ІНДИКАТОРИ РЕАЛЬНИХ ЗАГРОЗ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ В ІНФОРМАЦІЙНІЙ СФЕРІ

М. А. Ожеван, С. Л. Недбаєвський, Д. В. Дубов

Ризики, загрози й виклики детермінують масштаби людської діяльності. Відповідно, за основу методології їхнього розуміння й обліку (аудиту) має бути покладене чітке усвідомлення якісного й кількісного аспектів ризиків, які виникають у кожному конкретному різновиді людської діяльності.

Так, у процесі стратегічного планування в США використовують два терміни: «загроза» (threat) і «виклик» (challenge). Вони позначають можливості якої-небудь країни, групи осіб або певного явища загрожувати («загроза») або протидіяти («виклик») досягненню цілей національної безпеки.

Джерела загроз зумовлюють:

небезпеки для реалізації цілей національної безпеки в рамках відповідного періоду планування;
певні тенденції розвитку військово-політичної обстановки;
необхідність негайних акцій силового характеру із безпосереднім залученням Збройних Сил та інших «силових» структур.

Характер загроз національним інтересам визначається конкретними інтересами, яким вони загрожують, як унікальним поєднанням:

інтересів, що зачіпають усю країну;
у певному місці за конкретних обставин;
за належного розуміння можливостей, намірів і волі потенційного супротивника;
за наявних засобів нейтралізації (ліквідації, мінімізації).

Ці чотири елементи визначають ступені ризику, пов'язаного з конкретною загрозою, через виявлення її:

природи (характеру);
імовірності реалізації в межах відведеного періоду попередження;
рівня можливого збитку від реалізації.

Загрози класифікують як потенційні й безпосередні. Відповідно, перший етап визначення загроз у сфері інформаційної безпеки має бути започаткований категоризацією пов'язаних з ними ризиків, які:

обов'язково мають бути мінімізовані/усунуті;

можуть бути мінімізовані/усунуті;
є певною мірою прийнятними.

Індикатори загроз відображують контури загроз інформаційній безпеці держави, їх основні структурні характеристики, а також порогові критерії інтенсивності, що сигналізують відповідним державним органам про необхід-

Ожеван Микола Андрійович — доктор філософських наук, професор, завідувач відділу Національного інституту проблем міжнародної безпеки

Недбаєвський Сергій Леонідович — державний експерт Національного інституту проблем міжнародної безпеки

Дубов Дмитро Володимирович — головний консультант Національного інституту проблем міжнародної безпеки

ність прийняття тих чи інших заходів щодо їх нейтралізації.

До основних індикаторів загроз національній безпеці в інформаційній сфері належать:

суб'єкти загрози;
структура загрози;
характеристика загрози;
можливі наслідки загрози;
рівень інтенсивності загрози.

Суб'єкт загрози — це той індикатор, який «відбирає» загрози національній безпеці в інформаційній сфері за ступенем значущості їх суб'єкта або всередині країни, або ззовні.

Структура загрози. Загроза може бути більш чи менш керованою зсередини та структурно розгалуженою. Більш структуровані загрози містять у собі сильнішу небезпеку, аніж менш структуровані.

Характеристика загрози — елемент, який окреслює **контури загрози**, а також, за необхідності, містить у собі порівняльні характеристики того, як ця загроза нейтралізується в інших країнах.

Можливі наслідки загрози — критерії оцінки загроз, які дозволяють диференціювати їх з погляду ступеня дискримінації національних інтересів.

Щодо «національних інтересів», то у Стратегії національної безпеки США вони класифіковані за трьома категоріями:

• **життєво важливі** (вітальні), пов'язані із виживанням і безпекою нації;

• **важливі**, що не пов'язані з виживанням країни, але здатні відчутно впливати на добробут США й характер міжнародних відносин;

• **гуманітарні**, що пов'язані з широким спектром міжнародних проблем, які безпосередньо не зачіпають тріаду «свобода — виживання — процвітання», але тактично вигідні США у плані позиціонування як усередині країни, так і на міжнародній арені.

