

У статті розглянуто проблему впровадження ризик-орієнтованого підходу в державне управління кібербезпекою інформаційних систем органів сектору безпеки і оборони України. Гібридна агресія проти нашої держави засвідчила, що кіберпростір перетворився на повноцінний театр протиборства. Атаки на об'єкти енергетики, масштабні кампанії шкідливого програмного забезпечення, втручання в роботу державних реєстрів показали вразливість не окремих ресурсів, а цілих контурів управління. Реактивна модель захисту, зорієнтована переважно на ліквідацію наслідків інцидентів, за таких умов вичерпує свій потенціал. Метою роботи є обґрунтування теоретико-методологічних засад і практичних напрямів застосування ризик-орієнтованого підходу як основи формування механізмів державного управління кібербезпекою в секторі безпеки і оборони. Показано, що ризик у цій сфері доцільно трактувати як управлінську категорію, а не лише як технічну характеристику систем. Ефективність підходу залежить від узгодженості нормативного, організаційного та інформаційно-аналітичного механізмів, від єдиної методики оцінювання ризиків і сталого обміну даними про загрози. Окреслено напрями вдосконалення, пов'язані з розбудовою національної системи кібербезпеки та наближенням до підходів ЄС і НАТО.

УДК 351.86:004.056

*Ласуков О. Є., здобувач НУЦЗ України***Ризик-орієнтований підхід у державному управлінні кібербезпекою інформаційних систем сектору безпеки і оборони України****(Risk-Oriented Approach in Public Administration of Cybersecurity of Information Systems of the Security and Defense Sector of Ukraine)**

<i>Ключові слова: ризик-орієнтований підхід, державне управління, кібербезпека, сектор безпеки і оборони, інформаційні системи, механізми державного управління, оцінювання ризиків, національна система кібербезпеки.</i>	
--	--

Постановка проблеми. Кібербезпека тривалий час розглядалася як сфера діяльності вузьких фахівців: адміністраторів мереж, інженерів із захисту інформації, підрозділів технічного захисту. Події останніх років істотно змінили таке уявлення. Гібридна агресія проти України засвідчила, що ураження інформаційної системи здатне спричинити наслідки, співмірні з наслідками застосування звичайних засобів ураження, зокрема знеструмлення регіонів, порушення функціонування органів державної влади, дезорганізацію логістики, компрометацію службової інформації [2; 8]. Для органів сектору безпеки і оборони, інформаційні системи яких забезпечують управління військами, оперативну діяльність, охорону державного кордону та реагування на надзвичайні ситуації, подібні наслідки є неприпустимими.

Відповіддю держави на ці виклики стало формування відповідної нормативно-правової бази. Ухвалено Стратегію кібербезпеки України [9], Закон України «Про основні засади забезпечення кібербезпеки України» [10], Доктрину інформаційної безпеки України [11], а Законом України «Про національну безпеку України» визначено склад сектору безпеки і оборони [12]. Водночас нормативна база сама по собі не дає відповіді на питання щодо пріоритетності розподілу обмежених ресурсів, черговості захисту інформаційних систем і рівня залишкового ризику, який держава вважає прийнятним.

Аналіз останніх досліджень і публікацій. Проблематика кібербезпеки у вітчизняній науці тривалий час розвивалася переважно в технічній і правовій площинах. Соціотехнічний вимір захисту інформації, зокрема роль людського чинника та організаційних заходів, ґрунтовно висвітлено в працях В. Бурячка, В. Толубка та В. Хорошка [1]. Геополітичне прочитання кіберпростору як нового поля суперництва держав запропонував Д. Дубов [2], і саме ця лінія стала вихідною для багатьох подальших розвідок

у галузі державного управління. Теоретичні засади аналізу загроз і ризиків у сфері національної безпеки, зокрема математичні методи їх оцінювання, розробив А. Качинський [3]. Інформаційні операції як інструмент впливу на безпеку суспільства та моделі протидії їм дослідили В. Горбулін, О. Додонов і Д. Ланде [4]. Концептуальні засади безпекознавства, на яких ґрунтується розуміння загрози й ризику як управлінських категорій, розроблено В. Ліпканом [5].

