КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (26), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.26.659
УДК 004.056

Байдур Олексій Володимирович
аспірант
Національний університет біоресурсів і природокористування України, Київ, Україна
Збройні Сили України, Київ, Україна
ORCID ID: 0000-0001-7036-1264
alexvb1981@gmail.com

КІЛЬКІСНА МЕТОДОЛОГІЯ ОЦІНКИ РИЗИКІВ КІБЕРБЕЗПЕКИ ПРИ ВІДСУТНОСТІ ФІНАНСОВИХ ДАНИХ ПРО ВТРАТИ

Анотація. Стаття присвячена актуальній проблемі оцінки ризиків кібербезпеки в інформаційно-комунікаційних системах військового призначення в умовах агресивної війни, коли неможливо оцінити потенційні збитки у грошовому еквіваленті та із враховуванням специфіки гібридних загроз. У вступі статті обговорюється актуальність проблеми та підкреслюється необхідність проактивної стратегії кібероборони, важливість своєчасної оцінки ризиків, особливо в умовах активного застосування противником кіберзброї. Особлива увага приділяється неможливості оцінити потенційні втрати від кібератак у грошовому еквіваленті, що зумовлює необхідність нових підходів до оцінки ризиків. Розділ «Особливості оцінки ризиків кібербезпеки ІКС ВП України» аналізує існуючі стандарти та методології, такі як стандарти групи ДСТУ ISO/IEC 27000, а також актуальні методології оцінки ризиків кібербезпеки та виявляє обмеження їх застосування в умовах ведення війни. В розділі підкреслюється важливість автоматизації процесу оцінки ризиків для забезпечення швидкої реакції на кіберзагрози. Розглядаються переваги кількісних моделей оцінки ризиків над якісними, особливо в контексті військових інформаційно-комунікаційних систем. У наступних розділах детально розглядаються ключові процеси оцінки ризиків згідно з ДСТУ ISO/IEC 27005:2023 та згідно актуальних методологій. Проводиться порівняльний аналіз методологій OCTAVE, NIST, COBIT, TARA та FAIR з точки зору їх придатності для потреб ЗСУ. Обговорюються переваги та недоліки кожної методології, та обґрунтовується необхідність розробки нової методології на основі OpenFAIR (відкритої версії методології FAIR), адаптованої до специфіки інформаційно-комунікаційних системах військового призначення та реалій гібридної війни. Результат досліджень представлений у вигляди діаграми діяльності алгоритму оцінки ризиків кібербезпеки в інформаційно-комунікаційних системах військового призначення та детальний опис цих кроків з акцентом на відмінності від методології OpenFAIR У розділі «Висновки» підводяться підсумки проведеної роботи і формуються пропозиції для подальших досліджень.

Ключові слова: інформаційні технології; кібербезпека; оцінка ризиків; гібридна війна; кількісна оцінка; ІКС військового призначення; війна у кіберпросторі.

ВСТУП

Початок повномасштабного вторгнення російської федерації на територію України був також і початком безперервних та багатовекторних кібератак на інформаційно-комунікаційні системи Збройних Сил України. Основною причиною цього стало те, що інформаційні технології та системи відіграють критичну роль у сучасних військових операціях, забезпечуючи зв’язок, розвідку та управління військами. В цьому контексті вони стають пріоритетною ціллю ворога, тому захист інформаційно-комунікаційних систем військового призначення (ІКС ВП) від кібератак є невід’ємною складовою національної безпеки України. Дослідники Фонду Карнегі за міжнародний мир [1] та

корпорації Microsoft [2] виділяють широкий спектр інструментів, що використовується російськими агентами кібервпливу, та щільну інтеграцію цих кібератак в загальну військову стратегію. Серед різноманітних методів кібервпливу є використання, як легальних додатків, так і шкідливого програмного забезпечення та бекдорів у піратському програмному забезпеченні. Наприклад, пов'язана з головним розвідувальним управлінням рф група Iridium, розробила бекдор інтегрований в піратські версії Microsoft Office з метою отримання доступу до робочих місць розгорнутих в українських державних установах та урядових організаціях [2]. Щодо інтеграції кібератак в загальні плани війни, то це супроводжується постійними намаганнями отримати доступ до військової інформації, спробами руйнування, нанесення максимальної шкоди інфраструктурі Україні та здійснення впливу на її інформаційних простір [1].

Постановка проблеми. В попередній роботі автора [3] були проаналізовані згадані вище особливості дій російських агентів кібервпливу. Висновок цієї статті звучить так, що в умовах інтенсивного застосування противником кіберзброї в комбінації із активними військовими діями пасивна стратегія кібероборони інформаційно-комунікаційних системах військового призначення (ІКС ВП) є недостатньою, а єдиним ефективним способом протидії є застосування проактивної стратегії кібероборони. Проактивна стратегія протидії кіберзагрозам вимагає розробки та впровадження систем, які в режимі реального часу будуть аналізувати кіберзагрози, оцінювати рівень захисту ІКС та виявляючи вразливості [4]. Відповідно до прийнятих в Україні міжнародних стандартів одним з перших і ключових кроків при розбудові системи управління інформаційною безпекою є управління ризиками та їх оцінка ризиків [5]. При цьому проактивна стратегія кібероборони передбачає автоматизацію і цього процесу. Саме своєчасна та адекватна оцінка ризиків (кіберзагроз) сприяє швидкому прийняттю рішень і є критично важливою для ефективної протидії ворогу у кіберпросторі у такому агресивному та швидкозмінному середовищі, як ІКС ВП в умовах ведення війни. Недооцінка загроз, наприклад таких як, використання піратського програмного забезпечення, несвоєчасне оновлення програмного забезпечення або несвоєчасне інформування про нові критичні вразливості може призвести до витоку чутливої інформації та/або несанкціонованого доступу до інформаційних систем. Особливістю ІКС ВП в умовах ведення війни і інтеграції кібератак в загальну військову стратегію є неможливість оцінити потенційний негативний економічний ефект від кібератаки ворога, що досягне часткового або повного успіху. Так тимчасове виведення з ладу ІКС ВП, що забезпечує роботу сил оборони країни, в комбінації із атакою проведеною на час виведення системи із ладу такою може призвести до значних руйнувань об'єктів критичної інфраструктури і масової загибелі людей, тому прорахувати сумарний об'єм фінансових втрат на етапі планування є неможливим. Водночас огляди методологій оцінки ризиків кібербезпеки останніх років [6] – [8] свідчать, що кількісні методології оцінки ризиків кібербезпеки спираються в основному на прагнення осіб, що приймають рішення по розбудові системи кібербезпеки, мінімізувати фінансові втрати від успішної кібератаки. Враховуючи викладене постає завдання створення або адоптації однієї з методологій оцінки ризиків кібербезпеки для потреб оцінки ризиків кібербезпеки в ІКС ВП, коли відомості про можливі фінансові втрати в разі успішної кібератаки неможливо сформувати.

Аналіз останніх досліджень і публікацій. Специфіка поставленого завдання, а саме орієнтація на системи військового призначення сильно звужує кількість матеріалів, що можливо знайти за цією тематикою у відкритому доступі. Однак перегляд відкритих джерел свідчить, що існує настанова Міністерства оборони США DoD Program Manager's

Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle [9], яка надає рекомендації по розбудові системи управління ризиками кібербезпеки саме в структурі міністерства оборони. Ця настанова спирається на стандарт NIST SP 800-37 Revision 2 [10], але має і свої відмінності від загальнофедерального підходу в США. В першу чергу це те, що вона застосовується не лише до інформаційних систем, а й до всіх інформаційних технологій (далі — ІТ), включаючи системи озброєння, системи управління підрозділами, розвідки. По-друге, при оцінці ризиків враховуються не лише стандартні фактори, такі як конфіденційність, цілісність та доступність даних, а й потенційний вплив кібератак на виконання військових завдань та боєготовність, при цьому процес управління ризиками кібербезпеки тісно інтегрований з процесом придбання ІТ систем у Міністерстві оборони США. В цьому контексті особлива увага приділяється забезпеченню стійкості систем до кібератак, тобто їх здатності протистояти, реагувати та відновлюватися після кіберінцидентів.

