

Закалад М. А. (ORCID 0000-0002-0624-4140);
Беляченко В. В. (ORCID 0000-0003-3938-5158);
Мулявка А. С. (ORCID (0000-0002-3113-0719)

Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняхівського, Київ

Підходи до організації управління ризиками впровадження Єдиної інформаційної системи управління оборонними ресурсами

Резюме: У статті на підставі досвіду реалізації проектів впровадження автоматизованих систем, зокрема, в секторі безпеки та оборони країн НАТО, розглянуто вагомі ризики впровадження. Окреслено підходи до визначення змісту заходів з оброблення ризиків, які необхідно внести в плани управління ризиками зацікавлених сторін під час впровадження Єдиної інформаційної системи управління оборонними ресурсами Збройних Сил України.

Ключеві слова: ризики проектів; ЄІСУ оборонними ресурсами; план управління ризиками.

Постановка проблеми. Кількість автоматизованих систем (АС) або їх окремих складових, які фрагментарно відповідають оперативно-стратегічним вимогам до АС “Управління логістичним забезпеченням” Збройних Сил України і успішно доведені до стадії прийняття на озброєння та експлуатації незначна (Логістично-інформаційна система LIS, Система управління складом (WMS), Майно та житло, МедЕвак), хоча роботи в цьому напрямі ведуться багато років. Діяльність з управління проектами впровадження АС не є повсякденною та унормованою для Міністерства оборони України та Збройних Сил України, що пояснює недостатній рівень системності заходів щодо управління ризиками на всіх стадіях створення АС. Із зростанням складності проектів, збільшується кількість суб’єктів – зацікавлених сторін, що впливають на задум, процес і завершення проектів, – задача управління ризиками ускладнюється, підвищується рівень невизначеності на усіх стадіях проекту, що вимагає створення планів управління ризиками на кожний проект окремо і на портфель проектів загалом.

Завдання управління ризиками проектної діяльності у відомчій нормативній базі залишається нерегульованим відповідно до рекомендацій ДСТУ, міжнародних стандартів і рекомендацій усталених світових практик управління проектами і, відповідно, не має систематичної методичної підтримки. Однією з причин неповного охоплення відомчою нормативною базою ризиків проектної діяльності під час впровадження АС є те, що ця діяльність не є профільною для Міністерства оборони України та Збройних Сил України. Гальмування впровадження

Єдиної автоматизованої системи управління (ЄАСУ) ЗС України, Єдиної інформаційної системи управління (ЄІСУ) оборонними ресурсами та відповідної інформаційної інфраструктури окрім інших чинників ресурсного та зовнішнього характеру пояснюється також і тривалим періодом конкуренції концептуальних підходів і поглядів на склад і шляхи побудови інформаційної архітектури та фрагментарністю дій замовників і виконавців щодо управління ризиками проектів впровадження АС.

Кожний етап життєвого циклу АС потребує тісної взаємодії представників МО України та ЗС України, виконавців проектних робіт зі створення АС. Із зростанням кількості суб’єктів системи управління життєвим циклом АС, які розробляються на замовлення МО України в рамках дослідно-конструкторських робіт, що можуть вплинути на задум, процес і завершення проектів ЄАСУ ЗС України, ЄІСУ оборонними ресурсами та інформаційної інфраструктури – задача управління ризиками проектів ускладнюється, взаємозалежність проектних процесів посилюється, рівень невизначеності підвищується на усіх стадіях проекту, що потребує створення планів профілактичних заходів на кожний проект окремо і на портфель проектів загалом.

АС, створювані на замовлення МО України та ЗС України, нині перебувають на різних стадіях життєвого циклу, що зумовлює різницю рівнів технологічної зрілості. Розроблення здійснювались на різноманітних програмних платформах, які змінюються і морально застарівають швидше, ніж зразок АС доводиться до стадії створення КСЗІ та прийяття на озброєння. Виникають

також ускладнення з ресурсним забезпеченням супроводу АС з боку виконавців через неможливість комерціалізації розробки та її тиражування, що призводить до значних витрат на супровід. Усі ці чинники значно ускладнюють завдання досягнення інтегрованості між АС, що вже прийняті на озброєння і які готуються для прийняття.

Зміни змісту робіт (процедур), перерозподіл ролей та повноважень учасників процесів, які змінюються внаслідок інформатизації, потребує також заходів із залучення учасників процесів до проектів інформатизації до того, як АС перейде від стадії розроблення до стадії впровадження та експлуатації. Витрати на залучення учасників процесів як експертного середовища на стадіях концептуального проектування, розроблення та випробувань значно менші, ніж витрати на виправлення відхилень чи невідповідностей АС на стадії експлуатації. Щоб уникнути гальмування створення ЄІСУ оборонними ресурсами необхідно врахувати вже існуючий світовий досвід типових ризиків, які можуть призвести до виникнення проблем.