У зарубіжній практиці ризик-орієнтована логіка давно закріплена в рамкових документах NIST [6] і стандартах серії ISO/IEC 27000 [7]. У вітчизняних дослідженнях питання її адаптації до специфіки сектору безпеки і оборони розкрито ще фрагментарно, що почасти пояснюється нещодавнім законодавчим закріпленням самого поняття сектору безпеки і оборони.

Виклад основного матеріалу дослідження. Вихідним пунктом аналізу є саме поняття ризику, оскільки з ним пов'язана основна методологічна складність дослідження. У технічній літературі ризик інформаційної безпеки зазвичай визначають як поєднання ймовірності реалізації загрози через певну вразливість і величини шкоди, що може настати [1; 7]. Таке визначення є продуктивним для інженерних розрахунків. Для потреб державного управління воно недостатнє.

Це зумовлено насамперед природою джерела загрози. У випадку інформаційних систем Міністерства оборони, Служби безпеки чи Державної прикордонної служби ним здебільшого виступає не випадкова подія, а цілеспрямована діяльність противника, який володіє ресурсами, мотивацією та здатністю до навчання. Імовірність за таких умов не може розглядатися як статистична величина в класичному розумінні, оскільки її неможливо визначити на підставі частоти минулих інцидентів. У разі невдачі противник, як правило, змінює тактику, у разі успіху ймовірним є повторення спроби щодо інших об'єктів. Відтак оцінювання ризику в секторі безпеки і оборони закономірно зміщується від імовірнісних моделей до сценарного аналізу, що передбачає зіставлення можливостей і намірів супротивника з критичністю функцій, які забезпечує конкретна система.

У безпекознавстві ustalеним є розмежування понять небезпеки, загрози та ризику [5]. Небезпека означає об'єктивну можливість заподіяння шкоди. Загроза являє собою небезпеку, що набула конкретного джерела та спрямованості. Ризик, на нашу думку, доцільно розглядати як міру здатності загрози, з урахуванням наявних вразливостей і вжитих заходів, порушити виконання завдань, покладених на суб'єкт сектору безпеки і оборони. Запропоноване визначення переносить акцент із технічного стану системи на її функціональне призначення. Ризиком у такому розумінні є не компрометація окремого сервера, а зумовлена нею неможливість своєчасного доведення розпоряджень або розголошення відомостей про особовий склад.

Звідси впливає ключове положення дослідження: ризик у сфері кібербезпеки сектору безпеки і оборони є управлінською категорією. Рішення щодо прийнятного рівня ризику не належить до компетенції технічного персоналу. Воно ухвалюється керівником, відповідальним за виконання завдань органу, а на вищому рівні державою, яка визначає пріоритети національної безпеки.

Доцільним є порівняння ризик-орієнтованого підходу з двома іншими моделями, що фактично співіснують у вітчизняній практиці. Перша модель є нормативно-відповідною. Її сутність полягає у виконанні встановлених вимог, що передбачає побудову комплексної системи захисту інформації, проходження державної експертизи та атестації. Перевагою цієї моделі є забезпечення базового, однакового для всіх суб'єктів рівня захищеності та чітких критеріїв контролю. Разом із тим вона має статичний характер. Вимоги формулюються заздалегідь, з огляду на певний перелік загроз, і тому закономірно відстають від їх фактичної динаміки. Друга модель є загрозо-орієнтованою: захисні заходи в ній формуються з урахуванням найбільш резонансних інцидентів. Вона вирізняється більшою гнучкістю, проте зумовлює схильність до реагування переважно на останні за часом атаки й до розпорошення ресурсів.

Ризик-орієнтований підхід не заперечує зазначених моделей, а інтегрує їх у єдину систему. Нормативні вимоги зберігають значення мінімального рівня захищеності. Відомості про загрози набувають статусу вхідних даних для оцінювання. Над ними

вибудовується управлінський цикл, що охоплює ідентифікацію активів і функцій, оцінювання ризиків, вибір способу їх обробки (зниження, передання, уникнення або свідоме прийняття), моніторинг і перегляд. Саме така циклічна логіка закладена в рамкових документах NIST [6] та стандарті ISO/IEC 27005 [7]. На наш погляд, вона найповніше відповідає умовам, за яких загрози змінюються швидше, ніж відбувається оновлення нормативного регулювання.

