Адміністративне право і процес

**УДК 355:004:005.32**

**DOI https://doi.org/10.5281/zenodo.19966320**

# Міжнародні підходи до цифровізації як інструмент розбудови доброчесності в оборонних секторах: аналіз практик та імплементаційні уроки для України

**Слободяник Станіслав Петрович**,
кандидат економічних наук, старший науковий співробітник,
науковий співробітник Наукового центру проблем виховання доброчесності та запобігання корупції у секторі безпеки та оборони Національного університету оборони України, м. Київ, Україна
https://orcid.org/0000-0001-5537-2723

**Долгий Олександр Олександрович**,
доктор юридичних наук, старший науковий співробітник,
провідний науковий співробітник Наукового центру проблем виховання доброчесності та запобігання корупції у секторі безпеки та оборони Національного університету оборони України, м. Київ, Україна
https://orcid.org/0000-0003-4433-454X

**Куриліна Оксана Василівна,**
кандидат економічних наук, доцент,
старший науковий співробітник
Наукового центру проблем виховання доброчесності
та запобігання корупції у секторі безпеки та оборони
Національний університет оборони України, м. Київ, Україна
https://orcid.org/0000-0002-8813-4243


ISSN: 3041-2110

**Руснак Дмитро Іванович**,
доктор філософії в галузі права,
старший науковий співробітник
Наукового центру проблем виховання доброчесності
та запобігання корупції у секторі безпеки та оборони
Національного університету оборони України, м. Київ, Україна
https://orcid.org/0000-0001-8388-8786

**Прийнято: 12.04.2026 | Опубліковано: 30.04.2026**

**Анотація: Актуальність.** Розробка дослідження та процес написання даної статті був спрямований на теоретичне обґрунтування та розробку концептуальних засад перезапуску системи внутрішнього контролю в Міністерстві оборони України базуючись на використанні сучасних цифрових технологій на основі аналізу кращих міжнародних практик розбудови доброчесності.

**Мета.** Метою статті є теоретичне обґрунтування та розроблення концептуальних засад перезапуску системи внутрішнього контролю в Міністерстві оборони України на основі сучасних цифрових технологій з урахуванням міжнародних практик розбудови доброчесності в оборонному секторі.

**Методи.** У дослідженні використано комплекс загальнонаукових і спеціальних методів, зокрема аналіз і синтез, структурно-функціональний метод, порівняльно-правовий метод, метод інституційного аналізу, а також елементи процесного підходу для інтерпретації моделей цифровізації контролю та управління ризиками. Емпіричну основу становили міжнародні практики цифрової трансформації оборонного управління, нормативно-правові акти України та аналітичні матеріали щодо розвитку внутрішнього контролю й аудиту.

 ISSN: 3041-2110

**Результати.** В межах статті визначено системні недоліки існуючої системи внутрішнього контролю, проаналізовано кращі міжнародні практики – зокрема досвід аналітичної платформи Advana, процесний підхід відповідно до Постанови КМУ № 50 від 17.01.2025, а також стандарти COSO та ISO 9001. Вони включають фрагментарність нормативної бази, недостатню кваліфікація кадрів, відсутність єдиної методології ризик-орієнтованого підходу та слабку координація між органами влади. Також було встановлено, що для покращення ситуації з неефективність виявлення фінансових порушень необхідно впровадити автоматизовані платформи моніторингу ризиків та аналітики даних для узгодження з відповідними міжнародними стандартами.

**Висновки.** Запропоновано концепцію «СВК 2.0» як платформи превентивного управління ризиками з елементами Big Data, штучного інтелекту та технологій розподілених реєстрів. Зважаючи на це, пропонується також усунути сприйняття даної концепції як поточного інструменту звітності, а сприймати саме як стратегічний інформаційний механізм планування, контролю та забезпечення доброчесності в умовах війни та мирного часу. Це вирішить проблеми реактивності, фрагментованості та малозв'язаності чинної СВК у МО України і усуне питання несвоєчасного виявлення критичних відхилень у русі ресурсів та прийнятті управлінських рішень. Таким чином, в межах формування рекомендацій було обґрунтовано, що цифровізація в оборонному секторі є не лише інструментом підвищення ефективності, але й фундаментальним механізмом запобігання корупції.

**Ключові слова:** система внутрішнього контролю; цифровізація; доброчесність; оборонний сектор; defence governance; risk-based control; digital integrity systems; process mining; Big Data; blockchain.