Аналіз останніх досліджень і публікацій свідчить про актуальність проблеми гальмувань, зупинок і провалів проектів впровадження АС, зокрема в секторі безпеки і оборони, через неврахування проектних ризиків. Одним з найвідоміших прикладів невдалих проектів впровадження АС був проект ВПС США з розроблення системи підтримки експедиційних бойових дій (ECSS Expeditionary Combat Support System) з багатомільярдними витратами згідно зі звітом Рахункової палати уряду США (United States Government Accountability

Office) [1] щодо поточного статусу проектів впровадження ERP-систем у Збройних силах США. Мета проекту ВПС США полягала у створенні єдиної уніфікованої системи управління логістикою та ланцюгами постачання, яка давала змогу відстежувати всі матеріальні активи та ефективніше заощаджувала витрати ресурсів. Проект почався в 2004 р. та був призупинений в 2012 р. без досягнення своєї мети. Велика кількість проблемних і неуспішних проектів впровадження АС, втрати часу і ресурсів, змусили замовників і виконавців проектів уважно поставитись до питання управління проектними ризиками, відпрацьовувати стандарти з управління ризиками і впроваджувати в свою діяльність обґрунтовані практики управління проектами.

Корпус відомчої нормативної бази МО України щодо управління ризиками станом на 01 липня 2019 року охоплює виключно ризики фінансово-господарської повсякденної діяльності структур МО України та ЗС України, використовує як концептуальну основу рекомендації ДСТУ ISO 31000:2013 Ризик менеджмент [2-6].

Метою статті є визначення чинників, що можуть вплинути на проект, обґрунтування підходів до змісту профілактичних заходів з оброблення ризиків, що стосуються наукових відомств, замовника та виконавців і формулювання пропозицій.

Виклад основного матеріалу. Управління ризиками проекту включає процеси, пов'язані з проведенням планування, ідентифікації, аналізу, реакцій, моніторингу і контролю управління ризиками проекту (рис. 1). Більшість цих процесів оновлюється під час проекту.



Рис. 1. Управління ризиками проекту

Системне управління ризиками проекту – один з фундаментальних чинників гарантування успіху проекту. Отже важливо якомога раніше встановити механізм

управління ризиками як частину загального плану проекту. Аналіз, моніторинг і контроль ризиків повинен стосуватись усіх зацікавлених сторін проекту. Документація має включати:

ідентифікацію зацікавлених сторін, політику управління ризиками, реєстр ідентифікованих ризиків та їх класифікацію з боку усіх зацікавлених сторін проекту, переліки заходів оброблення ризиків усіма зацікавленими сторонами, ідентифікацію, аналіз та перелік

профілактичних дій на кожній стадії проекту, план заходів контролю та моніторингу, план дій на випадок настання ризиків та план дій, що сприяють підвищенню впливу факторів успіху.

Ризики можна класифікувати таким чином, як наведено у табл. 1.

Таблиця 1

Класифікація ризиків	
РИЗИК	ХАРАКТЕРИСТИКА РИЗИКУ
Нечіткість цілей	Багато великих проектів не вдаються через нечіткість формулювання проблем, чи неформалізовані вимоги. У проєкті беруть участь багато учасників (архітектори, менеджери ризиків, операційні керівники) кожен з яких має власне бачення АС. Після нескінченних дискусій і втрати часу на пошуки компромісів підсумковий документ містить розпливчасті нечіткі цілі (вимоги), розмиті обсяги проєкту і, як наслідок, неадекватне проєктування архітектури.
Надмірний оптимізм	Під час представлення замовнику прикладів успішного використання АС постачальники і продавці програмних, апаратних платформ та консалтингових послуг через об'єктивний конфлікт інтересів максимізують прибутки та вигоди і мінімізують оцінки ризиків проєктів інформаційних систем та витрати, щоб довести замовнику можливість швидкого досягнення ефективності та результативності без ґрунтовного врахування поточних вимог та умов діяльності замовника. Окрім того, необ'єктивність виконавців щодо продуктивності власних виробничих потужностей призводить до нереалістичності графіків впровадження, надмірної віри в технології, недооцінки складності програмно-апаратних рішень
Складність	Великі ІТ-проєкти мають високу ступінь складності внаслідок використання нових технологій, інтерфейсів з іншими системами, необхідності імпорту та трансформації даних, вимог замовників щодо підтримки "старих" процесів, конкуренції проєктної команди за ресурси з іншими проєктами, що все разом значно збільшує вплив та імовірності ризиків проєктів. Процеси стають нестійкими через намагання членів проєктної групи подолати ускладнення за стислий час і недокументованими засобами і методами, що у підсумку призводить до виходу проєктних процесів з під контроль, до зменшення якості, зсуву планових термінів та перевищення бюджету
Необґрунтовано швидке впровадження АС	Зазвичай для скорочення строків впровадження виконавці штучно обмежують функціональність системи. Проте, якщо надати перевагу швидкості реалізації в стилі Agile шляхом нехтування детальністю проєктування, заощадження на інноваційності та надійності і технологічності програмної платформи, то ризики появи численних помилок програмної реалізації або недосягнення АС необхідного рівня продуктивності значно зростають. На практиці у разі швидкого початку робіт із впровадження дослідного зразка АС на базі нашвидкуруч зібраного макету без попередніх експериментальних випробувань у стресовому режимі, може виникнути необхідність у масштабних виправленнях, внаслідок чого плановий бюджет і терміни реалізації проєкту перевищується і економія на "швидкому впровадженні" зникає
Слабке спонсорство	Великі проєкти часто мають декілька зацікавлених сторін або центрів ухвалення рішень зі своїми власними цілями та програмами. Керівники мають різні очікування щодо переваг і варіантів проєкту, які можуть бути несумісними цілком або частково. Жоден з керівників не повністю підтримує чи супроводжує проєкт, і в таких проєктах бракує ефективного куратора-суперспонсора, відповідального за цілі та вигоди проєкту загалом, який може узгоджувати суперечливі вимоги або бути арбітром, який ухвалює підсумкове рішення щодо суперечливих вимог
Ускладнене управління	Надмірність використання інструментарію управління проєктами і надмірна бюрократія, яка затримує управління змінами в організації через численні узгодження запитів із менеджерами змін, менеджерами ризиків, менеджерами з якості, архітекторами рішень, проєктними менеджерами, експертами з проєктних методологій, аудиторами, менеджерами з корпоративної відповідності – є перегином у спробі досягти найвищих показників якості. Формальне дотримання практик проєктного менеджменту, витрати часу на форми, звітності, показники замість результативної роботи над пошуком програмно-технічних рішень вимог замовника, що збільшує вартість проєкту до того ж не додаючи цінності замовнику
Чинник менеджера проєкту (недостатні професійні та лідерські якості)	Менеджер проєкту має знати предмет, галузеву специфіку замовника і вміти збалансувати потреби проєкту з потребами якісного управління за допомогою правильної методології в потрібних та адекватних обсягах. Окрім того, менеджер проєкту мусить уникати замовчування ризиків та проблем задля тверезого погляду на статус проєкту та вжиття запобіжних заходів для його вирівнювання. Варто також залучати зовнішніх експертів для оцінки статусу проєкту і звертатись за необхідності до спонсора проєкту для ухвалення дій