Перелічені особливості сприяють, з одного боку створенню більш ефективної та адаптивної системи управління ризиками кібербезпеки в Міністерстві оборони США, а з іншого роблять цю методологію невід'ємною частиною нормативно-правового поля США. При всіх перевагах цієї методології і її спрямованості на застосування саме в контексті систем військового призначення, у випадку із завданням розбудови системи управління ризиками в Україні її не можливо застосовувати без прийняття у якості відомчих стандартів цілого пакету пов'язаних документів. При чому, специфіка тестування і закупівлі ІТ систем для потреб Міністерства оборони США взагалі не може бути перенесена на український контекст у зв'язку із значними відмінностями національного законодавства. Враховуючи, що в України в якості державного стандарту управління ризиками кібербезпеки прийнятий саме ДСТУ ISO/IEC 27005:2023 прямий переніс вимог відповідних документів США не є доцільним. При цьому особливості саме військового спрямування згаданої настанови Міністерства оборони США слід приймати до уваги під час розробки методології оцінки ризиків кібербезпеки в ІКС ВП.

Мета статті. Метою цієї статі є розробка нового алгоритму оцінки ризиків кібербезпеки в інформаційно-комунікаційних системах військового призначення. Цей алгоритм має враховувати специфіку ІКС ВП, особливості гібридної війни, неможливість оцінити потенційні фінансові втрати внаслідок успішних кібератак, а також необхідність виконання вимог профільного державного стандарту України.

ОСОБЛИВОСТІ ОЦІНКИ РИЗИКІВ КІБЕРБЕЗПЕКИ В ІКС ВП УКРАЇНИ

В Україні основним керівництвом для розбудови захисту інформаційних систем є група міжнародних стандартів ISO/IEC 27000, яка описує методологію розбудови системи управління інформаційною безпекою на основі циклічного підходу, що включає планування, впровадження, виконання, перевірку та вдосконалення [11]. Є певна кількість методологій і декілька готових до використання програмних рішень, що реалізують процес оцінки ризиків у відповідності до цього стандарту. Так у статті авторів Isaac Daniel Sánchez-García, Jezreel Mejía та Tomás San Feliu Gilabert [12] проведений огляд і порівняння 35 інструментів оцінки ризиків з 40 первинних досліджень, опублікованих за останнє десятиліття. У цьому огляді описані також і інструменти, що автоматизують етап оцінки ризиків кібербезпеки. Ці інструменти можна умовно поділити на дві окремі групи, які орієнтовані на використання якісних та кількісних

моделей відповідно. Це дослідження показало, що більшість експертів використовують якісні інструменти, але віддають перевагу кількісним [12].

Слід зазначити, що інструменти якісної оцінки переважно орієнтовані на отримання експертної думки, що ставить швидкість виконання оцінки в пряму залежність від швидкості реакції експерта-людини і є неприйнятним, коли за мету ставиться досягнення максимально швидкої реакції на зміну вхідних параметрів. Попередньо сформоване завдання здійснювати оцінку (переоцінку) ризиків в умовах агресивного і швидкозмінного середовища змушує концентруватися саме на методиках кількісної оцінки ризиків, що спираються на математичні моделі і оперують чітко визначеними числовими показниками. Це дозволяє значно зменшити час реакції автоматизованого інструменту оцінки ризиків на зміну вхідних параметрів та зменшити залежність оцінки від рівня компетентності експертів — людей. Інструмент, що використовує кількісну оцінку ризиків здатних провести оцінки (переоцінки) ризиків одразу, коли буде зафіксована поява нової кіберзагрози або зміна статистичних даних по вже відомим загрозам. Це допоможе оперативно застосувати найбільш ефективні контрзаходи та зосередити зусилля на захисті найбільш вразливих активів. В умовах ведення агресивної війни в кіберпросторі усталені корпоративні практики з періодичністю оцінки (переоцінки) ризиків кібербезпеки до декількох разів на рік не можуть бути прийнятими.

Перейдемо до розгляду моделей з кількісною оцінкою ризиків. Подібні моделі наведені в статтях, як закордонних [13] – [15], так і українських авторів [16], [17] зазвичай орієнтовані на визначення величини потенційних збитків у разі успішної кібератаки, що є зручним інструментом при плануванні суми витрат на організацію кіберзахисту комерційних систем, так і об’єктів критичної інфраструктури, але є неприйнятним для планування кіберзахисту ІКС ВП. Неможливо реально оцінити збитки, що може нанести ворожа ракета, яка досягне цілей внаслідок відмови ІКС відповідальної за роботу систем протиповітряної оборони, так само як і не можливо оцінити збитки, які може нанести проникнення ворога в систему, що відповідальна за визначення цілей для ураження артилерією. Всі ці приклади свідчать, що в у разі активного збройного протистояння для оцінки наслідків втрати працездатності систем, що забезпечують бойову роботу, неможливо використовувати загально прийняту практику оцінки потенційних втрат від настання події передбаченої ризиком кібербезпеки у грошовому еквіваленті.

У підсумку можна стверджувати, що методології, що були проаналізовані в статтях [13] – [17] не відповідають вимогам до процесу оцінки ризиків в ІКС ВП. Так, дійсно, специфіка сфери застосування знижує вірогідність знайти у вільному доступі готову методологію оцінки ризиків орієнтовану на ІКС військового призначення, а враховуючи унікальний масштаб та інтенсивність застосування агресором кіберзброї з моменту повномасштабного вторгнення російської федерації в Україну є маловірогідним, що необхідна методологія взагалі існує. Тому доцільною є розробка методології, що буде орієнтованої з одного боку на діючу в України групу галузевих стандартів ISO/IEC 27000, а з другого на досягнення кінцевої мети у вигляді створення автоматизованої системи оцінки ризиками, що адаптована для потреб організації кіберзахисту ІКС ВП. В основу цієї методології слід покласти визнані сучасні кількісні методології, що мають бути адаптовані до специфіки застосування. Ця специфіка породжує наступні вимоги:

1. Оцінка ризиків має бути кількісною з використанням математичної моделі, що дає можливість здійснювати перерахунок оцінок в реальному часі при зміні вхідних даних;

2. Результатом кількісної оцінки має бути прогнозований параметр, що дозволить прийняти обґрунтоване рішення по вибору ефективних контрзаходів наявним загрозам та технічним рішенням з організації системи кіберзахисту ІКС ВП.

ОЦІНКА РИЗИКІВ ЗГІДНО СТАНДАРТУ ДСТУ ISO/IEC 27005:2023

Як вже було зазначено оцінка ризиків в ІКС ВП має в цілому відповідати вимогам, що встановлює стандарт ДСТУ ISO/IEC 27005:2023 «Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки» [18], який відповідає міжнародному стандарту ISO/IEC 27005:2022. З метою визначення ключових процесів оцінки ризиків, що можуть бути автоматизовані, побудуємо діаграму діяльності яку передбачає стандарт (рис. 1).

Перший наведений на діаграмі крок — це «Встановлення контексту». Він передбачає визначення обсягу та меж управління ризиками, визначення критеріїв ризику, визначення методології оцінки ризиків. Цей крок виконується на етапі розробки і впровадження ІКС і не може бути повною мірою автоматизований, так як на цьому кроці необхідно встановити стратегічні цілі, встановити загальний внутрішній та зовнішній контекст організації та вимоги керівних документів. Водночас, у відповідності до стандарту цей крок в ітераційному циклі повторюється тільки при зміні контексту та/або виявленні нових ризиків, тому не існує потреби у здійсненні цього кроку в режимі реального часу.