Життєво важливі інтереси — це захист території, недопущення розвалу систем міжнародної торгівлі; забезпечення доступу до ринків фінансів, джерел енергії; захист території союзників тощо. Тобто заради чого нація не йтиме на компроміси й ладна використати всю сукупність інструментів національної потуги, тоді як для захисту важливих інтересів наявні ресурси й інструменти будуть використані обережніше із виваженням ціни ризику і цінності відповідних інтересів (міркування національної вигоди).

Комісія Харта-Рудмана («Комісія з національної безпеки США у XXI столітті») свого часу запропонувала чітко розмежувати інтереси, пов'язані із виживанням націй, від інтересів менш пріоритетних. Таким чином, національні інтереси запропоновано поділити на три категорії:

інтереси виживання (survival interests);
критично важливі (critical interests);
істотні (significant interests).

До інтересів виживання віднесено національні інтереси, без захисту яких США не зможуть забезпечити своє нинішнє існування і які жодним чином не можуть бути предметом торгу, а для їх захисту повинні залучатися всі наявні інструменти національної потуги.

З огляду на ці міркування, можливі наслідки загрози як індикатора загроз національній безпеці слід поділяти за триступеневою схемою:

загрози життєво важливим інтересам країни в інформаційній сфері (загрози інтересам виживання);
загрози важливим інтересам;
істотні загрози.

Рівень інтенсивності загрози — це індикатор ступеня напруження в державі та суспільстві, який у США та деяких інших країнах позначається кольорами загроз, що означає у якій послідовності держава має реагувати на певні загрози. Відповідно, загрози поділяють на:

високої інтенсивності (червоний колір): сигналізують, що держава опинилася на порозі реальної небезпеки, і термінове невжиття невідкладних заходів обернеться катастрофічними наслідками;

середньої інтенсивності (помаранчевий колір): ситуація є контрольованою, однак без належного реагування уповноважених органів може трансформуватися на загрозу високої інтенсивності.

низької інтенсивності (жовтий колір): ситуація є контрольованою, однак реагування на неї державних органів є нескоординованим та неадекватним масштабам загрози.

Слід розрізняти «небезпеку» й «ризик». Небезпеки існують завжди, оскільки ніде і ні в чому немає абсолютної надійності. Ризики ж існують там і тоді, де і коли доводиться приймати рішення щодо реагування на небезпеку. Причому відмову від прийняття рішення теж можна вважати рішенням.

Будь-який «розвиток» практично є синонімом «криз» і «ризиків». Пришвидшення розвитку, характерне для сучасної епохи «постмодерну», породило феномени «моральної паніки» й «катастрофічної свідомості» [7]. Небезпеки й ризики нині видаються самоочевидними й доступними для сприймання на рівні відчуттів.

Але це оманлива очевидність, бо те, що ми сприймаємо як безпечне або небезпечне, регулюється суспільною свідомістю, яка підпорядковує собі свідомість індивідуальну. Якщо досі суспільна свідомість формувалася під впливом презирства до «міщанського» намагання убезпечитися від небезпек, то нині настав час «міщанського реваншу», а «безпека» із усіма похідними від неї категоріями перетворилася на ключовий концепт епохи «масового споживання ризиків».

Саме слово «ризик» вперше з'явилося в ігровому контексті і не мало однозначно негативного відтінку. Воно означало «шанс», яким варто скористатися. Нове розуміння «ризику» співвідносить його виключно з небезпекою. «Хороші ризики» до уваги не беруться. Банальністю стали констатації того, що, усуваючи одні небезпеки, людство автоматично породжує нові, ще проблематичніші. Глобалізація й інформаційна революція, істотно збільшивши ймовірність різноманітних вразливостей й ризиків, породили відчуття непевності й непередбачуваності майбутнього, відсутності раціонального вибору. Усе це дало підстави деяким західним соціологам уже наприкінці 80-х років XX століття сформулювати концепцію «світового суспільства ризиків» [1 — 2]. Йдеться про суспільство «пізнього капіталізму», у якому зникають традиційні класові поділи, орієнтація на високопродуктивну працю, прирощення багатства, а натомість виникає відчуття всезагальної небезпеки, страху й невпевненості.