РИЗИК	ХАРАКТЕРИСТИКА РИЗИКУ
Нераціональна економія ресурсів	Фінансисти або менеджери іноді затримують виділення ресурсів на тій або іншій стадії проекту заради оптимізації витрат. Насправді будь-які затримки у фінансуванні та реалізації стратегічних програм збільшують приховані витрати на період затримки проекту. У випадку з проектом, що передбачає комплексну інтеграцію, від прихованих витрат страждає не тільки функціональна сфера що підлягає автоматизації, а уся організація загалом. Наприклад, для організації, яка згідно з техніко-економічним обґрунтуванням проекту мала отримати економію в розмірі 1,2 млрд грн на рік, щомісячна затримка введення системи в експлуатацію буде коштувати 100 млн грн витрат, яких можна було б уникнути

У процесі аналізу проблем створення ЄІСУ оборонними ресурсами, виявилось, зокрема, що вони є наслідком необґрунтованої квапливості замовника, недостатнього ресурсного забезпечення виконавця, невиконання рекомендацій науково-технічного супроводження у повному обсязі та несистемне і фрагментарне використання практик проектного менеджменту. Зміст проектних документів внаслідок квапливості виявляється недостатньо опрацьованим. Практики проектного менеджменту в процесах проектної діяльності використовуються вибірково та формально. Ставлення до робіт з документування проектних процесів як до зайвих і бюрократичних робіт, що потребують ресурсів і часу також призводить до втрати можливості контролю показників процесу проекту. Наприклад, відсутність Статуту проекту призводить до нечіткості формалізованих цілей і пріоритетів проекту, розмиванню прав та відповідальності усіх зацікавлених сторін, яке не виправляється лише відомчими наказами та державним

контрактом з виконавцем, поверхневому та неповному визначенню робіт на всіх стадіях: на початковому етапі функціонального моделювання та макетування, на стадіях реалізації налаштувань, проведення інтеграційних випробувань і дослідної експлуатації та введення в постійну експлуатацію. Відсутність чітких показників призводить до гальмування досягнення мети створення АС і збільшує ймовірність появи проектних помилок з перевитратою бюджету та перевищенням термінів.

Про важливість створення системи управління ризиками проектної діяльності в сфері створення інформаційних систем свідчить світова статистика успішності, часткової успішності та неуспішності проектів.