Другий крок — це «Оцінка ризиків», що поділяється на ідентифікацію ризиків (визначення активів, загроз та вразливостей), аналіз ризиків (оцінка ймовірності та впливу ризиків) та оцінювання ризиків (порівняння з критеріями ризику та пріоретизація). Саме на цьому кроці відбуваються розрахунки, які можуть бути виконані в автоматизованій системі. При чому ітерації в межах стандарту передбачають повторення цього кроку до того моменту, поки ризики не будуть визнані прийнятними. З цього випливає висновок, що вимоги стандарту по виконанню цього кроку і мають бути закладеними в алгоритм оцінки ризиків кібербезпеки ІКС ВП.

Третій крок передбачений стандартом — це «Обробка ризиків», що передбачає вибір варіантів обробки ризиків (визначення стратегії реагування на ризики — це зниження, уникнення, передача або прийняття), визначення та впровадження заходів контролю (застосування заходів для зниження ризиків до прийнятного рівня) та оцінку залишкових ризиків (перевірка ефективності заходів контролю та визначення рівня ризику, що залишився). На цьому кроці можливо повноцінно автоматизувати тільки оцінку залишкових ризиків і є очевидним, що в цілому ця оцінка відповідатиме тій, що була проведена на попередньому кроці.

ISSN 2663 - 4023

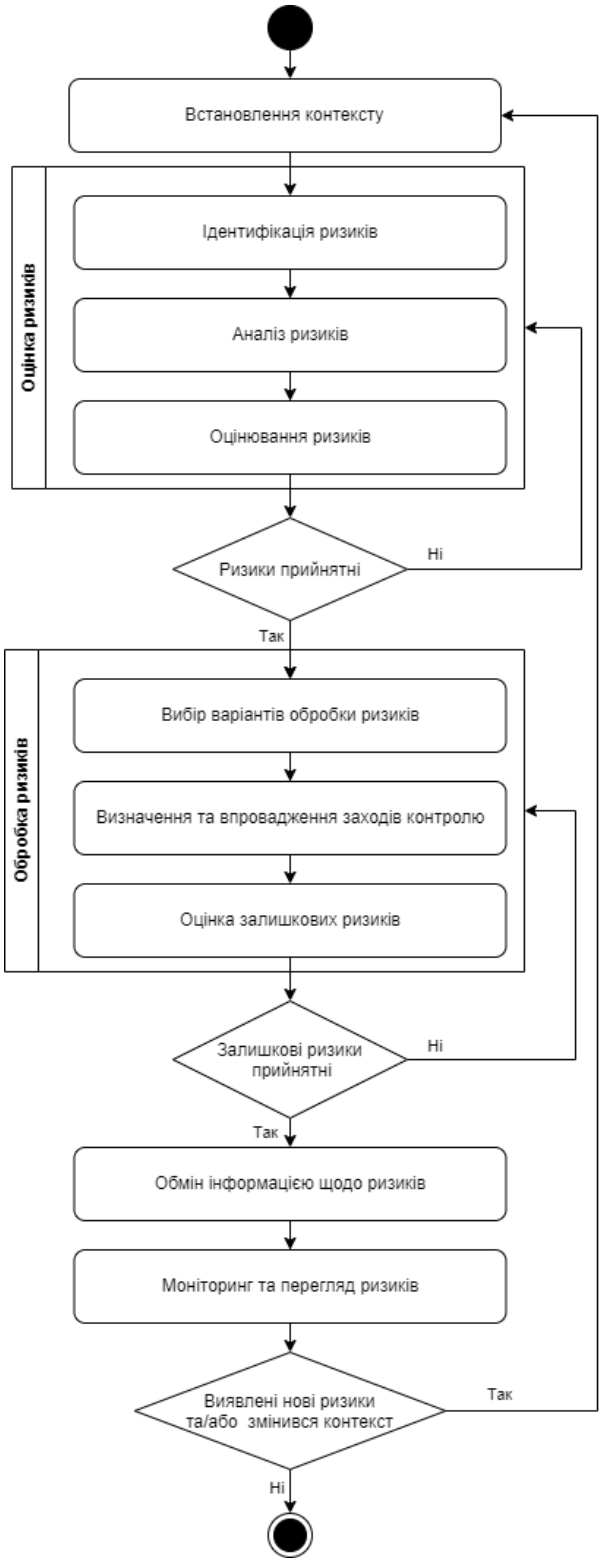

Рис. 1. Діаграма діяльності ISO/IEC 27005

Подальші кроки стандарту передбачають прийняття ризиків (прийняття обґрунтованих рішень щодо ризиків, які не можуть бути повністю усунені або знижені), кроки «Обмін інформацією щодо ризиків» (комунікація з відповідними сторонами про виявлені ризики, їх оцінку та обрані заходи контролю) та «Моніторинг та перегляд ризиків»

(постійне відстеження ризиків, оцінка ефективності заходів контролю та оновлення плану управління ризиками за потреби). Автоматизація цих кроків можлива, але має здійснюватися після того як виконані всі попередні передбачені стандартом заходи.

Слід окремо виділити кроки де відбувається оцінка залишкових ризиків і повторення процесу у разі, якщо ризики визнані не прийнятними. Це очевидно є закладеною в алгоритми адаптивністю розбудованої системи захисти під зміни безпекового середовища. У випадку швидкоплинності безпекових змін і критичної залежності загального стану кіберзахисту від можливості негайної адаптації до цих змін слід зосередитися на автоматизації саме другого кроку передбаченого стандартом ДСТУ ISO/IEC 27005:2023, а саме на оцінці ризиків. При цьому подальший розвиток перспективної системи оцінки ризиків в ІКС ЗСУ можливий за допомогою автоматизації кроків прийняття ризиків, обміну інформацією щодо ризиків та перегляду ризиків.

ОЦІНКА РИЗИКІВ КІБЕРБЕЗПЕКИ ВІДПОВІДНО ДО МЕТОДОЛОГІЙ

Зрозуміло, що стандарт не розкриває конкретні кроки по оцінці ризиків кібербезпеки, а тільки встановлюють загальні вимоги до організації цього процесу. На практиці для деталізації процесу використовуються методології, що відповідають стандарту. Серед визнаних і поширених методологій оцінки ризиків кібербезпеки автори оглядів [12] – [14] виділяють наступні:

OCTAVE — це методологія академічного спрямування, розроблена Університетом Карнегі-Меллона [19];

NIST — це урядова методологія США, розроблена Національним інститутом стандартів і технологій [10];

COBIT — методологія, розроблена ISACA для управління IT-процесами [17];

TARA — методологія, розроблена CERT Coordination Center для оцінки ризиків IT-систем [20];

FAIR — методологія, розроблена The Open Group для кількісної оцінки ризиків [21].

Розглянемо ці методології з метою вибору основи для створення алгоритму оцінки ризиків кібербезпеки.

Методологія OCTAVE і її варіації, такі як OCTAVE Allegro [22], OCTAVE S [23] вимагають залучення експертів — людей, хоча всі вони і розроблені для самостійного проведення організацією, їх успішне виконання залежить від участі персоналу з різних рівнів організації, включаючи керівництво, менеджерів операційних областей та технічних фахівців. Саме знання та досвід залученого персоналу є критичними для виявлення ключових активів, оцінки загроз та вразливостей, а також розробки ефективної стратегії захисту. OCTAVE надає переважно якісні оцінки, хоча вони можуть мати деякі кількісні елементи. Наприклад, активи оцінюються за їх відносною цінністю (висока, середня, низька), а ймовірність загроз оцінюється якісно (висока, середня, низька). Наведені особливості цієї методології не дозволяють її використати для оцінки ризиків в ІКС ВП, так система побудована на базі цієї методології не буде здатна проводити переоцінку ризиків в реальному часі, тому подальшій її розгляд не є доцільним.

Методологія на основі групи стандартів NIST, що вже була згадана в контексті існування спеціалізованої настанови Міністерства оборони США спирається на стандарт NIST SP 800-37 Revision 2 [10] та пропонує гнучку структуру, яка дозволяє адаптувати процес оцінки ризиків до потреб організації. Розглянемо діаграму діяльності згідно цієї методології, що спільно із іншими профільними документами (рис. 2).