 ISSN: 3041-2110

# International approaches to digitalisation as a tool for building integrity in the defence sector: an analysis of practices and lessons for implementation in Ukraine

**Stanislav Slobodianyk,**
Candidate of Economic Sciences, Senior Research Fellow,
Research Fellow of the Scientific Center for Problems of Integrity Education and Prevention of Corruption in the Security and Defense Sector of the National Defense University of Ukraine, Kyiv, Ukraine
https://orcid.org/0000-0001-5537-2723

**Oleksandr Dolhyi,**
Doctor of Law, Senior Research Fellow,
Leading Research Fellow of the Scientific Center for Problems of Integrity Education and Prevention of Corruption in the Security and Defense Sector of the National Defense University of Ukraine, Kyiv, Ukraine
https://orcid.org/0000-0003-4433-454X

**Oksana Kurylina,**
Candidate of Economic Sciences, Associate Professor,
Senior Research Fellow of the Scientific Center for Problems of Integrity Education and Prevention of Corruption in the Security and Defense Sector of the National Defense University of Ukraine, Kyiv, Ukraine
https://orcid.org/0000-0002-8813-4243


ISSN: 3041-2110

**Dmytro Rusnak,**
Doctor of Philosophy in Law,
Senior Researcher, Scientific Center for Problems of Integrity Education
and Corruption Prevention in the Security and Defense Sector,
National Defense University of Ukraine, Kyiv, Ukraine
https://orcid.org/0000-0001-8388-8786

**Abstract: Relevance.** The research and writing process for this article was aimed at providing a theoretical justification and developing the conceptual framework for the relaunch of the internal control system at the Ministry of Defence of Ukraine, based on the use of modern digital technologies and an analysis of best international practices in integrity building.

**Purpose.** The purpose of the article is to theoretically substantiate and develop conceptual principles for restarting the internal control system in the Ministry of Defense of Ukraine based on modern digital technologies, taking into account international practices for building integrity in the defense sector.

**Methods.** The study used a complex of general scientific and special methods, in particular analysis and synthesis, structural-functional method, comparative legal method, institutional analysis method, as well as elements of a process approach for interpreting models of digitalization of control and risk management. The empirical basis was international practices of digital transformation of defense management, regulatory legal acts of Ukraine and analytical materials on the development of internal control and audit.

**Results.** The article identifies systemic shortcomings in the existing internal control system and analyses best international practices – in particular, the experience of the Advana analytical platform, the process-based approach in accordance with CMU Resolution No. 50 of 17 January 2025, as well as the COSO and ISO 9001 standards. These include the fragmented nature of the regulatory framework, insufficient staff qualifications, the lack of a unified methodology for a

risk-based approach, and poor coordination between government bodies. It was also established that, to improve the situation regarding the ineffective detection of financial violations, it is necessary to implement automated risk monitoring and data analytics platforms to bring them into line with relevant international standards.

**Conclusions.** In addition, the concept of 'ICS 2.0' was proposed as a platform for preventive risk management incorporating elements of Big Data, artificial intelligence and distributed ledger technologies. In view of this, it is also proposed to move away from viewing this concept as a mere reporting tool, and instead regard it as a strategic information mechanism for planning, control and ensuring integrity in both wartime and peacetime. This will resolve the issues of reactivity, fragmentation and lack of coordination within the current SCM system at the Ministry of Defence of Ukraine and eliminate the problem of untimely detection of critical deviations in resource flows and management decision-making. Thus, in formulating the recommendations, it was argued that digitalisation in the defence sector is not only a tool for improving efficiency but also a fundamental mechanism for preventing corruption.

**Keywords:** internal control system; digitalisation; integrity; defence governance; risk-based control; digital integrity systems; process mining; Big Data; blockchain; anti-corruption management.

**Постановка проблеми** Сучасна архітектурна рамка безпеки та оборони України знаходиться в процесі трансформації, зумовленої війною з рф, глибокою інституційною інтеграцією до євроатлантичних структур та суспільним усвідомленням необхідності підвищення ефективності використання обмежених ресурсів. У цьому контексті розбудова доброчесності та боротьба з корупцією перетворюється на критичний чинник, що безпосередньо впливає на національну безпеку та обороноздатність держави.


ISSN: 3041-2110

Існуючі системи внутрішнього контролю (далі – СВК) в Міністерстві оборони України тривалий час демонструють ознаки незрілості та неефективності як інструменту запобігання зловживанням у сфері управління ресурсами держави та підвищення ефективності організації в цілому.

Ключовою вразливістю існуючої СВК залишається «людський фактор» – відсутність дієвих механізмів контролю, широкі дискреційні повноваження, визначені для посади в ланцюжках процесів у точках прийняття критичних рішень (логістика, управління ресурсами, закупівлі). В цих процесах цифровізація є не тільки оптимізацією за рахунок ІТ-рішень, але й фундаментальним інструментом попередження корупційних злочинів. Досвід розвинутих країн та кращих транснаціональних корпорацій (далі – ТНК) свідчить: перехід на алгоритмізоване управління та автоматизований моніторинг на основі Big Data та штучного інтелекту (далі – ШІ) спроможний не тільки забезпечити прозорість прийнятих рішень, але й підвищити ефективність менеджменту організації в цілому.

Актуальність дослідження підсилюється тим, що партнери України вимагають прозорої системи моніторингу та контролю за ефективним використанням отриманих ресурсів. Існуюча СВК не вирішує цю нагальну проблему, однак це не означає, що система непридатна для українських реалій. Перезапуск СВК, побудованої за принципами Integrity-by-Design (доброчесність через дизайн системи), вочевидь стає безальтернативним.

Запровадження «СВК 2.0» (Integrity-by-Design) передбачає предиктивну аналітику, здатну ідентифікувати аномалії в режимі реального часу – до підписання фінансових документів, – смарт-контракти та завершення переходу на автоматизовану систему документообігу.