Згідно з аналізом даних про статус понад 50 тис. ІТ-проектів, проведеного міжнародною дослідною компанією Standish Group до 2015 року виявилось, що в категоріях “дуже великих” і “великих” ІТ-проектів успішними є лише 8 % (2 % + 6 %), а проблемними 24 % (7 % + 17 %), і припиненими 41 % (17 % + 24 %) (рис. 2). [6]

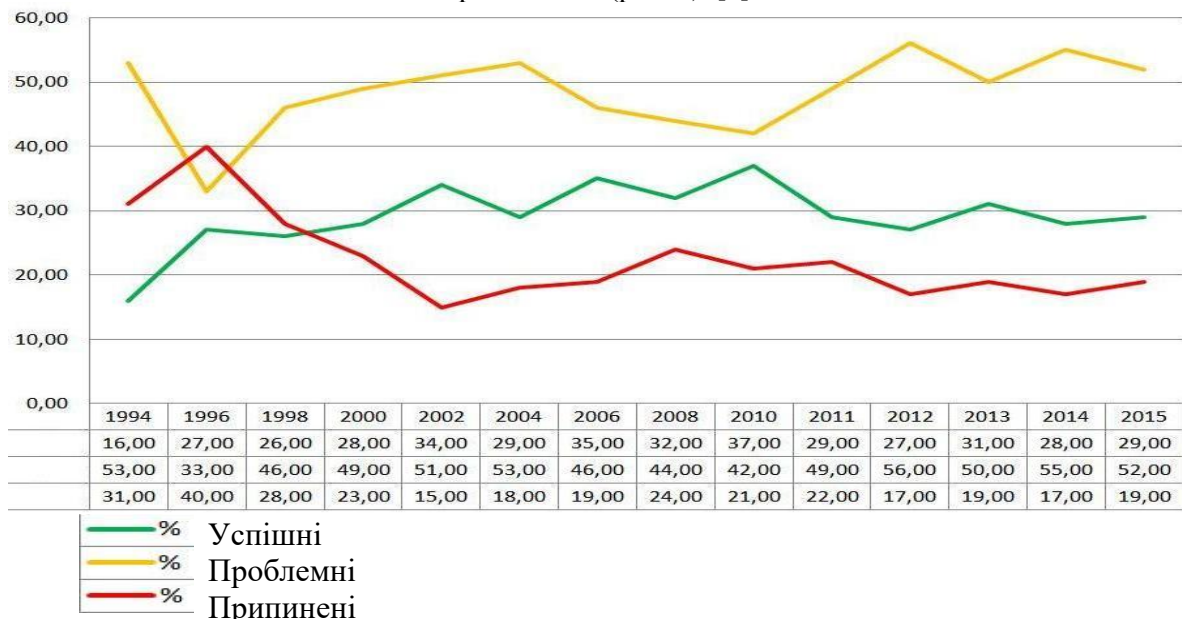


Рис. 2. Дані Standish Group по успішності ІТ-проектів усіх “вагових” категорій з 1994 до 2015 рік

Ці чинники провалу виявились у проекті оборонного аналізу США щодо оцінки ERP-систем для оборонного сектору, в якому вказані експедиційних бойових дій, що зазначено у звіті 2012 року, підготовленому Інститутом

оборонного аналізу США щодо оцінки ERP-систем для оборонного сектору, в якому вказані виявлені дослідниками проблеми, пов'язані з проектом створення управління логістикою в

ВПС США, а також з іншими впровадженнями систем на базі ERP [7]:

нехтування існуючою базовою практикою проєктів та ігнорування ефективних заходів для досягнення бажаних результатів;

структура військової організації та її спрямованість на операційні можливості, а не на фінансовий результат, означали, що використання систем, спроектованих для організацій спрямованих на одержання прибутку, було малоприсадибним для військової організації;

ієрархічні структури прийняття рішень в збройних силах були погано узгоджені з структурою управління проєктом, що виявлялось в тому, що функціональні спонсори (рушії змін) були іноді нижчими за рангом, ніж ті начальники, підрозділи яких піддавались змінам;

необхідність наскрізної інтеграції функцій через організаційні кордони та нездатність створити структуру управління на досить високому рівні для подолання цих кордонів;

брак довіри між групами (емоційна незрілість);

небажання адаптувати операційні процеси відповідно до можливостей програмного забезпечення (гальмування реінжинірингу);

звичка військовослужбовців доповідати в стилі “можемо-зробимо!” призвела до створення видимості нормального процесу проєкту та приховування проблем через відсутність прозорості справжнього статусу проєкту;

зосередження уваги на розкладі та бюджеті призвело до недостатньої уваги до фактичних результатів діяльності проєкту, внаслідок чого питання, що пов’язані з якістю, відправляються “під сукно”;

проєкт розглядався виключно як ІТ-проєкт, а не як проєкт трансформації організації;

інші ідентифіковані чинники провалу проєкту у ВПС США: неефективна структура та процес управління проєктом; невдалий вибір базового програмного забезпечення, який не відповідав меті та вимогам проєкту;

недостатність досвіду команди проєкту щодо розроблення та впровадження складних інтегрованих систем у великих масштабах; “кругова порука” у діяльності персоналу; неефективне залучення до роботи всіх зацікавлених сторін; брак співпраці всередині команди проєкту та брак розуміння керівництва як управляти змінами; власники процесів не були ідентифіковані; постійна зміна складу команди проєкту.

Приклади ідентифікованих видів проєктних ризиків і рекомендовані заходи щодо зменшення або розподілу ризику згідно зі стандартами внутрішнього контролю, прийнятих в МО України наведені у табл. 2.