Упровадження такого підходу на рівні окремої установи є складним, однак цілком реалістичним завданням. На рівні сектору безпеки і оборони воно набуває якісно іншого змісту й потребує відповідних механізмів державного управління. Під механізмом державного управління кібербезпекою ми розуміємо сукупність взаємопов'язаних методів, інструментів, організаційних структур і процедур, за допомогою яких суб'єкти управління впливають на стан захищеності інформаційних систем з метою утримання ризику на прийнятному рівні. Цей механізм має комплексний характер. У його структурі доцільно виокремлювати нормативно-правову, організаційну, інформаційно-аналітичну, кадрову та ресурсну складові [2; 8].

Кожна зі складових по-своєму відображає ризик-орієнтовану логіку. Нормативно-правова складова має закріплювати не лише перелік вимог, а й обов'язок суб'єктів оцінювати ризики, визначати їх власників і звітувати про результати оцінювання. Організаційна складова передбачає такий розподіл відповідальності, за якого кожен ризик має визначеного власника, а рішення про його прийняття ухвалюється на належному рівні управління. Інформаційно-аналітична складова покликана забезпечувати суб'єктів управління достовірними й своєчасними даними про загрози, вразливості та інциденти. За відсутності таких даних оцінювання ризиків втрачає об'єктивність і набуває суто експертного характеру. Кадрова складова забезпечує наявність фахівців, здатних здійснювати оцінювання та інтерпретувати його результати, причому це стосується як технічного персоналу, так і керівного складу. Ресурсна складова пов'язує результати оцінювання з бюджетним та оборонним плануванням; за відсутності такого зв'язку результати аналітичної роботи не набувають практичного втілення.

Окремої уваги потребує специфіка сектору, що ускладнює безпосереднє запозичення зарубіжних моделей. По-перше, суб'єкти сектору є неоднорідними. До його складу належать органи з принципово різними функціями, від Збройних Сил України до Державної служби України з надзвичайних ситуацій, які характеризуються різною управлінською культурою та неоднаковим рівнем технічного оснащення [12]. По-друге, діє режим обмеженого доступу до інформації. Відомості про вразливості та інциденти в секторі нерідко становлять державну таємницю, що ускладнює горизонтальний обмін ними. По-третє, наслідки помилкових управлінських рішень є особливо тяжкими, оскільки вимірюються не фінансовими втратами, а здатністю держави забезпечувати свою оборону.

Зазначені особливості зумовлюють принципи ризик-орієнтованого управління кібербезпекою сектору безпеки і оборони. До них належать пріоритетність функцій над активами, пропорційність заходів рівню ризику, безперервність оцінювання, персоніфікована відповідальність власника ризику, а також контрольована відкритість, що передбачає обмін інформацією про загрози в обсязі, який не порушує вимог режиму секретності.

Розглянемо можливості вбудовування ризик-орієнтованої логіки в механізми, що нині формуються. Законом України «Про основні засади забезпечення кібербезпеки України» визначено основних суб'єктів національної системи кібербезпеки, якими є Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України [10]. Координацію їхньої діяльності здійснює Рада національної безпеки і оборони України через Національний координаційний центр кібербезпеки. Таким чином, інституційне підґрунтя для загальнодержавного управління ризиками вже створено. Подальше завдання полягає в його змістовному наповненні.

Показовими в цьому контексті є уроки масштабних кібератак, яких зазнала Україна. Атаки на енергетичні компанії, що призвели до знеструмлення споживачів у низці областей, засвідчили здатність противника тривалий час готувати операції, приховано

закріплюючись в інформаційних мережах [8]. Ще більш показовим став інцидент, коли шкідливе програмне забезпечення поширилося через оновлення поширеної бухгалтерської програми й упродовж короткого часу порушило функціонування мереж значної кількості державних установ і підприємств. З позицій ризик-менеджменту цей інцидент виявив ризик, який традиційно недооцінювався, а саме ризик ланцюга постачання. Загроза була реалізована через легітимний, довірений канал, і формальна відповідність установленим вимогам не забезпечила захисту від неї. Звідси випливає висновок, актуальний для органів сектору, що тією чи іншою мірою використовують комерційне програмне забезпечення. Оцінювання ризиків має охоплювати не лише власну інфраструктуру, а й постачальників, підрядників і суміжні системи.