ISSN 2663 - 4023

На першому кроці «Підготовка» розробляється план управління ризиками безпеки та конфіденційністю, визначаються межі системи та її середовища, створюється команда для впровадження системи управління ризиками та визнаються ролі в ній та розподіл відповідальності. Цей крок також включає визначення ключових зацікавлених сторін та їх очікувань і збір документації та інформації про систему.

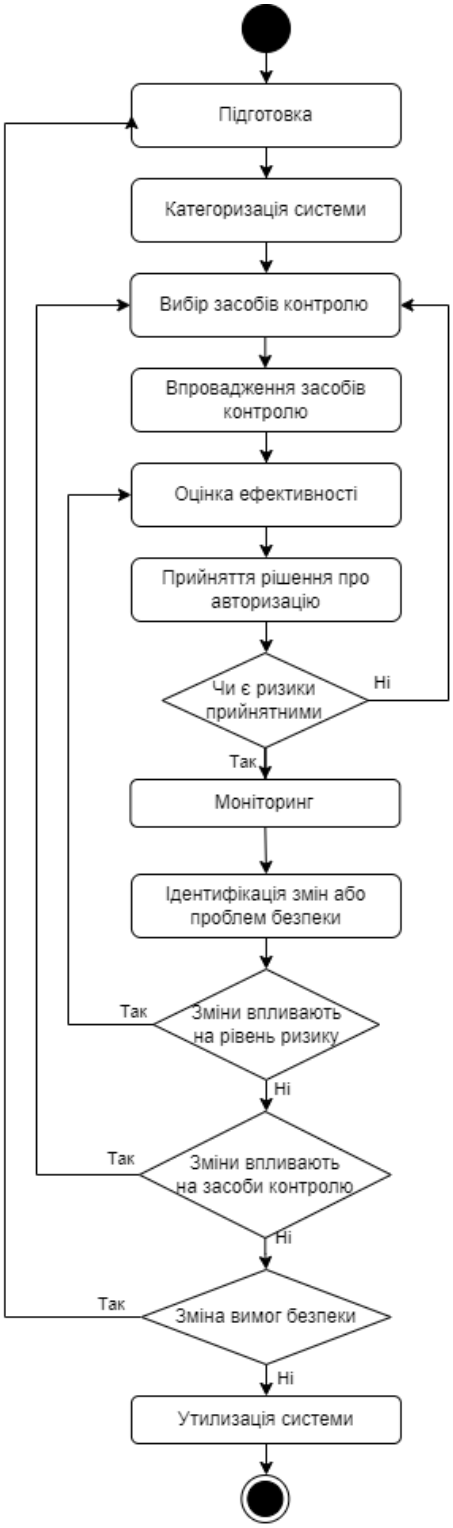

Рис. 2. Діаграма діяльності по NIST SP 800-37

Другий крок «Категоризація системи», виконується з метою визначити рівень впливу системи на безпеку та конфіденційність, щоб вибрати відповідні засоби контролю. Під час цього кроку визначається рівень потенційного впливу на конфіденційність (високий, помірний або низький) на основі типу оброблюваної інформації, рівень потенційного впливу на безпеку (високий, помірний або низький) на основі критичності системи для виконання місії організації та документування результатів категоризації з обґрунтуванням прийнятих рішень.

На третьому кроці «Вибір засобів контролю» використовуються затверджені каталоги засобів контролю безпеки та конфіденційності (наприклад, NIST SP 800-53, NIST SP 800-66), що відповідають рівням впливу на безпеку та конфіденційність, визначеним на етапі категоризації, та документування вибору.

Четверний крок «Впровадження засобів контролю» передбачає розробку детального плану впровадження, встановлення та налаштування засобів контролю в системі, а також тестування впроваджених засобів і оновлення документації системи.

На кроці «Оцінка ефективності» проводиться оцінки безпеки та конфіденційності з використанням різних методів оцінки (наприклад, тестування на проникнення, аналіз вразливостей, аудит) під час якої проходить документування результатів оцінки та виявлених недоліків та розробляється план дій щодо усунення виявлених недоліків.

Крок «Прийняття рішення про авторизацію» передбачає прийняття рішення про прийнятність залишкового ризику та надати дозволу (або відмови) на експлуатацію системи. Якщо ризик визнано неприйнятним, то слід повторно повернутися до кроку «Вибір засобів контролю».

Кроки «Моніторинг» та «Ідентифікація змін або проблем з безпекою» передбачають впровадження процесів та інструментів для безперервного моніторингу зі збором та аналізом даних для виявлення потенційних загроз та вразливостей та проведення періодичних оцінок безпеки та конфіденційності з оновленням системи та її засобів контролю у відповідь на зміни в середовищі або виявлені ризики відповідно.

Процес управління ризиками згідно NIST SP 800-37 Revision 2 є ітеративним і кроки можуть повторюватися. Наприклад, якщо під час моніторингу виявляються зміни, що впливають на рівень риску, то процес повертається до «Оцінка ефективності», у разі впливу на засоби контролю повторно виконується «Вибір засобів контролю», а якщо змінюються вимоги безпеки, то весь процес проводиться з першого кроку.

Однією із ключових відмінностей NIST SP 800-37 від ISO/IEC 27005 є виділення категоризації системи в окремий процес. Цей процес також присутній в стандарті ISO/IEC 27005, але він присутній неявно в кроці «Встановлення контексту». На категорізації системи, як окремому процесу також наголошується в загаданій настанові Міністерства оборони США і це в цілому відповідає вимогам керівних документів Державної служби спеціального зв'язку та захисту інформації України та Міністерства оборони України, тому, відповідно цей крок має бути відокремлений під час оцінки ризиків кібербезпеки ІКС ВП.

Далі розглянемо зрілі комерційні методології, які по суті своїй є універсальними в різних сценаріях застосування.

Методологія COBIT (Control Objectives for Information and Related Technology) [17] розроблена Асоціацією аудиту і контролю інформаційних систем (ISACA) розташованою в США призначена для управління та контролю інформаційних технологій (IT) в організаціях. Багато в чому вона базується на принципах методології FAIR, але надає більш комплексний підхід до управління IT, охоплюючи всі аспекти, від стратегії до операцій. COBIT орієнтована на бізнес так, як ставить потреби бізнесу на

перше місце маючи основним завданням узгодження IT-цілей організації зі стратегічними цілями бізнесу. COBIT є кількісною методологією та надає інструменти та метрики для вимірювання та моніторингу продуктивності IT, але ця методологія не є безкоштовною. ISACA пропонує різні публікації та ресурси COBIT, які зазвичай вимагають придбання ліцензії або членства в асоціації. При цьому, існує відкрита та безкоштовна версія методології, що надає доступ до основних концепцій та принципів COBIT. Це методологія OpenFAIR, яка буде розглянута пізніше.

Методологія TARA (Threat Assessment and Remediation Analysis) розроблена для виявлення та оцінки кіберзагроз, а також вибору ефективних контрзаходів для їх пом'якшення [20]. На відміну COBIT, що охоплює всі аспекти управління IT, від стратегії до операцій, TARA зосереджена конкретно на виявленні та пом'якшенні кіберзагроз. Так як і COBIT, TARA використовує FAIR як один з інструментів для оцінки ризиків, але також включає інші етапи, такі як визначення обсягу оцінки та вибір контрзаходів Вона включає два основні етапи, це преший етап — Оцінка вразливості до кіберзагроз (CTSA), що спрямований на виявлення та оцінку вразливостей системи до кібератак, та другий етап — Аналіз та усунення кіберризиків (CRRA), який орієнтований на вибір та оцінку контрзаходів для зниження вразливості системи, виявленої на етапі CTSA. Слід зазначити, що обидві розглянуті комерційні методології, як COBIT, так і TARA, в частині кількісної оцінки ризиків спираються на методологію FAIR, яка буде розглянутою наступною.