Необхідно також планувати заходи, що збільшують впливовість чинників успіху. У Табл. 4 наведено ідентифіковані ключові чинники успіху та їх ранжування згідно зі світовою практикою станом на 2015 рік [13].

Для забезпечення успіху проєкту та запобігання виникненню проблем через ігнорування та/або недооцінку заходів із забезпечення якості у всіх учасників проєкту та зацікавлених сторін, а також заходів, передбачених планами управління ризиками на всіх стадіях життєвого циклу системи необхідно створювати змішані проєктні групи у складі представників оборонного відомства, представників наукових відомств та представників виконавця із залученням за необхідності зовнішніх постачальників послуг та обладнання:

Для ідентифікації та ранжування ризиків (Табл. 3) корисними є дані статистики типових чинників виникнення проблем станом на 2014 рік під час реалізації проєктів впровадження ІТ на усіх стадіях життєвого циклу інформаційної системи [12].

апаратного устаткування, стандартного та спеціального програмного забезпечення;

послуг з налаштування та доопрацювання АСУ в процесі дослідиної експлуатації, навчання персоналу;

систем захисту інформації та інших аспектів, властивих динамічно змінюваним АСУ;

експертних послуг з оцінювання систем якості, систем ризик-менеджменту тощо.

Заходи за стандартами внутрішнього контролю

№	ПЕРЕЛІК РИЗИКІВ	ЗАХОДИ ЩОДО ЗМЕНШЕННЯ
1	Помилки в підборі кадрів з боку зацікавлених сторін щодо розробників, архітекторів, адміністраторів і кінцевих користувачів. Непідготовленість кінцевих користувачів до зміни технології управління процесами	Кадрові ризики Кваліфікаційні вимоги на стадії вибору Виконавця. Кваліфікаційні вимоги на стадії вибору персоналу Замовника, який братиме участь у роботі проектної групи. Створення центрів компетенції організаціями зацікавленими сторін. Підвищення кваліфікації учасників проектних груп та вищого керівництва зацікавлених сторін у сфері проектного менеджменту та, зокрема, ризик-менеджменту
		Корупційні ризики Введення (або підвищення кваліфікації штатних спеціалістів) до штату підрозділу з координації внутрішнього контролю Міністерства оборони України та підрозділу з координації внутрішнього контролю Генерального штабу спеціалістів з управління корупційними ризиками в проектній діяльності. Розроблення регламенту з управління проектом та його гармонізація з міжнародними стандартами та перевіреними практиками проектного менеджменту, у т.ч. галузевого спрямування (наприклад, PMI:PMBoK Guide; PMI:Practice Standard for Project Risk Management; NASA:The Orange Book – Risk Management Handbook; The Association for Project Management (APM): Project Risk Analysis and Management (PRAM Guide), Workbook APM Body of Knowledge (6 edition) [8-11] Залучення менеджерів проектів, що мають досвід управління проектами, знання процесів властивих для об'єкта впровадження АС та пройшли навчання і сертифікацію
3	Невідповідність проектних документів вимогам ДСТУ, ISO та відомчих нормативних документів. Ризики недотримання вимог законодавства України та інших країн, які стосуються (наприклад) прав інтелектуальної власності	Нормативно-правові ризики Підготовка проектних документів, що дотримуються вимог міжнародних стандартів, ДСТУ [14-24], стандартів країн-членів НАТО (AAP-20, AAP-48, AQAPx) та шаблонів концептуальних проектів, запропонованих виробником інформаційної системи. Залучення до розробки проектних документів спеціалістів зі знанням стандартів
		Операційно-технологічні ризики Створення центрів компетенції в предметній області. Дотримання регламенту керування змінами згідно проектної документації. Навчання персоналу та проектної групи методикам управління проектами [8-11] Співробітники підрозділів, на яких може вплинути впровадження АС, мають бути підключені до роботи над проектом і поінформовані про зміни процесів. Вимоги, пропонувані підрозділами, мають бути по можливості простими. Дотримання принципу залучення “перших керівників” до управління проектом, як головних зацікавлених осіб
4	Необґрунтовані зміни порядку виконання проектних завдань, переускладнення вимог, конфігурування множинних рішень. Невиділення представників Замовника до вироблення проектних рішень. Неоперативність прийняття рішень керівництвом Замовника.	Програмно-технічні ризики Дотримання регламенту впровадження СПЗ Навчання персоналу та проектної групи. Дотримання вимог виробника інформаційної системи щодо використання стандартних засобів розроблення. Внесення відповідних кваліфікаційних вимог на стадії вибору СПЗ. Використання для створення АС програмних платформ, перевірених застосуванням в збройних силах країн-членів НАТО
		Репутаційні ризики Внесення відповідних вимог на стадії вибору СПЗ. Навчання персоналу та проектної групи методики управління проектами
5	Невикористання програмних і технічних засобів забезпечення впровадження АС, які передбачено методикою впровадження та ігнорування вимог спеціального програмного забезпечення (надалі СПЗ) до апаратної платформи, наприклад, невикористання стандартних засобів розроблення, наданих виробником. Загрози кібербезпеці (використання програмних кодів походженням з країни-агресора, неналежний контроль розробок з погляду створення зловмисних програмних закладок). Невідповідність можливостей АС в стані повної проектної потужності та функціональності вимогам замовника	Фінансово-господарські ризики Планування бюджету в обсягах та термінах надходження, обґрунтованих масштабом ризиків для національної безпеки, які необхідно зменшити через надання засобами ЄІСУ оборонними ресурсами своєчасної, повної, достовірної, захищеної інформації замовнику.
		Фінансово-господарські ризики Планування бюджету в обсягах та термінах надходження, обґрунтованих масштабом ризиків для національної безпеки, які необхідно зменшити через надання засобами ЄІСУ оборонними ресурсами своєчасної, повної, достовірної, захищеної інформації замовнику.
6	Використання СПЗ постачальників/розробників з недостатнім рівнем підтримки галузевого рішення, або з наявністю програмного коду розробленого спеціалістами країни-агресора. Неповна професійна відповідність керівництва проектом з боку виконавця та/або з боку замовника	Фінансово-господарські ризики Планування бюджету в обсягах та термінах надходження, обґрунтованих масштабом ризиків для національної безпеки, які необхідно зменшити через надання засобами ЄІСУ оборонними ресурсами своєчасної, повної, достовірної, захищеної інформації замовнику.
		Фінансово-господарські ризики Планування бюджету в обсягах та термінах надходження, обґрунтованих масштабом ризиків для національної безпеки, які необхідно зменшити через надання засобами ЄІСУ оборонними ресурсами своєчасної, повної, достовірної, захищеної інформації замовнику.
7	Ненадання потрібних видів ресурсів, зменшення обсягів ресурсів, або несвоєчасність надходження	Фінансово-господарські ризики Планування бюджету в обсягах та термінах надходження, обґрунтованих масштабом ризиків для національної безпеки, які необхідно зменшити через надання засобами ЄІСУ оборонними ресурсами своєчасної, повної, достовірної, захищеної інформації замовнику.
		Фінансово-господарські ризики Планування бюджету в обсягах та термінах надходження, обґрунтованих масштабом ризиків для національної безпеки, які необхідно зменшити через надання засобами ЄІСУ оборонними ресурсами своєчасної, повної, достовірної, захищеної інформації замовнику.