Дискусія навколо цифровізації антикорупційних заходів у Міністерстві оборони України (далі – МО України) потребує переходу від загальних декларативних закликів до чітких дій із формування архітектурних рішень. Аналіз досвіду запровадження таких систем у розвинутих країнах (зокрема, в

Сполучених Штатах Америки діє платформа Advana [1], а також цифрові протоколи NSPA [2]) допоможе Україні уникнути «дитячих хвороб» цифровізації та побудувати дійсно ефективну СВК.

Таким чином, дослідницьке питання статті може бути сформульоване так: яким чином міжнародні підходи до цифровізації внутрішнього контролю та управління ризиками в оборонному секторі можуть бути адаптовані до інституційних умов Міністерства оборони України для формування дієвої системи доброчесності превентивного типу?

**Аналіз останніх досліджень і публікацій.** У вітчизняному науковому полі проблематика внутрішнього контролю в секторі безпеки й оборони досліджується переважно через нормативно-правову та організаційно-методичну призму. Зокрема, А. А. Бойко [3], Н. В. Козловська [4], А. А. Лойшин [5, 6], С. П. Слободяник [7] та інші вказують на фрагментарність регулювання, недостатню узгодженість контрольних процедур, потребу в чіткіших критеріях оцінювання ефективності системи внутрішнього контролю та необхідність посилення її ролі в управлінні державними ресурсами. Окрему увагу дослідники [3-7] приділяють питанням інституційної спроможності внутрішнього контролю, його зв’язку з внутрішнім аудитом, управлінням ризиками та формуванням підходів до оцінювання результативності контрольного середовища в органах публічного управління, зокрема у структурі МО України. Натомість у міжнародному контексті акцент зміщується з нормативного осмислення проблеми саме на цифрові інструменти забезпечення прозорості, простежуваності процесів і зниження корупційних ризиків. Так, Г. Лін [8], Л. Перес [9], В. М. П. ван дер Алст [10] та інші визначають інтеграцію даних, process mining, цифровий моніторинг, автоматизоване виявлення відхилень і використання захищених розподілених реєстрів як дієві засоби підвищення підзвітності та доброчесності організаційних систем.


ISSN: 3041-2110

Водночас між цими двома групами досліджень простежується суттєвий методологічний розрив. Якщо вітчизняні автори переважно зосереджуються на нормативному оформленні, інституційних повноваженнях і процедурній стороні внутрішнього контролю, то міжнародні публікації орієнтовані на технологічні механізми забезпечення простежуваності, автоматизованого виявлення відхилень та інтеграції даних. Унаслідок цього український сегмент літератури недостатньо розкриває питання цифрової архітектури доброчесності як операційного середовища контролю, тоді як міжнародний сегмент, попри високий інструментальний потенціал, здебільшого не враховує специфіку правового режиму, інституційної фрагментації та воєнного контексту функціонування оборонного сектору України.

Отже, наявні дослідження створюють важливе підґрунтя для осмислення внутрішнього контролю та цифровізації, проте недостатньо розкривають цифровізацію саме як інструмент розбудови доброчесності в оборонному секторі, що й зумовлює доцільність даного дослідження. Тому ***метою статті*** є теоретичне обґрунтування та розроблення концептуальних засад перезапуску системи внутрішнього контролю в МО України шляхом використання сучасних цифрових технологій на основі аналізу кращих міжнародних практик розбудови доброчесності.

**Виділення невирішених раніше частин загальної проблеми**. Незважаючи на широкий обсяг літератури, що стосується внутрішнього контролю та аудиту, процесного управління та цифровізації публічного сектору, у науковому дискурсі досі відсутнє цілісне бачення цифровізації саме як інструменту розбудови доброчесності в оборонному секторі. І якщо у вітчизняних працях висвітлено переважно нормативно-правовий вимір даного питання, то у міжнародному контексті пропонується та досліджується саме інструментарій, який міг би дозволити підвищити доброчесність організаційних систем, проте досі не цілком імплементований; що є недостатнім для вирішення наявних проблем, а саме: реактивність,

фрагментованість, малозв'язаність чинної СВК у МО України з процесним управлінням і неможливість забезпечення своєчасного виявлення критичних відхилень у русі ресурсів та прийнятті управлінських рішень.

**Формулювання цілей статті (постановка завдання).** Зважаючи на необхідність теоретичного обґрунтування та розробки концептуальних засад перезапуску системи внутрішнього контролю за рахунок цифрових технологій, було визначено наступні завдання дослідження:

- встановити ключові обмеження чинної системи внутрішнього контролю в МО України;
- проаналізувати ряд актуальних міжнародних практик цифрової трансформації у сфері оборони та розбудови доброчесності;
- визначити потенціал використання сучасних цифрових інструментів, зокрема BPM, Big Data, process mining тощо;
- обґрунтувати концептуальні засади моделі «СВК 2.0» як інтегрованої системи превентивного контролю;
- розробити рекомендації для України з урахуванням потреби створення єдиної оборонної аналітичної платформи.