Методологія FAIR (Factor Analysis of Information Risk) забезпечує структурований і кількісний підхід до оцінки та управління інформаційними ризиками. Вона допомагає організаціям зрозуміти та кількісно оцінити ймовірність і величину потенційних втрат, пов'язаних із загрозами їх інформаційним активам [21]. При цьому FAIR є комерційною методологією, що вимагає ліцензування та оплати за використання. Водночас існує її безкоштовна версія Open FAIR, яка підтримується провідними компаніями IT-індуструї, такими як Intel, IBM та Fujitsu [24]. Враховуючи, що мета цієї статі — створити перспективний алгоритм автоматизованої оцінки ризиків в ІКС з можливістю його адаптації, з метою недопущення порушення умов ліцензування FAIR далі буде розглядатися діаграма діяльності згідно вільної версії методології (рис. 3), а саме OpenFAIR, як перспективна основа для вже згаданого алгоритму.

Перший крок діаграми діяльності по OpenFAIR це — «Ідентифікація сценарію втрат», що передбачає визначення активів, загроз (які можуть вплинути на активи) та типу втрат (наприклад, фінансові, репутаційні, операційні).

На другому кроці «Оцінка частоти втрат» спочатку визначається частота подій загроз, потім вразливість (це ймовірність того, що загроза призведе до втрат) та відбувається розрахунок частоти втрат, як комбінації частот загроз та вразливості.

Третій крок «Оцінка величини втрат» складається з визначення первинних втрат (це безпосередні фінансові втрати від інциденту), вторинних втрат (це непрямі втрати, такі як втрата репутації або продуктивності) та відбувається розрахунок величини втрат, як суми первинних та вторинних втрат.

ISSN 2663 - 4023

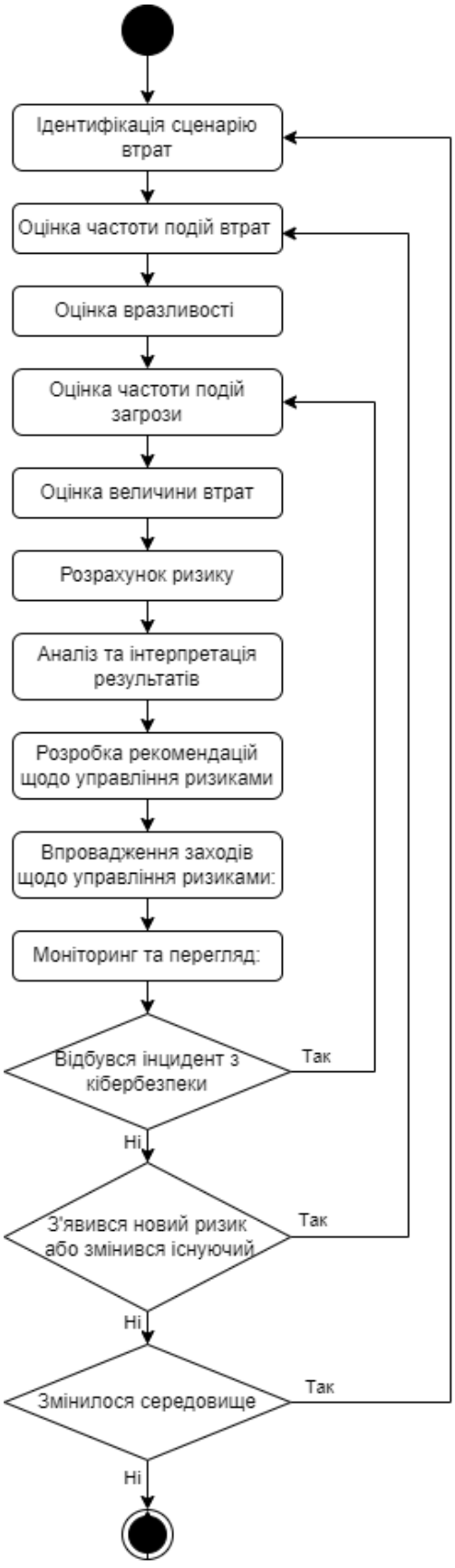

Рис. 3. Діаграма діяльності по OpenFAIR

Для виконання кроку «Розрахунок ризику» використовується модель Монте-Карло для моделювання різних сценаріїв на основі оцінок частоти та величини втрат з отриманням розподілу ймовірностей для ризику, вираженого у фінансових термінах.

Крок «Аналіз та звітування» складається з інтерпретації результатів моделювання з визначенням рівня ризику та створення звіту, містить ключові висновки та рекомендації щодо управління ризиком.

Останній крок діаграми «Управління ризиком» вимагає розробити та впровадити стратегії управління ризиком на основі результатів проведеного аналізу, а також регулярно переглядати та оновлювати оцінки ризиків, щоб враховувати зміни в середовищі.

Методологія OpenFAIR передбачає ітеративний процес і кроки можуть повторюватися. Так, якщо відбувається інцидент з кібербезпеки відбувається переоцінка частоти подій загроз, а подія виникнення нового ризику з кібербезпеки вимагає повторення всього кроку «Оцінка частоти втрат», ну і відповідно зміна середовища запускає весь процес з первого кроку.

В контексті основного завдання цієї статті перевагою методології OpenFAIR є наявність керівництв, що дозволяють виконувати методологія у контексті розбудови систему управління інформаційною безпекою відповідно до стандарту ISO/IEC 27005.

Підсумовуючи викладене можна стверджувати, що є доцільним в якості основи для алгоритму оцінки ризиків кібербезпеки ІКС ВП використати безкоштовну методологію OpenFAIR за умови переорієнтації її кількісних оцінок з фінансової оцінки потенційних втрат на показники, що можуть бути корисними в процесі прийняття рішень по управлінню ризиками кібербезпеки в умовах ведення бойових дій.

МЕТОДИКА ДОСЛІДЖЕННЯ

Методологічною основою цього дослідження є системний підхід до аналізу проблем кібербезпеки, що дозволяє розглядати ІКС ВП як складні об’єкти, що функціонують в умовах гібридної війни, широкогомаштабного застосування противником засобів кібервливу за умови високої інтенсивності таких дій. Для досягнення поставленої мети були використаний аналіз літературних джерел та нормативних документів з питань кібербезпеки, оцінки ризиків та управління інформаційною безпекою, включаючи стандарти ISO/IEC 27000, NIST, та інші, порівняльний аналіз існуючих методологій оцінки ризиків кібербезпеки, таких як OCTAVE, NIST, COBIT, TARA та FAIR, з метою виявлення їх переваг та недоліків у контексті оцінки ризиків кібербезпеки в системах військового призначення, моделювання процесів оцінки ризиків за допомоги діаграм діяльності з метою візуалізувати та структурувати ключові етапи процесу. За результатом застосування вказаних методів була здійснена розробка алгоритму оцінки ризиків кібербезпеки, адаптованого до специфіки інформаційно-комунікаційних систем військового призначення та реалій гібридної війни з деталізацією кроків цього алгоритму.

Застосування згаданих методів дослідження дозволило провести комплексний розгляд проблеми оцінки ризиків кібербезпеки в умовах гібридної війни та запропонувати новий алгоритм, який враховує специфіку військових інформаційно-комунікаційних систем та неможливість оцінки потенційних фінансових втрат. Цей алгоритм може бути використаний для розробки ефективних стратегій кіберзахисту та підвищення кіберстійкості військових систем.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Аналіз наведених вище діаграм діяльності дозволяє описати алгоритм оцінки ризиків кібербезпеки в ІКС ВП (скорочено АОРІКС-В), що відповідатиме вимогам військового часу і діючив в України державних стандартів. Почнемо опис кроків діяльності згідно алгоритму спираючись на методологію OpenFAIR. Під час цього розгляду будемо вносити зміни, що відповідають особливостям цього процесу в ІКС ВП. Ключовою відмінністю АОРІКС-В від розглянутих вище методологій є те, що оцінки потенційних збитків у фінансовому еквіваленті у разі роботи інформаційної системи в умовах ведення війни позбавлені сенсу, як це і було зазначено вище. Замість оцінки величини потенційних збитків від ризику будемо оцінювати час неготовності системи, який визначимо як час протягом якого система повністю або частково не здатна виконувати завдання згідно свого функціоналу у разі настання події пов’язаної із ризиком кібербезпеки.