Упровадження ризик-орієнтованого підходу в масштабі сектору, на нашу думку, передбачає низку взаємопов'язаних кроків.

Першим із них є формування єдиної методичної основи. Суб'єкти сектору спираються переважно на відомчі нормативні документи, що ускладнює зіставлення результатів оцінювання, отриманих різними органами. Йдеться не про повну уніфікацію відомчих підходів, а про запровадження спільної таксономії загроз і наслідків, узгоджених шкал оцінювання та єдиних підходів до визначення критичності функцій. За таких умов ризик, виявлений в одному органі, стає співвимірним з ризиками інших органів, що уможлиблює формування зведеної картини ризиків сектору. Логічним розвитком цієї ідеї є створення галузевого реєстру кіберризиків, ведення якого здійснювалося б з дотриманням вимог режиму секретності, але забезпечувало б координаційний орган цілісною інформацією про найбільш уразливі ланки.

Другим кроком є інтеграція оцінювання ризиків у цикл планування. Стратегічний оборонний бюлетень України передбачає перехід до планування на основі спроможностей [13], що створює належні передумови для такої інтеграції. Кібербезпеку в цьому разі слід розглядати не як окремий напрям видатків, а як умову збереження кожної зі спроможностей. Якщо певна спроможність критично залежить від функціонування інформаційної системи, ризики цієї системи мають ураховуватися під час планування

відповідної спроможності, а заходи з їх обробки мають отримувати ресурсне забезпечення одночасно з нею.

Третім кроком є розвиток обміну інформацією. Оцінювання ризику неможливе без знання загроз, тоді як відомості про загрози розподілені між різними командами реагування та підрозділами. Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA, ситуаційні центри відомств, профільні підрозділи Служби безпеки України та кіберполіції накопичують унікальні дані, цінність яких істотно зростає за умови їх спільного використання. Досвід держав – членів НАТО свідчить, що ефективний обмін інформацією ґрунтується на чітких правилах її класифікації, зокрема на протоколі «світлофора» (Traffic Light Protocol), а також на взаємній довірі, що формується в процесі тривалої співпраці [14]. Важливим чинником розвитку відповідних спроможностей України є підтримка, яка надається в межах трастового фонду НАТО з кібероборони.

Четвертим кроком є розвиток кадрового потенціалу. Ризик-орієнтований підхід висуває до персоналу вищі вимоги порівняно з нормативно-відповідним, оскільки передбачає не лише виконання встановлених процедур, а й прогнозування наслідків подій, що раніше не мали місця. Дефіцит кваліфікованих фахівців із кібербезпеки має глобальний характер, а в секторі безпеки і оборони він посилюється конкуренцією з приватним сектором. Розв'язання цієї проблеми вбачається в поєднанні кількох напрямів: підготовки фахівців у закладах вищої освіти, що належать до сфери управління органів сектору, запровадження програм підвищення кваліфікації для керівного складу з питань інтерпретації результатів оцінювання ризиків, формування резерву з числа цивільних фахівців, готових залучатися до виконання завдань в особливий період.

Узагальнення викладеного дає змогу запропонувати трирівневу модель ризик-орієнтованого управління кібербезпекою сектору безпеки і оборони. На стратегічному рівні координаційний орган за участю суб'єктів національної системи кібербезпеки визначає загальнодержавні пріоритети, перелік критичних функцій і прийнятний рівень ризику, а також формує зведений профіль ризиків. На оперативному рівні кожен орган

сектору ідентифікує ризики власних інформаційних систем, веде їх реєстр, затверджує плани обробки ризиків і звітує про стан їх виконання. На тактичному рівні власники та адміністратори конкретних систем реалізують захисні заходи, здійснюють моніторинг і повідомляють про інциденти. Принципове значення має наявність зворотного зв'язку: дані тактичного рівня мають надходити на вищі рівні та слугувати підставою для коригування оцінок, а стратегічні рішення мають доводитися до нижчих рівнів у формі конкретних пріоритетів.