Таблиця 3

Ранжування ризиків		
№	РИЗИК	%
1	Незалучення користувачів до проєкту	12,8
2	Неповнота вимог та специфікацій	12,3
3	Зміна вимог та специфікацій	11,8
4	Відсутність підтримки з боку керівництва	7,5
5	Невідповідність технології	7,0
6	Брак ресурсів	6,4
7	Нереалістичні очікування	5,9
8	Нечіткі цілі	5,3
9	Нереалістичні часові обмеження	4,3
10	Нові технології	3,7
11	Інші чинники	23,0

Практична цінність побудови системи управління ризиками значно зменшує масштаби втрат організації у разі настання подій, передбачених як ідентифікований ризик і щодо яких розроблено профілактичні заходи та сценарії реагування, підвищує стійкість організації у разі непередбачуваних подій та збільшує ймовірність настання подій, які є сприятливими для досягнення цілей організації. Окрім цього, система управління ризиками надає організації безпосередні переваги [11]:

більш поінформовані та надійні плани, графіки та бюджети;

збільшені шанси на успіх проєкту;

сприяє оптимізації типу контракту;

можливість більш повноцінного оцінювання та обґрунтування непередбачених обставин;

перешкоджає прийняттю фінансово недієздатних проєктів;

створює показники для використання в майбутніх проєктах;

дає змогу об'єктивного порівняння альтернатив;

визначає та розподіляє відповідальність на кращого власника ризику.

Окрім безпосередніх переваг систематичне управління ризиками сприяє загальному підвищенню рівня зрілості організації її керованості та стійкості, завдяки таким ефектам:

покрощує корпоративний досвід і загальне спілкування;

призводить до спільного розуміння та вдосконалення командного духу;

допомагає розрізняти вдале/гарне управління та невдале/погане управління;

допомагає розвивати компетентність та здатність персоналу оцінювати ризики;

фокусує увагу керівництва проєкту на реальних і найважливіших питаннях;

полегшує прийняття ризику через

Таблиця 4

Ключові чинники успіху		
№	ЧИННИКИ УСПІХУ	%
1	Підтримка з боку керівництва	15
2	Емоційна зрілість (членів груп)	15
3	Залучення користувачів	15
4	Оптимізація вимог	15
5	Кваліфікований персонал	10
6	Управління середовищем стандартних практик, сервісів і програмних рішень	8
7	Гнучкість проєктних команд, процесів, рішень	7
8	Помірне використання інструментів управління проєктами	6
9	Управління проєктами на експертному рівні	5
10	Чіткі ділові цілі	4

збільшення потенційних вигод;

демонструє професійний та відповідальний підхід до зацікавлених сторін; забезпечує свіжий погляд на кадрові питання в проєкті.