Початковим кроком розглянутих методологій є визначення активів. При цьому під активом мається на увазі будь-що, що має цінність для організації, і тому вимагає захисту. У випадку збройних сил це може включати інформацію (відкриті та конфіденційні дані, інформацію для службового користування та таємну інформацію тощо це спів), інформаційні системи (до складу яких, наприклад, входять сервери, бази даних, мережі, програмне забезпечення) та їх компоненти, людей (як особовий склад збройних сил, так і персонал фірм підрядників і представників сил оборони і країн партнерів тощо), фізичні об’єкти (будівлі, обладнання, інфраструктура) та фінансові активи. Враховуючи основне завдання цієї роботи в розробці АОРІКС-В звузимо коло активів до інформаційних систем та їх компонентів, при цьому слід виділити компоненти інформаційних систем від яких залежить час неготовності системи до виконання функцій на призначенням (далі — неготовність ІКС) в цілому, будемо називати це *Системоутвоючими компонентами,* і додамо крок класифікації компонентів з ознакою їх приналежності до системоутворювальних.

Підсумовуючи сказане, розглянемо діаграму діяльності розроблену на реалізації мети цієї роботи і опишемо всі кроки представленого на ній алгоритму (рис. 4).

Перший крок АОРІКС-В «Визначення активів» буде включати: визначення обсягу ІКС (приналежність конкретному структурному підрозділу чи збройним силам в цілому), опис ІКС (її функції, розташування, власника та інші відповідні характеристики), опис компонентів ІКС, класифікація компонентів ІКС.

Другий крок АОРІКС-В «Ідентифікація сценарію втрат» на якому визначається конкретна ситуація або подія, що може призвести до неготовності ІКС. На цьому кроку визначається агент загрози — це особа, група осіб або явище, яке може завдати шкоди активу (хакери, штатний персонал, фізичне знищення тощо), загрозлива подія (це конкретна дія або подія, за допомогою якої агент загрози намагається завдати шкоди активу), подія втрати (спостережувана подія, яка призводить до неготовності ІКС пов’язана з порушенням конфіденційності, цілісності або доступності активу), визначення засобів контролю (визначення вимірювальних параметрів, що відображають стан функціонування ІКС та засоби їх фіксації).

№ 2 (26), 2024
ISSN 2663 - 4023

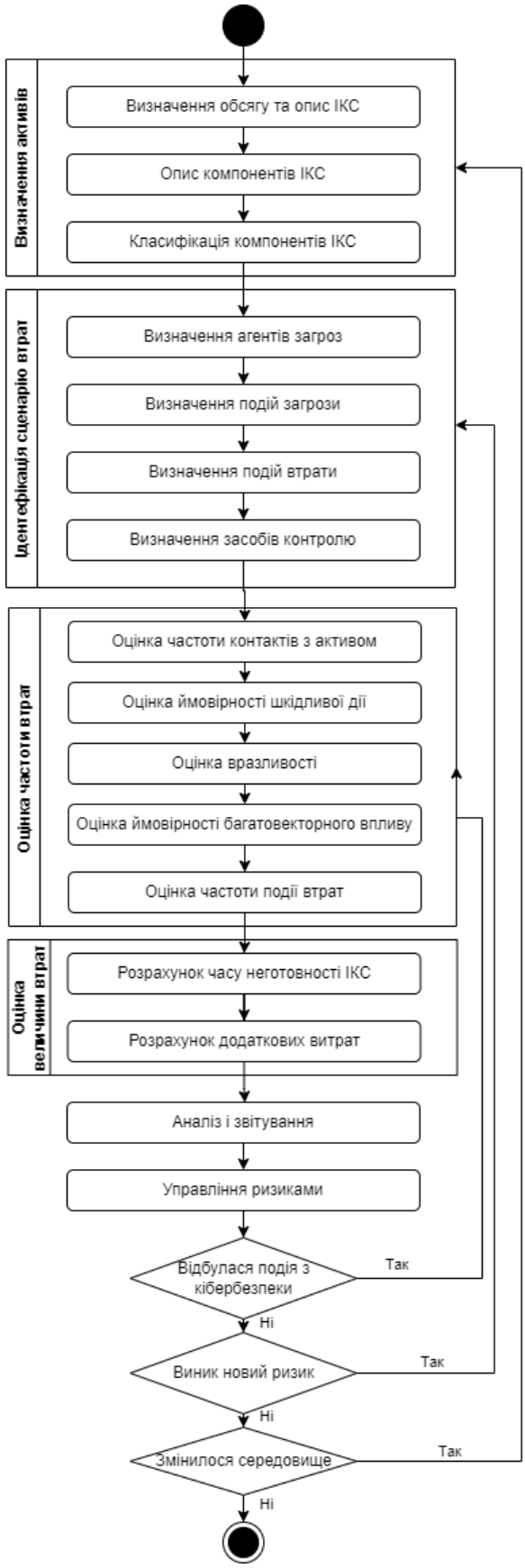

Рис. 4. Діаграма діяльності АОРІКС-В

На кроці «Оцінка частоти втрат» АОРІКС-В відбувається розрахунок таких параметрів, як частота контактів з активом (оцінка того, як часто агент загрози може взаємодіяти з активом), ймовірність шкідливої дії (ймовірність того, що під час контакту буде здійснено шкідливу дію), оцінка вразливості (розраховується на основі історичних даних про успішні та невдалі атаки, або шляхом порівняння можливостей агента загрози зі стійкістю активу). Ці параметри в цілому повторюють аналогічні в методології OpenFAIR, але у випадку АОРІКС-В існує потреба введення додаткового параметру, що є реакцією на неодноразове застосування російськими агентами кібервпливу багатовекторних атак, що зачіпають одразу декілька несистемоутворюючих активів. Кожна окрема така атака не несе загрози відмови ІКС, але їх комбінація в один момент часу цілком на це здатна. Назвемо цей параметр йомовірність багатовекторного впливу (цей параметр буде відповідати за ймовірність одночасного впливу на декілька несистемоутворювальних активів з метою виведення із ладу ІКС в цілому). Кінцевий параметр, що обраховується з попередніх це частота події втрат (використовуючи відповідну формулу або матрицю ризиків). На цьому кроці важливо задокументувати всі припущення та обґрунтування, які були використані під час оцінки частоти втрат, щоб забезпечити прозорість та можливість перевірки аналізу. Крок «Оцінка частоти втрат» є ітеративним процесом, який потребує перегляду в міру отримання нової інформації або зміни умов.

Наступний крок АОРІКС-В докорінно відрізняється від кроку «Оцінка величини втрат» методології OpenFAIR, який спрямований на кількісну оцінку фінансових наслідків, пов’язаних з реалізацією ризику. В АОРІКС-В цей крок передбачає визначення часу неготовності ІКС, який може виникнути в результаті конкретного сценарію втрати. Розрахунок цього часу проводиться як вибір між максимальною тривалістю відновлення працездатності ІКС після реалізації сценарію втрати або, за умови розроблених контрзаходів для цього сценарію втрати, як тривалість впровадження найбільш консервативної комбінації контрзаходів при настанні цього сценарії втрат. Такий підхід пов’язаний з тим, що це створює передумови для розробки найбільш ефективного пакету контрзаходів з метою ефективної протидії атакам ворога в умовах ведення агресивної війни в кіберпросторі і зменшує можливі прямі і непрямі втрати пов’язані із відмовою функціонування ІКС. Для кожного пакету контрзаходів або заходів відновлення, що приймають участь в розрахунку часу неготовності ІКС проводиться розрахунок величини додаткових фінансових витрат.