**Методологія дослідження.** Методологічну основу статті становить комплекс загальнонаукових і спеціальних методів дослідження. За допомогою методів аналізу та синтезу узагальнено теоретичні підходи до функціонування систем внутрішнього контролю в оборонному секторі. Порівняльно-правовий метод застосовано для зіставлення українських практик із міжнародними підходами до цифровізації контролю та забезпечення доброчесності. Структурно-функціональний метод використано для визначення взаємозв'язків між внутрішнім контролем, внутрішнім аудитом, процесним управлінням і цифровими інструментами моніторингу. На основі системного підходу обґрунтовано концепцію «СВК 2.0» як інтегрованої моделі превентивного контролю в Міністерстві оборони України.


ISSN: 3041-2110

**Виклад основного матеріалу дослідження.** Як свідчать сучасні наукові дослідження, існуюча модель СВК часто характеризується формалізмом, надмірною бюрократизацією, низьким рівнем розуміння системи, браком кваліфікованих спеціалістів, низьким рівнем автоматизації та відсутністю системного процесного підходу [3, 4, 5, 6]. Замість того щоб виступати механізмом запобігання ризикам, функціонування СВК часто зводиться до документування фактів порушень, що вже відбулися: тобто контроль існує, але «постфактум» і не має реального впливу на стримування корупції.

Офіційна парадигма спирається на принципи ризик-орієнтованого контролю, управління ресурсами та забезпечення прозорості в оборонному секторі, однак відсутність робочої методології, слабка інституційна культура та мінливість нормативно-правової бази утворюють системні «сліпі зони» у практиці застосування на рівні структурних підрозділів МО України. СВК залишається формальним інструментом звітності, а не механізмом реального управління ризиками та виявлення критичних відхилень в управлінні ресурсами держави.

Аудиторська рада Ukraine Facility у своєму звіті відзначає критичну необхідність посилення ролі СВК та внутрішнього аудиту в державному секторі з метою забезпечення розвитку доброчесності, ефективного управління ресурсами та підвищення ефективності процесів організації. Зокрема, підкреслюється, що інструменти НАЗК – управління конфліктами інтересів і механізми повідомлення про порушення – мають бути інтегровані в діяльність усіх міністерств і відомств, включно з оборонним сектором. У даному контексті цифрові інструменти слід розглядати як інфраструктуру підзвітності, що посилює контрольні та аналітичні можливості державного управління [11]. В українському контексті цифровізаційні зрушення є можливістю для розробки комплексних рішень, що, не будучи формалізованими, спрямовуватимуться на посилення прозорості й підзвітності в ключових сферах.

Зважаючи на це, до переліку системних недоліків функціонування державного внутрішнього фінансового контролю в Україні з огляду на її трансформацію відповідно до Угоди про асоціацію з ЄС варто віднести наступні:

- фрагментарність нормативно-парової бази щодо державного внутрішнього фінансового контролю. Це відображається передусім у відсутності цілісної, логічно узгодженої та однаково зрозумілої для всіх рівнів управління рамки практичного застосування; і, відповідно, призводить до ускладнення стандартизації регулюючих дій та створює можливості до різного трактування регламентації та управління ризиками;
- недостатня кваліфікація кадрів, що виражається у дефіциті та надмірному навантаженні на існуючих фахівців, здатних працювати з сучасною моделлю внутрішнього контролю;
- відсутність єдиної методології ризик-орієнтованого підходу. Тобто підхід, не маючи чіткої та дієвої методології, залишається переважно декларативним і не сприймається як операційний механізм для прогнозування відхилень, створення цифрового реєстру ризиків та інтеграції контролю ключових процесів (фінансових, закупівельних, логістичних тощо), а є реактивною системою для постфактумної фіксації;
- слабка координація між органами влади, що через відсутність стійких механізмів обміну інформацією, спільних аналітичних інструментів і зрозумілих процедур ескалації порушень призводить до неефективного виявлення фінансових порушень.

Наявність окреслених прогалин зумовлює потребу переходу до автоматизованих платформ моніторингу ризиків та аналітики даних, узгоджених із міжнародними стандартами COSO, INTOSAI, а також із сучасними підходами до процесного управління та цифрової підзвітності [6]. Для оборонного сектору це означає необхідність запровадження інструментів, здатних забезпечити безперервний моніторинг ключових контрольних

показників, виявлення аномалій і підвищення антикорупційної спроможності внутрішнього контролю в режимі реального часу [7].

Внутрішній аудит у державному секторі України було офіційно запроваджено у 2012 році відповідно до Закону «Про основні засади здійснення державного фінансового контролю в Україні» та методичних рекомендацій Міністерства фінансів України (далі – Мінфін). У посібнику Мінфін пропонує систематизований підхід до організації аудиту ефективності як окремого напряму внутрішнього аудиту, спрямованого на оцінку економічності, ефективності та результативності управління ресурсами [12]. Тобто даним документом підкреслюється важливість адекватної інтерпретації результатів аудиту, що у даному випадку постає інструментом, спрямованим на реалізацію рекомендацій та механізмів притягнення до відповідальності керівництва.