Для запобігання небажаного впливу на хід, результативність, ефективність проєктних робіт на всіх стадіях розроблення АС необхідно:

з боку наукових відомств надавати виконавцям та замовникам методичну допомогу щодо інтеграції в процеси дій та документів, передбачених процесами управління ризиками згідно відомчих нормативних документів, актуальних ДСТУ та рекомендацій ISO [14-24];

виконавцям і замовникам використовувати статистичні дані щодо вагомості факторів успіху та враховувати причини невдалих проєктів для планування профілактичних заходів у планах управління проєктами згідно з політикою організацій щодо оброблення ризиків;

представникам наукових відомств, визначених як організації, що здійснюють науково-технічне супроводження ДКР у сфері створення АС, ознайомлюватись з результатами моніторингу та результатами реагування виконавця та замовника на ризики, пропонувати дії з покращення управління ризиками та орієнтовний зміст заходів щодо забезпечення успішності проєкту в напрямках, визначених як критично важливі для врахування в планах управління ризиками;

розробити навчальні програми, конспекти лекцій для Вищих академічних курсів підвищення кваліфікації та професійного рівня Національного університету оборони України імені Івана Черняховського з питань управління проєктами у сфері інформатизації, зокрема щодо управління ризиками для членів проєктних груп, користувачів та керівного

складу;

у планах управління проектом усіх зацікавлених сторін передбачити виділення ресурсів на навчання персоналу проектних груп методології управління ризиками для подолання недооцінки важливості системи управління ризиками, для кращого розуміння вразливості організацій до певних видів ризиків і необхідності прозорості щодо ризиків, до яких схильна та чи інша сторона і для отримання вигод від впровадження системи управління ризиками.

Висновки. У статті наведено приклади та конкретні напрями для врахування ризиків і можливостей, які необхідно враховувати під час складання планів з управління ризиками зацікавленими сторонами у процесі проекту створення ЄІСУ оборонними ресурсам. доповнити існуючу відомчу нормативну базу з управління ризиками нормативними документами з порядку організації проектного менеджменту, зокрема в сфері управління ризиками, які мають передбачати і заходи з аудитів управління ризиками і аудит інформаційних технологій та кібербезпеки.

Подальші дослідження необхідно спрямувати на відпрацювання ранжування ризиків для підготовки типових шаблонів постадійних планів управління ризиками під час створення АС у секторі безпеки і оборони, підготовку змісту навчальних програм для підвищення кваліфікації учасників проектів з боку замовника та обґрунтування вимог до програмних засобів підтримки проектної діяльності з боку замовника.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Report to Congressional Requesters “Dod Business Transformation. Improved Management Oversight of Business System Modernization Efforts Needed” United States Government Accountability Office (US GAO) [Електронний ресурс] – Режим доступу: <https://www.gao.gov/new.items/d1153.pdf>
2. Стандарти внутрішнього контролю в Міністерстві оборони України та Збройних Силах України [Електронний ресурс] – Режим доступу: http://www.mil.gov.ua/content/pdf/vnytr_control/Internal%20Control%20Standards_ukr.pdf.
3. Наказ Генерального штабу Збройних Сил України № 340 від 29.08.2016 “Про затвердження Інструкції з організації внутрішнього контролю у Збройних Силах України” [Електронний ресурс] – Режим доступу: http://www.mil.gov.ua/content/pdf/vnytr_control/nakaz_340.pdf.
4. Тимчасовий порядок організації внутрішнього контролю та управління ризиками у Міністерстві оборони України і Збройних Силах України № 3551/з/5-2017 від 13.08.2018 [Електронний

ресурс] – Режим доступу: <http://www.mil.gov.ua/content/finance/arrangement-of-internal-control-and-risk-management-in-the-Mod.pdf>.