Наступний крок АОРІКС-В це «Аналіз та звітування» аналогічний методології OpenFAIR. Він передбачає інтерпретацію результатів кількісної оцінки ризиків та доведення результатів до осіб, які приймають рішення. На цьому кроці виконується інтерпретація результатів представлених у вигляді розподілу ймовірностей після проведення моделювання Монте-Карло та включає аналіз середніх значень, найбільш ймовірних значень, діапазонів та інших статистичних показників, щоб отримати повне уявлення про можливий час неготовності ІКС і потенційний вплив ризику на неї. Потім проводиться відбір релевантних результатів, що залежно від конкретної мети аналізу та потреб зацікавлених сторін може включати усереднені показники, такі як середньорічний час неготовності, або більш детальну інформацію, яка показує вплив вартості пропонованих пакетів контрзаходів на розрахункових час неготовності ІКС. Далі відбувається переклад кількісних результатів у якісні висновки з метою надати якісну інтерпретацію результатів, щоб вони були зрозумілішими для осіб, які приймають рішення (може включати використання якісних міток, таких як «високий», «середній» або «низький», для опису рівня ризику). Завершує цей крок розробка рекомендацій щодо

управління ризиками на основі результатів аналізу та створенням звіту, який містить ключові висновки аналізу, рекомендації щодо управління ризиками та будь-які інші відповідні дані.

Заключний крок AOPIKC-B це управління ризиками, що є ключовим етапом після проведення аналізу ризиків. Воно включає розробку та реалізацію стратегій, спрямованих на зниження або пом'якшення виявлених ризиків та базується на результатах аналізу, які надають кількісну оцінку ймовірності та величини потенційних втрат. Цей крок передбачає **використання кількісних** даних про ризики для прийняття обґрунтованих рішень щодо їх управління, вибір найбільш ефективних та економічно вигідних стратегій управління ризиками з урахуванням конкретного контексту застосування ІКС та регулярний моніторинг та перегляд ризиків та їх управління для врахування змін у середовищі та забезпечення актуальності стратегій.

Можливі стратегії AOPIKC-B це зниження ризику (впровадження заходів, спрямованих на зменшення ймовірності настання події втрати або її величини), уникнення ризику (ухилення від діяльності або ситуації, яка призводить до ризику) та прийняття ризику (свідоме рішення прийняти ризик, якщо його потенційні втрати вважаються прийнятними або вартість його зниження перевищує потенційні вигоди).

Так само як і OpenFAIR, AOPIKC передбачає ітеративний процес і кроки можуть повторюватися. Так, якщо відбувається інцидент з кібербезпеки відбувається переоцінка частоти подій загроз, а подія виникнення нового ризику з кібербезпеки вимагає повторення всього кроку «Оцінка частоти втрат», ну і відповідно зміна середовища запускає весь процес з першого кроку.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У сучасному світі, де гібридні загрози та кібератаки на широке коло об'єктів, де використовуються інформаційні технології та системи стають все більш поширеними та складними, забезпечення надійного захисту інформаційно-комунікаційних систем військового призначення є пріоритетним завданням. Проведений у цій статті аналіз існуючих методологій оцінки ризиків виявив їх обмеження в умовах сучасної війни, що підкреслює необхідність розробки нових підходів. Тому в роботі був запропонований алгоритм оцінки ризиків кібербезпеки, адаптований до специфіки систем військового призначення та реалій гібридної війни, який має потенціал значно підвищити ефективність процесу управління ризиками. Його впровадження дозволить забезпечити своєчасне виявлення та реагування на кіберзагрози, оптимізацію розподілу ресурсів на захист ІКС ВП та підвищення їх рівня кіберстійкості.

Однак, важливо розуміти, що запропонований алгоритм є лише одним з кроків на шляху до комплексного забезпечення кібербезпеки. Подальші дослідження мають бути спрямовані на розробку математичної моделі проведення оцінки ризиків кібербезпеки та формування повноцінної методології оцінки ризиків ІКС ВП розробку програмного забезпечення здатного здійснювати процес оцінки та переоцінки ризиків в реальному часі з метою підтримки прийняття рішень щодо удосконалення кіберзахисту ІКС ВП у найкоротші терміни.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Levite, A. E. (б. д.) *Integrating Cyber Into Warfighting: Some Early Takeaways From the Ukraine Conflict.* Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2023/04/integrating-cyber-into-warfighting-some-early-takeaways-from-the-ukraine-conflict?lang=en
2. Microsoft. (б. д.). *An overview of Russia's cyberattack activity in Ukraine.* https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/special-report-ukraine/?msockid=26f9b60dff436be1270ba25afe6b6a19#:~:text=Microsoft%20War%20in%20Ukraine
3. Baidur, O. (2022). Improvement of the cyber protection of the armed forces taking into account the experience of countering military cyber attacks of the russian federation in 2022. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique» 1(17),* 31–45. https://doi.org/10.28925/2663-4023.2022.17.3145
4. Байдур, О. В. (2023). Передумови створення моделі кіберзахисту Збройних Сил України. *Прикладні системи та технології в інформаційному суспільстві: Зб. тез VII Міжнар. науково-практ. конф.,* 19–22.
5. Байдур, О. В. (2022). Особливості правового регулювання питань кібербезпеки в Збройний Силах України та Міністерстві оборони України. *Інформаційні технології: економіка,техніка, освіта '2022: Зб. тез XIII Міжнар. науково-практ. конф. молодих вчен.,* 104–106.
6. Leszczyna, R. (2021). Review of cybersecurity assessment methods: Applicability perspective. *Computers & Security, 108.* https://doi.org/10.1016/j.cose.2021.102376
7. Cheimonidis, P., & Rantos, K. (2023). Dynamic risk assessment in cybersecurity: a systematic literature review. *Future internet, 15(10).* https://doi.org/10.3390/fi15100324
8. Devi, R. K., Sensuse, D. I., Kautsarina, & Suryono, R. R. (2022). Information security risk assessment (ISRA): a systematic literature review. *Journal of information systems engineering and business intelligence, 8(2),* 207–217. https://doi.org/10.20473/jisebi.8.2.207-217
9. Govinfo. (2015). DoD *Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (Rmf) into the System Acquisition Lifecycle: Executive Agency Publications*. https://www.govinfo.gov/app/details/GOVPUB-D-PURL-gpo62894
10. NIST SP 800-37 Rev. 2. Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (2018). https://doi.org/10.6028/NIST.SP.800-37r2
11. ДП «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» (ДП «УкрНДНЦ»). (2023). *Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2022, IDT)* (ДСТУ ISO/IEC 27001:2023).
12. Sánchez-García, I. D., Mejía, J., & San Feliu Gilabert, T. (2022). Cybersecurity Risk Assessment: A Systematic Mapping Review, Proposal, and Validation. *Applied Sciences. 13(1).* https://doi.org/10.3390/app13010395
13. Kalinin, M., Krundyshev, V., & Zegzhda, P. (2021). Cybersecurity Risk Assessment in Smart City Infrastructures. *Machines, 9(4).* https://doi.org/10.3390/machines9040078
14. Ferreira, D. J., Mateus-Coelho, N., & Mamede, H. S. (2023). Methodology for Predictive Cyber Security Risk Assessment (PCSRA). *Procedia Computer Science, 219,* 1555–1563. https://doi.org/10.1016/j.procs.2023.01.447
15. Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & Security, 56,* 1–27. https://doi.org/10.1016/j.cose.2015.09.009
16. Honchar, S. F. (2019). Methodology for risk assessment of cyber security of information systems of objects of critical infrastructure. *Scientific notes of Taurida National V.I. Vernadsky University. Series: Technical Sciences, 4(1),* 40–43. https://doi.org/10.32838/2663-5941/2019.4-1/08
17. Asieieva, L. A., & Shushura O. M. (2021). Assessment of confidentiality risks of information security of projects based on fuzzy logic. *Telecommunication and information technologies, 70(1).* https://doi.org/10.31673/2412-4338.2021.0108895
18. Alberts, C., & Dorofee, A. (2002). *Managing information security risks: The OCTAVE approach*. Addison-Wesley.
19. *COBIT 2019 Implementation Guide: Implementing and Optimizing an Information and Technology Governance Solution.* (2018). Isaca.
20. Wynn, J., Whitmore, J., Upton, G., Spriggs, L., McKinnon, D., McInnes, R., Graubart, R., Clausen, L. (2011). *Threat Assessment & Remediation Analysis (TARA). Methodology Description Version 1.0.*