Низка сучасних досліджень, зокрема аналіз проведений Інститутом внутрішніх аудиторів України, який узагальнює ситуацію у сфері внутрішнього аудиту на фоні воєнного стану та економічних перетворень [13], підкреслюють, що наразі простежується достатньо стійка культура корпоративного контролю зі структурно зрілою функцією внутрішнього аудиту. Тобто наголошується на тому, що сучасний аудит має бути спрямований не лише на постфактумній фіксації відхилень, а й враховувати існуючі та перспективні критичні ризики, зокрема і неперервність бізнес-процесів, кібербезпекові ризики, охорону персональних даних, можливості до боротьби зі шахрайством і корупцією тощо. Проте у даному випадку варто наголосити на вагомому обмеженні, що полягає у недостатньому фінансуванні через відсутність значних інвестицій у цифрові технології та засоби автоматизації і, як наслідок у дефіциті відповідно кваліфікованих фахівців ( тут мається на увазі галузі IT-аудиту, кібербезпеки та ESG), які також потребують вкладень у підготовку та оплату праці.


ISSN: 3041-2110

Слід також наголосити, що матеріали круглого столу Рахункової палати України зафіксували зацікавленість учасників у наявності взаємозв'язків між зовнішнім та внутрішнім аудитом, що розглядали це як фактор впливу на ефективність СВК [14]. Це обумовлено фактом неналежної організації внутрішнього аудиту, що і призводить до системного характеру відхилень у фінансово-бюджетних процесах, які виявляються завдяки зовнішньому аудиту.

Постанова Кабінету Міністрів України від 17 січня 2025 року № 50, яка містить положення щодо впровадження процесного підходу, закріплює обов'язок створення спеціалізованих структурних підрозділів для аналізу та оптимізації робочих процесів за центральними органами влади (зокрема оборонними) [15]. Внаслідок чого перелічені у документі органи влади мають, перш за все, формувати каталог процесів, а також визначати відповідних власників та відповідальних осіб; крім того, за ними закріплюється обов’язок визначати ключові контролі та проводити щорічне звітування щодо їхнього удосконалення. Це підводить державні установи до моделі управління якістю, де кожен процес є повторюваним, регульованим і підлягає безперервному вимірюванню та вдосконаленню. У цьому контексті доцільно інтегрувати вимоги міжнародного стандарту ISO 9001, що передбачає формалізацію процесів, документування процедур, управління вимірюваннями та постійне вдосконалення системи управління.

Управлінська модель, побудована на процесах, спроможна виявляти «вузькі місця» та контрольні точки прийняття рішень, безпосередньо пов'язувати регламенти процесів з процедурами внутрішнього контролю, підвищувати прозорість, скорочувати дублювання функцій та підвищувати відповідальність конкретних підрозділів і посадових осіб. Кожен процес узгоджується з власником процесу, що робить процесне управління системно необхідним для ефективної СВК.


ISSN: 3041-2110

Модель ризик-орієнтованого контролю, процесного управління і прозорості в оборонному секторі вже дала основу для впровадження автоматизації в існуючі процедури і інформаційні системи МО України. Йдеться не про радикальну зміну, а про «надбудову» розумних засобів над вже затвердженими процесами, регламентами і моделями управління ризиками.

По-перше, умови Постанови КМУ № 50 вже дозволяють автоматизувати управління процесами. Каталог процесів, їх власники, контрольні точки і звіти про оптимізацію можна вбудувати в процесний портал або в модуль BPM (Business Process Management). BPM є не просто автоматизацією окремих завдань; це підхід, що розглядає будь-який процес (від оформлення договору до управління ризиками) як об'єкт управління: процес описують у вигляді моделі, вимірюють показники, виявляють «вузькі місця», оптимізують і регулярно переглядають. Портал відстежує статус процесу, час виконання, відхилення від регламенту й автоматично формує аналітичні звіти для СВК. Автоматизація зменшує бюрократичне навантаження: паперові звіти замінюються реальними KPI, а відповідальні за СВК зосереджуються на відхиленнях, а не на зборі даних.

По-друге, у МО України вже наявний ризик-орієнтований підхід і порядок внутрішнього контролю. Це створює основу для автоматизації реєстру ризиків. Цифровий реєстр ризиків, підключений до реєстрів закупівель, кадрових систем і фінансових баз, самостійно виявлятиме відхилення від лімітів, нестандартні умови контракту або зміни у власниках замовників.

По-третє, підхід до внутрішнього аудиту відкриває можливість підключити модулі автоматизованого аудиту з аналізом Big Data. Такий підхід може об'єднати модулі автоматизованого аудиту з електронними закупівлями, бюджетним плануванням і логістично-матеріальними системами. Це дозволить будувати сценарії ризик-орієнтованих перевірок, виявляти аномалії у споживанні ресурсів і відхилення у строках виконання програм.


ISSN: 3041-2110

Нарешті, імплементація міжнародних стандартів COSO, ISO 9001 і вимог NATO створить чітку рамку, в якій автоматизація не зменшує відповідальність керівництва, а навпаки – фіксує в системних журналах усі рішення, зміни регламентів та відповідності процедур показникам якості (KPI). Система цифрових інструментів забезпечує об'єктивність, повторюваність, швидку реакцію і підвищує відповідальність на кожному рівні управління.

