg (Ed.) (2012, January 10), National Cyber Security Framework Manual, NATO CCD COE Publication, Tallinn, 253. https://www.ccdcoe.org/uploads/2018/10/NCSFM_0.pdf.

[6] Koltsov, M., Prykhodko, O., & Aushev, E. Policy Proposals for Reform Policy Proposals for Cybersecurity Reform in Ukraine (NIS Directives for the EU), retrieved January 10 from https://pdf.usaid.gov/pdf_docs/PA00XC84.pdf [in Ukrainian]

[7] ND TZI 2.5.004-99. Criteria for evaluating the security of information in computer systems against unauthorized access. Approval on no. 806 DSTSZI SBU 28.12.2012 [in Ukrainian].

[8] ND TZI 1.1-002-99. General provisions on the protection of information in computer systems from NSD. Approval on DSTSZI SBU No. 22 of April 28, 1999 [in Ukrainian].

[9] Dezhstandard of Ukraine Information technologies. Information technology security management guidelines. Part 4. Selection of means of protection: DSTU ISO/IES TR 133354:2005 (ISO/IES TR 13335-4:2000, IDT), [Valid from 2006-01-07], Kyiv, 2005, 30 p. [in Ukrainian].

[10] ND TZI 3.7-003-2005. The procedure for carrying out work on the creation of a comprehensive system of information protection in the information and telecommunications system of the enterprise. on DSTSZI SB U no. 806 dated 12.28.2012 [in Ukrainian].

Стаття надійшла до редколегії 16.03.2023

Formation of the cyber protection system for the integrated industry information system of Ukraine of the national cyber security sector

This The article is devoted to the disclosure and elucidation of the envisaged composition, structure of measures and tools that will be part of a comprehensive system of protection of industry-integrated MIS in the national cybersecurity sector. The article also describes the specifics and strategic value of the involved resources, which will be operated by the established system of cybersecurity. It is noted that the industry-integrated cyber defense MIS envisages the use of a set of interconnected means and measures, the implementation of which is necessary and sufficient for the full protection of industry-integrated MIS to counter external unauthorized access, etc. Emphasis is placed on the compliance of the envisaged cybersecurity system with international criteria and standards of protection of such control systems for NATO countries, in particular, the US Department of Defense cybersecurity standard (TCSEC also known as "Orange Book"); with international criteria and standards for the protection of similar control systems for other leading countries, in particular, the international technical standard ISO/IEC 15408 "General criteria for assessing IT security", which has been ratified by most leading countries; with guidelines and recommendations of the International Organization NCSS (National Cyber Security Strategies) for NATO Partner countries, as set out in the National Cyber Security Strategy and developed by international national cybersecurity experts, scholars and European international cybersecurity advisers in the context of NATO's "Science for Peace and Security (SPS) Programme"; with national technical standards of Ukraine. The article also presents in detail the full range of mandatory resources and tools for the cybersecurity of designed industry-integrated MIS in the national cybersecurity sector, which include five levels of cybersecurity (organization, software, hardware, engineering, additional physical level).

Keywords: *IGIS cyber protection system; the sector of national cyber security; feature of the cyber protection system; components of cyber protection systems; compliance of the cyber protection system.*

Сергій Толюпа,
д-р техн. наук, проф.
Професор кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка. Київ, Україна.

Serhii Toliupa,
Dr. Sci. (Engin.), Prof.
Professor of the Department of Cyber Security and Information Protection of Taras Shevchenko Kyiv National University. Kyiv, Ukraine.

Лада Сліпачук,
аспірантка кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка. Київ, Україна.

Lada Slipachuk,
PhD Student of the Department of Cyber Security and Information Protection of Taras Shevchenko Kyiv National University. Kyiv, Ukraine.