21. Freund, J., & Jones, J. (2014). *Measuring and Managing Information Risk: A FAIR Approach*. Butterworth-Heinemann.
22. Caralli, R., Stevens, J., Young, L., & Wilson, W. (2007). *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process*. Carnegie Mellon University.
23. Alberts, C., Dorofee, A., Stevens, J., & Woody, C. (2005). *OCTAVE-S Implementation Guide, Version 1*. Pittsburgh, PA: Carnegie Mellon Software Engineering Institute.
24. *The Open Group Risk Analysis (O-RA) Standard, Version 2.0.1*. (2021). Berkshire, United Kingdom: The Open Group.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (26), 2024
ISSN 2663 - 4023

Oleksii Baidur
PhD student
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
The Armed Forces of Ukraine, Kyiv, Ukraine
ORCID ID: 0000-0001-7036-1264
alexvb1981@gmail.com

QUANTITATIVE METHODOLOGY FOR ASSESSING CYBERSECURITY RISKS IN THE ABSENCE OF FINANCIAL DATA ON LOSSES

Abstract. The article addresses the pressing issue of cybersecurity risk assessment in military information and communication systems (ICS) during aggressive warfare, where it is impossible to assess potential losses in monetary terms, and considering the specifics of hybrid threats. The introduction discusses the relevance of the problem and emphasizes the need for a proactive cyber defense strategy and timely risk assessment, especially in the context of the active use of cyberweapons by the adversary. Particular attention is given to the impossibility of assessing potential losses from cyberattacks in monetary terms, which necessitates new approaches to risk assessment. The section "Specifics of Cybersecurity Risk Assessment in the ICS of the Armed Forces of Ukraine" analyzes existing standards and methodologies, such as the standards of the DSTU ISO/IEC 27000 group, as well as current cybersecurity risk assessment methodologies, and reveals the limitations of their application in wartime conditions. The section emphasizes the importance of automating the risk assessment process to ensure a rapid response to cyber threats. The advantages of quantitative risk assessment models over qualitative ones are considered, especially in the context of military information and communication systems. The following sections examine in detail the key risk assessment processes according to DSTU ISO/IEC 27005:2023 and in accordance with current methodologies. A comparative analysis of the OCTAVE, NIST, COBIT, TARA, and FAIR methodologies is conducted from the perspective of their suitability for the needs of the Armed Forces of Ukraine. The advantages and disadvantages of each methodology are discussed, and the necessity of developing a new methodology based on OpenFAIR (an open version of the FAIR methodology), adapted to the specifics of military ICS and the realities of hybrid warfare, is substantiated. The research results are presented in the form of an activity diagram for a cybersecurity risk assessment algorithm in military information and communication systems, along with a detailed description of these steps, emphasizing the differences from the OpenFAIR methodology. The "Conclusions" section summarizes the work done and formulates proposals for further research.

Keywords: information technologies; cybersecurity; risk assessment; hybrid warfare; quantitative assessment; military ICS; cyber warfare.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Levite, A. E. (б. д.) *Integrating Cyber Into Warfighting: Some Early Takeaways From the Ukraine Conflict.* Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2023/04/integrating-cyber-into-warfighting-some-early-takeaways-from-the-ukraine-conflict?lang=en
2. Microsoft. (б. д.). *An overview of Russia's cyberattack activity in Ukraine.* https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/special-report-ukraine/?msockid=26f9b60dff436be1270ba25afe6b6a19#:~:text=Microsoft%20War%20in%20Ukraine
3. Baidur, O. (2022). Improvement of the cyber protection of the armed forces taking into account the experience of countering military cyber attacks of the russian federation in 2022. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique» 1(17),* 31–45. https://doi.org/10.28925/2663-4023.2022.17.3145
4. Baidur, O. (2023). Prerequisites for creating a cyber defence model for the Armed Forces of Ukraine. *Applied systems and technologies in the information society: Collection of abstracts of the VII International scientific and practical conference,* 19–22.

5. Baidur, O. (2022). Features of legal regulation of cybersecurity issues in the Armed Forces of Ukraine and the Ministry of Defence of Ukraine. *Information technologies: economy, technology, education '2022: Collection of abstracts of the XIII International scientific and practical conference of young scientists*, 104–106.
6. Leszczyna, R. (2021). Review of cybersecurity assessment methods: Applicability perspective. *Computers & Security, 108.* https://doi.org/10.1016/j.cose.2021.102376
7. Cheimonidis, P., & Rantos, K. (2023). Dynamic risk assessment in cybersecurity: a systematic literature review. *Future internet, 15(10).* https://doi.org/10.3390/fi15100324
8. Devi, R. K., Sensuse, D. I., Kautsarina, & Suryono, R. R. (2022). Information security risk assessment (ISRA): a systematic literature review. *Journal of information systems engineering and business intelligence, 8(2),* 207–217. https://doi.org/10.20473/jisebi.8.2.207-217
9. Govinfo. (2015). DoD *Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (Rmf) into the System Acquisition Lifecycle: Executive Agency Publications.* https://www.govinfo.gov/app/details/GOVPUB-D-PURL-gpo62894
10. NIST SP 800-37 Rev. 2. Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (2018). https://doi.org/10.6028/NIST.SP.800-37r2
11. Ukrainian Research and Training Centre for Standardisation, Certification and Quality (2023). *Information security, cybersecurity and privacy protection. Information security management systems. Requirements. (ISO/IEC 27001:2022, IDT)* (ISO/IEC 27001:2023).
12. Sánchez-García, I. D., Mejía, J., & San Feliu Gilabert, T. (2022). Cybersecurity Risk Assessment: A Systematic Mapping Review, Proposal, and Validation. *Applied Sciences. 13(1).* https://doi.org/10.3390/app13010395
13. Kalinin, M., Krundyshev, V., & Zegzhda, P. (2021). Cybersecurity Risk Assessment in Smart City Infrastructures. *Machines, 9(4).* https://doi.org/10.3390/machines9040078
14. Ferreira, D. J., Mateus-Coelho, N., & Mamede, H. S. (2023). Methodology for Predictive Cyber Security Risk Assessment (PCSRA). *Procedia Computer Science, 219,* 1555–1563. https://doi.org/10.1016/j.procs.2023.01.447
15. Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & Security, 56,* 1–27. https://doi.org/10.1016/j.cose.2015.09.009
16. Honchar, S. F. (2019). Methodology for risk assessment of cyber security of information systems of objects of critical infrastructure. *Scientific notes of Taurida National V.I. Vernadsky University. Series: Technical Sciences, 4(1),* 40–43. https://doi.org/10.32838/2663-5941/2019.4-1/08
17. Asieieva, L. A., & Shushura O. M. (2021). Assessment of confidentiality risks of information security of projects based on fuzzy logic. *Telecommunication and information technologies, 70(1).* https://doi.org/10.31673/2412-4338.2021.0108895
18. Alberts, C., & Dorofee, A. (2002). *Managing information security risks: The OCTAVE approach*. Addison-Wesley.
19. *COBIT 2019 Implementation Guide: Implementing and Optimizing an Information and Technology Governance Solution.* (2018). Isaca.
20. Wynn, J., Whitmore, J., Upton, G., Spriggs, L., McKinnon, D., McInnes, R., Graubart, R., Clausen, L. (2011). *Threat Assessment & Remediation Analysis (TARA). Methodology Description Version 1.0.*
21. Freund, J., & Jones, J. (2014). *Measuring and Managing Information Risk: A FAIR Approach*. Butterworth-Heinemann.
22. Caralli, R., Stevens, J., Young, L., & Wilson, W. (2007). *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process.* Carnegie Mellon University.
23. Alberts, C., Dorofee, A., Stevens, J., & Woody, C. (2005). *OCTAVE-S Implementation Guide, Version 1.* Pittsburgh, PA: Carnegie Mellon Software Engineering Institute.
24. *The Open Group Risk Analysis (O-RA) Standard, Version 2.0.1.* (2021). Berkshire, United Kingdom: The Open Group.