Можливості BPM-систем необхідні, проте їх недостатньо для того, щоб визнати СВК реально ефективною, відкритою до передбачення ризиків, у тому числі корупційних, і стратегічно орієнтованою. Коли впроваджується процесний підхід, каталоги процесів і автоматичні потоки, СВК стає прозорішою, проте лишається здебільшого реактивною: вона бачить, що вже сталося, а не передбачає, що може статися і де виникнуть критичні відхилення. Тому необхідне переосмислення самої парадигми СВК.

Показовим орієнтиром є досвід Міністерства оборони (з 2025 р. перейменованого адміністрацією чинного президента США Д. Трампа на «Міністерство війни») США, де функціонує Advana – єдина суцільна платформа даних, аналізу та прогнозування із застосуванням ШІ [1]. Відповідно до відкритих джерел 2021 року, Advana об'єднала понад 1200 систем в єдину корпоративну аналітичну платформу, що інтегрує дані з фінансів, інфраструктури, контрактів та інших сфер [8]. Завдяки Advana вдалося суттєво скоротити час на звітність, відстеження використання ресурсів і візуалізацію витрат. Використання ШІ-рішень дає можливість візуально об'єднувати дані з різних джерел, створювати гнучкі дашборди та впроваджувати вбудовані моделі прогнозування. Практично, Advana вже використовується не лише для фінансових даних, а й у сценаріях оперативного управління, що відображає трансформацію платформи з інструменту звітності в інструмент стратегічного контролю, планування і прогнозування.


ISSN: 3041-2110

У відповідь на зростаючу технічну складність платформи та потребу у прискоренні впровадження ШІ, у США вирішили провести радикальну реорганізацію Advana. Заступник секретаря оборони Стівен Фейнберг підписав меморандум від 9 січня 2026 року, за яким фінансові дані Advana виокремлюються в окремий блок «Advana for financial management», паралельно створюється «War Data Platform» для підтримки бойових та розвідувальних завдань [9]. Новий формат показує перезапуск системи контролю як стратегічного інструменту, де фінансовий аудит, воєнні операції та розвиток ШІ керуються з єдиної, але спеціалізованої інформаційно-аналітичної архітектури, що забезпечує вищий рівень контролю, гнучкості та аудитабельності.

Розглядаючи Advana функціонально, можна констатувати, що вона збирає фінансову, контрактну, логістичну та іншу інформацію, перетворюючи її на корисні висновки для управління ризиками, зниження витрат і підвищення готовності. Advana демонструє, що перехід до «СВК 2.0» в МО України має не лише автоматизувати процеси, а створити єдину базу даних і аналізу – одне достовірне джерело даних для фінансів, закупівель, логістики, кадрів. Система автоматично виявляє аномалії, ризики постачальників, відхилення від планів і перенавантаження ресурсів, а також аналізує середньоринкові ціни на товари та послуги. Для МО України такий підхід означає необхідність відмовитися від розрізнених ізольованих автоматизацій і створити цілісну оборонну аналітичну платформу, що об'єднує IT-системи фінансів, закупівель, логістики, кадрів і внутрішнього аудиту. Вбудована аналітика, моделі ризику і ШІ виявлятимуть зловживання і слабкі місця до того, як вони переростуть у кризу [8, 9, 16].

«СВК 2.0» перетворюється із поточного інструменту звітності на стратегічний інформаційний механізм планування, контролю та забезпечення доброчесності в умовах війни та мирного часу. Модель процесно-орієнтованої цифрової системи доброчесності (Integrity-by-Design Model) змінює контроль

з реактивного на превентивний. Антикорупційні механізми «вшиваються» у процеси шляхом їхньої інтеграції через повну автоматизацію та інтелектуальний аналіз процесів. Система візуалізує етапи процесів (від заявки до акту) та блокує відхилення на мікрокроках, замість існуючого нині «функціонального» підходу і паперового формалізму.

Процесний підхід у моделі «СВК 2.0» вирішує важливу проблему існуючої СВК МО України – проблему функціональних «колодязів», тобто ізольованості відділів, коли кожен займається своїми справами, але ніхто не бачить всього процесу в цілому. Це є причиною втрати часу, помилок і виникнення можливостей для зловживань. Процесний підхід, на відміну від цього, звертає увагу на весь шлях операції від початку до завершення та передбачає чітко визначеного власника процесу, який несе відповідальність за результати й ефективність, спирається на встановлені KPI та прагне їх покращувати. Окрім цього, процесний підхід передбачає застосування матриці RACI, де в процесі чітко визначені ролі осіб, задіяних на кожному етапі.

Основна інструментальна база – технологія інтелектуального аналізу процесів (process mining). Ця технологія автоматично збирає дані з усіх цифрових баз даних міністерства – журналів ERP, реєстрів закупівель ProZorro тощо – і будує візуальну карту реальних процесів, показує цифровий слід, демонструє реальний рух документів, затримки та несанкціоновані обходи правил [10]. Система миттєво позначає відхилення від стандартного регламенту. Такий підхід перетворює контроль з окремої перевірки на вбудовану частину самого процесу: кожен крок автоматично порівнюється з узгодженими правилами; якщо щось не відповідає – процес блокується або ескалюється на рівень керівника.