5. Наказ Міністерства оборони України № 145 від 02.04.2019 “Про затвердження Порядку організації в системі Міністерства оборони України внутрішнього контролю та управління ризиками” [Електронний ресурс] – Режим доступу: http://www.mil.gov.ua/content/pdf/vnytr_control/n145_020419.pdf.
6. А. М. Тимофеев “Картина стабільного кризиса”. Інтернет-журнал “Практика проектирования систем” (июнь 2017). [Електронний ресурс] – Режим доступу: <https://reqcenter.pro/why-it-fails/>.
7. Institute for Defense Analyses “Assessment of DoD Enterprise Resource Planning Business Systems” [Електронний ресурс] – Режим доступу: <https://apps.dtic.mil/dtic/tr/fulltext/u2/a563798.pdf>.
8. Project Management Institute – PMBoK Guide 2000 edition [Електронний ресурс] – Режим доступу: <http://www.cs.bilkent.edu.tr/~cagatay/cs413/PMBoK.pdf>.
9. PMI – Practice Standard for project risk management [Електронний ресурс] – Режим доступу: <http://www.innovativeprojectguide.com/documents/PMIPracticeStandardforProjectRiskManagement.pdf>.
10. NASA. The Orange Book – Risk Management Handbook (2011) [Електронний ресурс] – Режим доступу: <https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20120000033.pdf>.
11. Workbook based on the APM Body of Knowledge (BoK) Version 6 [Електронний ресурс] – Режим доступу: <https://www.qa.com/Courseware/PCW/PCW-APMP-3.pdf>.
12. Project Smart. The Standish Group Report (digest) 2014. [Електронний ресурс] – Режим доступу: <https://www.projectsmaart.co.uk/white-papers/chaos-report.pdf>.
13. Standish Group 2015 Chaos Report – Q&A with Jennifer Lynch [Електронний ресурс] – Режим доступу: <https://www.infoq.com/articles/standish-chaos-2015/>.
14. ДСТУ 4302:2004 Інформаційні технології. Настанови щодо документування комп’ютерних програм (ISO/IEC 6592:2000 MOD). – Надано чинності 30 квітня 2004 р. – К. : Держспоживстандарт України, 2007. – 30 с.
15. ДСТУ ISO 10006:2005. Системи управління якістю. Настанови щодо управління якістю в проектах: (ISO 10006:2003, IDT). – Надано чинності 1 серпня 2007 р. – К. Держспоживстандарт України, 2007. – IV, 27 с.
16. ДСТУ ISO/IEC 12207:2016 – Інженерія систем і програмного забезпечення. Процеси життєвого циклу програмного забезпечення: (ISO/IEC 12207:2008, IDT). – Надано чинності 27 грудня 2016 р. – К. ДП “УкрНДНЦ”, 2018. – 98 с.
17. ДСТУ ISO/IEC/IEEE 15288:2016 – Інженерія систем і програмного забезпечення. Процеси життєвого циклу систем. (ISO/IEC/IEEE 15288:2015, IDT). – Надано чинності 27 грудня 2016 р. – К. ДП “УкрНДНЦ”, 2018. – 84 с.

18. ДСТУ ISO/IEC 15289:2014 - Інженерія систем і програмного забезпечення. Контент життєвого циклу інформаційної продукції (документації): (ISO/IEC 15289:2011). – Надано чинності методом підтвердження від 30 грудня 2014 р.
19. ДСТУ ISO/IEC 16085:2016 – Інженерія систем і програмних засобів. Процеси життєвого циклу. Керування ризиками: (ISO/IEC 16085:2006, IDT). – Надано чинності 27 грудня 2016 р. – К. ДП “УкрНДНЦ”, 2018. – 34 с.
20. ДСТУ ISO/IEC/IEEE 16326:2015 – Розроблення систем та програмного забезпечення. Процеси життєвого циклу. Керування проектами: (ISO/IEC/IEEE 16326:2009, IDT). – Надано чинності 18 грудня 2015 р. – К. ДП “УкрНДНЦ”, 2018. – 31 с.
21. ISO 21500:2012 Guidance on project management. International Organization for Standardization. [Електронний ресурс] – Режим доступу: <https://www.iso.org/standard/50003.html>
22. ДСТУ ISO/IEC 27005:2015 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки: (ISO/IEC 27005:2011, IDT). – Надано чинності методом підтвердження 18 грудня 2015 р. – К. ДП “УкрНДНЦ”, 2016. – 65 с.
23. ДСТУ ISO 31000:2018 Менеджмент ризиків. Принципи та настанови: (ISO 31000:2018, IDT). – Надано чинності методом підтвердження 29 листопада 2018 р. – К. ДП “УкрНДНЦ”, 2018.
24. ДСТУ IEC/ISO 31010:2013 Керування ризиком. Методи загального оцінювання ризику: (IEC/ISO 31010:2009, IDT). – Надано чинності 11 грудня 2013 р. – К. Мінекономрозвитку України, 2015. – 74 с.

Стаття надійшла до редакційної колегії 07.06.2019

Закалад Н. А.;
Беляченко В. В.;
Мулявка А. С.

Центр военно-стратегических исследований Национального университета обороны Украины имени Ивана Черняховского, Киев

Подходы к организации управления рисками внедрения Единой информационной системы управления оборонными ресурсами

Резюме: В статье на основании опыта реализации проектов внедрения автоматизированных систем, в частности, в секторе безопасности и обороны стран НАТО, рассмотрены весомые риски внедрения. Определены подходы к определению содержания мероприятий по обработке рисков, которые необходимо внести в планы управления рисками заинтересованных сторон при внедрении Единой информационной системы управления оборонными ресурсами Вооруженных Сил Украины.

Ключевые слова: риски проектов; ЕИСУ оборонными ресурсами; план управления рисками.

Zakalad M. A.;
Beliachenko V. V.;
Muliavka A. S.

Center for Military and Strategic Studies of the National Defense University of Ukraine named after Ivan Cherniakhovskyi, Kyiv

Development of information systems for the management of defense resources

Resume: In the article, based on the experience of implementation of automated systems projects, particularly in the defense sector of the NATO countries, significant risks of implementation are considered. The approaches to determining the content of risk management measures that need to be put in the risk management plans of stakeholders during the implementation of the Unified Information Management System of the Defense Resources of the Armed Forces of Ukraine are outlined.

Keywords: project risks; UIMS of defense resources; risk management plan.