Запропонована модель не потребує реорганізації чинних інституцій. Вона передбачає узгодження їхньої діяльності на основі спільної методологічної логіки. Разом із тим її впровадження потребуватиме часу, послідовності та готовності керівників брати на себе відповідальність за рішення про прийняття ризику, чого нормативно-відповідна модель від них не вимагала. Основний виклик, таким чином, пов'язаний не стільки з технологічним, скільки з управлінсько-культурним виміром змін.

Проведене дослідження дає підстави стверджувати, що ризик-орієнтований підхід є методологічною основою формування механізмів державного управління кібербезпекою інформаційних систем органів сектору безпеки і оборони України. Його застосування зумовлене тим, що нормативно-відповідна та загрозо-орієнтована моделі захисту, зберігаючи власну цінність, не забезпечують належної адаптивності до цілеспрямованих і динамічних загроз, характерних для умов гібридної агресії. Обґрунтовано, що ризик у цій сфері доцільно розглядати як управлінську категорію, яка відображає міру здатності загрози порушити виконання функцій суб'єкта сектору, а не лише технічний стан інформаційної системи. Таке розуміння зумовлює перенесення відповідальності за рішення щодо прийнятного рівня ризику на керівний склад і державний рівень управління.

Визначено, що ефективність ризик-орієнтованого управління залежить від узгодженості нормативно-правової, організаційної, інформаційно-аналітичної, кадрової та ресурсної складових відповідного механізму, а також від урахування специфіки сектору: неоднорідності суб'єктів, режиму обмеженого доступу та особливої тяжкості наслідків інцидентів. Запропоновано трирівневу модель ризик-орієнтованого управління

кібербезпекою сектору, що охоплює стратегічний, оперативний і тактичний рівні та передбачає наявність зворотного зв'язку між ними. Її реалізація потребує формування єдиної методичної основи оцінювання ризиків, інтеграції оцінювання в цикл планування на основі спроможностей, розвитку обміну інформацією про загрози та посилення кадрового потенціалу.

Список використаних джерел:

1. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект : підручник / за заг. ред. В. Б. Толубка. Київ : ДУТ, 2015. 288 с.
2. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва : монографія. Київ : НІСД, 2014. 328 с.
3. Качинський А. Б. Безпека, загрози і ризик: наукові концепції та математичні методи. Київ : Ін-т проблем національної безпеки, 2004. 472 с.
4. Горбулін В. П., Додонов О. Г., Ланде Д. В. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання : монографія. Київ : Інтертехнологія, 2009. 164 с.
5. Ліпкан В. А. Безпекознавство : навч. посіб. Київ : Вид-во Європ. ун-ту, 2003. 208 с.
6. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1 / National Institute of Standards and Technology. Gaithersburg, 2018. 55 p. URL: <https://doi.org/10.6028/NIST.CSWP.04162018>.
7. ISO/IEC 27005:2011. Information technology – Security techniques – Information security risk management. Geneva : ISO, 2011. 68 p.
8. Горбулін В. П. Світова гібридна війна: український фронт : монографія. Київ : НІСД, 2017. 496 с.

9. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 15.03.2016 № 96/2016. URL: <https://zakon.rada.gov.ua/laws/show/96/2016>.
10. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19>.
11. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25.02.2017 № 47/2017. URL: <https://zakon.rada.gov.ua/laws/show/47/2017>.
12. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2469-19>.
13. Про рішення Ради національної безпеки і оборони України від 20 травня 2016 року «Про Стратегічний оборонний бюлетень України» : Указ Президента України від 06.06.2016 № 240/2016. URL: <https://zakon.rada.gov.ua/laws/show/240/2016>.
14. National Cyber Security Framework Manual / ed. by A. Klimburg. Tallinn : NATO CCD COE Publications, 2012. 235 p.