Подолання формалізму в СВК МО України передбачає перехід до принципу, за яким порушити правила не є вигідним. Замість перевірки документів після їх створення контроль вбудовується в процес їх створення. Наприклад, закупівля палива для Збройних Сил України розбивається на

кілька послідовних кроків: подання заявки, її затвердження, вибір постачальника, підписання акта приймання і лише потім здійснення оплати. Ці кроки не мають бути зосереджені в одних руках, а повинні бути розподілені між кількома особами за принципом «чотирьох очей». Такий підхід усуває конфлікт інтересів і маніпуляції, які ховаються за формальними підписами.

Технологія розподілених реєстрів, зокрема на основі Hyperledger Fabric [17], адаптована для МО України, створює незмінний цифровий слід. Кожен підпис, кожна зміна, кожне рішення фіксуються з датою, часом і автором у захищеному журналі, який неможливо підробити або видалити. При перевірці або судовому розгляді цей слід стає чітким доказом і скорочує час розслідування з місяців до годин. Відповідальність стає невідворотною, що робить корупційні дії економічно та правово невигідними.

Інженерні рішення реалізуються через смарт-робочі процеси. Система автоматично формує стандартні документи – заявку чи акт – за введеними даними, а посадовець лише перевіряє і підписує. Електронний підпис нового покоління доповнюється біометрією (розпізнавання обличчя або відбитка) та геолокацією через мобільний пристрій – підписати акт приймання товару на складі в м. Харкові, перебуваючи у м. Києві, стає технічно неможливим. Аналіз великих даних за допомогою ШІ виявляє підозрілу поведінку: підпис за кілька секунд на складний документ, нічну активність, шаблонні помилки. При виявленні аномалії система надсилає повідомлення аудиторам МО України, що забезпечує превентивний контроль без зайвого бюрократичного навантаження.

Для МО України підхід Advana означає, що «СВК 2.0» перетворить складні і перевантажені методики, формалізовані у незліченній кількості наказів МО України, на впорядкований і передбачуваний інструмент. Платформа стає інформаційним засобом для планування оборони, кращого управління ресурсами та прозорості під час війни. Посадові особи та керівники структурних підрозділів опиняться у «прозорому та яскраво освітленому

просторі», де зловживання стають невигідними, оскільки внутрішній аудит МО України зможе в реальному часі фіксувати ознаки недоброчесності окремих посадових осіб та своєчасно надавати відповідну оцінку.

**Висновки.** Проведений аналіз засвідчує, що існуюча СВК в МО України та в державному секторі в цілому характеризується низьким рівнем ефективності і потребує термінового переосмислення своєї ролі. Кращі практики функціонування СВК демонструють стрімкий розвиток цифрових рішень, які не просто роблять процеси ефективнішими, але й здешевлюють та прискорюють внутрішній аудит, роблять його ризик-орієнтованим, а не контрольно-ревізійним із постфактумним принципом роботи.

Аналіз показав, що поточна СВК не відповідає очікуванням партнерів України та громадянського суспільства. Війна з росією на виснаження, швидка інтеграція до євроатлантичних структур і обмеженість ресурсів зумовлюють ситуацію, за якої доброчесність в управлінні оборонним сектором стає не лише моральною нормою, але й реальним чинником безпеки та сили України.

Цифровізація в МО України має бути не просто інструментом економії, а головним засобом, що робить управлінські процеси чесними. Досвід США (платформа Advana), НАТО і кращих корпорацій показує, що перехід до автоматизованого управління на основі Big Data, ШІ і процесного підходу покращує прозорість, підвищує ефективність і значно знижує корупційні ризики. В Україні необхідно відмовитися від окремих «інформаційних колодязів» і локальних автоматизацій. Потрібна цілісна оборонна аналітична платформа, що об’єднує фінанси, закупівлі, логістику, кадрові та аудиторські системи в єдину систему управління ризиками.

Це потребує повного перезапуску – «СВК 2.0» в МО України, що створить суспільний резонанс та підвищить рівень довіри до оборонного сектору, оскільки масштабні корупційні скандали під час війни використовуються ворогом в інформаційних атаках на наше суспільство, послаблюючи мобілізаційну готовність України.


ISSN: 3041-2110

Внутрішній аудит МО України, при впровадженні такої платформи, здобуде спроможність окреслювати підвищену ризикованість конкретної операції в ланцюжку процесу та розробляти рекомендації щодо запобігання подібним ситуаціям у майбутньому, підвищуючи цінність МО України відповідно до міжнародних стандартів внутрішнього аудиту.

Принципова здійсненність такої платформи не викликає сумнівів: МО України вже спроможне створювати й офіційно використовувати надзвичайно складні та ефективні цифрові платформи, як-от «DELTA», що підвищує ситуаційну обізнаність командирів на всіх рівнях до показників, які вважалися малоймовірними до повномасштабної війни. Аналогія очевидна: МО України нагально необхідна платформа ситуаційної обізнаності в русі ресурсів з метою забезпечення максимального ефекту їх кінцевого застосування.

## Список використаних джерел

1. Advana // Chief Digital and Artificial Intelligence Office. URL: https://www.ai.mil/Initiatives/Analytic-Tools/ (дата звернення: 30.01.2026).

2. NSPA Procurement Operating Instruction (OI 4200-01) // NATO Support and Procurement Agency. 2024. 27 Mar. URL: https://www.nspa.nato.int/resources/site1/General/business/procurement/General-information/OI-4200-01-EN.pdf (дата звернення: 30.01.2026).

3. Бойко А. А. Аналіз нормативно-правової бази, що регламентує питання організації системи внутрішнього контролю у Міністерстві оборони України та підпорядкованих установах. Social Development and Security. 2025. Т. 15, № 1. С. 214–226. DOI: 10.33445/sds.2025.15.1.20. URL: https://paperssds.eu/index.php/JSPSDS/article/download/815/981 (дата звернення: 30.01.2026).

4. Юрченко А. М. Проблемні аспекти вдосконалення внутрішнього контролю в органах державної влади в сучасній Україні. Право та публічне управління. 2025. Вип. 1. С. 296-304. DOI: 10.32782/pdu.2025.1.41

5. Лойшин А. А. Обґрунтування рекомендацій з оцінки ефективності системи внутрішнього контролю установи Міністерства оборони України: дис. ... д-ра філос. Київ, 2023. URL: https://nuou.org.ua/assets/dissertations/diser/diser-loishyn.pdf (дата звернення: 30.01.2026).

6. Лойшин А. О. Проблематика функціонування державного внутрішнього фінансового контролю в Україні. Social Development and Security. 2022. Т. 12, № 4. С. 27–36. DOI: 10.33445/sds.2022.12.4.4. URL: https://paperssds.eu/index.php/JSPSDS/article/download/463/550 (дата звернення: 30.01.2026).

7. Слободяник С. П. Концептуальні підходи до формування критеріїв оцінювання ефективності системи внутрішнього контролю в Міністерстві оборони України. Social Development and Security. 2021. Т. 11, № 3. С. 162–178. DOI: 10.33445/sds.2021.11.3.16. URL: https://paperssds.eu/index.php/JSPSDS/article/download/339/391/ (дата звернення: 30.01.2026).

8. Lin G. Meet Advana: How the Department of Defense Solved its Data Interoperability Challenges // Government Technology Insider. 2021. 6 Apr. URL: https://governmenttechnologyinsider.com/meet-advana-how-the-department-of-defense-solved-its-data-interoperability-challenges/ (дата звернення: 30.01.2026).

9. Perez L. Pentagon to Split Advana Data Platform // MeriTalk. 2026. 15 Jan. URL: https://www.meritalk.com/articles/pentagon-to-split-advana-data-platform/ (дата звернення: 30.01.2026).

10. van der Aalst W. M. P. Process Mining: Data Science in Action. 2nd ed. Berlin: Springer, 2016. 467 p. DOI: 10.1007/978-3-662-49851-4. URL: https://link.springer.com/book/10.1007/978-3-662-49851-4 (дата звернення: 30.01.2026).

11. Звіт Аудиторської Ради Ukraine Facility акцентує необхідність посилення ролі внутрішнього контролю і внутрішнього аудиту і ролі НАЗК //

Національне агентство з питань запобігання корупції. 2025. 11 груд. URL: https://nazk.gov.ua/uk/novyny/zvit-audytorskoi-rady-uf-aktsentue-neobhidnist-posylennya-roli-vnutrishnogo-kontrolyu-i-vnutrishnogo-audytu-i-roli-nazk/ (дата звернення: 30.01.2026).

12. Внутрішній аудит ефективності: методичні засади та практичні аспекти: посібник / Міністерство фінансів України. Київ, 2022. 104 с. URL: https://www.mof.gov.ua/storage/files/project_vn_audit_efect.pdf (дата звернення: 30.01.2026).

13. Стан внутрішнього аудиту в Україні: зрілість управління проти дефіциту ресурсів // Інститут внутрішніх аудиторів України. 2026. 31 січ. URL: https://theiia.org.ua/2026/01/31/stan-vnutrishnogo-audytu-v-ukrayini-zrilist-upravlinnya-proty-deficzytu-resursiv/ (дата звернення: 30.01.2026).

14. Вплив зовнішнього та внутрішнього аудитів на формування системи внутрішнього контролю державних органів: матеріали круглого столу / Рахункова палата України. Київ, 2025. URL: https://rp.gov.ua/PressCenter/News/?id=2842 (дата звернення: 30.01.2026).

15. Деякі питання впровадження процесного підходу в центральних органах виконавчої влади: постанова Кабінету Міністрів України від 17 січ. 2025 р. № 50. URL: https://www.kmu.gov.ua/npas/deiaki-pytannia-vprovadzhennia-protsesnoho-pidkhodu-v-tsentralnykh-orhanakh-vykonavchoi-vlady-i170125-50 (дата звернення: 30.01.2026).

16. The Siemens Compliance System: Prevent — Detect — Respond and Continuous Improvement / Siemens AG. Basel: Basel Institute on Governance, 2019. URL: https://baselgovernance.org/sites/default/files/2019-02/compliance_system_en.pdf (дата звернення: 30.01.2026).

17. Introduction to Blockchain // Hyperledger Fabric Documentation. URL: https://hyperledger-fabric.readthedocs.io/en/latest/blockchain.html (дата звернення: 30.01.2026).