Поворотним пунктом тут слід вважати 26 квітня 1986 р. — День Чорнобильської катастрофи, коли, з одного боку, було продемонстровано існування невидимої, безпосередньо не відчутної небезпеки, з другого, нечуваних раніше масштабів набуло маніпулювання проблемами безпеки в політичних цілях, замаскованe турботами про «простих людей». Провладні медіа наполягали тоді на небезпеках «радіофобії» (страху перед радіацією), антивладні — на небезпеках, пов'язаних із самою радіацією. Але ті й інші прислужилися (кожен по своєму) розвалові СРСР, який не зміг налагодити ефективний «кризовий інформаційний менеджмент», звівши проблему інформаційного супроводу катастрофи подібного масштабу до пропаганди «героїзму ліквідаторів». У будь-якому разі Чорнобиль став підтвердженням істини щодо регулювання сфер безпечного й небезпечного на рівні «колективного розуму». Іншим підтвердженням соціальної метаморфози із вектором, скерованим на формування суспільства «масового споживання ризиків», стали події 11 вересня 2001 р., внаслідок яких страхові компанії втратили 20 млрд. дол. США, що породило поняття «незастрахованих ризиків» («uninsurable»).

Ульріх Бек визначає ризик як «сучасний підхід до передбачення й контролю майбутніх наслідків людської діяльності» включно із «незумисними наслідками радикальної модернізації». Досить цікавим є спостереження автора щодо характеру «ризикованого суспільства», яке всіляко заохочує людей до азартних (ризикованих) форм поведінки, культивує її, але не здатне його контролювати. У. Бек при цьому підкреслює, що ризики у сучасному соціумі перетворилися на переважаючу форму політичної мобілізації, сучасний політичний дискурс, який замінив традиційний. Серед неприємних рис такого суспільства, на думку У. Бека, є й приємні, бо воно повертає людей до солідарного колективізму, адже їм доводиться разом долати небезпеки й зустрічати виклики й ризики. Оскільки офіційна влада зазвичай демонструє безсилля приборкати ризики, громадянське суспільство має нагоду вимагати від цієї влади відкритості, прозорості механізмів прийняття рішень. Зрештою, створюються приводи для співучасті у прийнятті рішень [2].

Марк Даніель вважає системні ризики («Compounded risk») «новими мета-нормами у мережево-організованому соціумі» (new meta-norm in a networked society) й наголошує на негативних аспектах ризиків, пов'язаних з корпоративними впливами на процеси прийняття рішень: вибір пріоритетів («пріоритизацію»), розміщення ресурсів, вкладення коштів тощо [5].

Національну безпеку України в інформаційній сфері слід розглядати як інтегральну цілісність чотирьох складових — персональної, публічної (суспільної), комерційної (корпоративної) й державної безпеки. Тому в процесі визначення характеру ризиків слід брати до уваги наступні елементи:

1. Стисле концептуальне пояснення зацікавленим суб'єктам безпекової політики її принципів, стандартів та правил, погоджених із чинним законодавством й принципами забезпечення безперервності системи інформаційної безпеки особистості, суспільства, комерційних (корпоративних) структур та держави.

2. Визначення об'єктів та цілей.

3. Визначення прийнятних з погляду забезпечення інтересів усіх чотирьох суб'єктів

структур встановлення контролю над об'єктами безпеки, а також оцінки ризиків та управління ризиками.

4. Визначення статусно-функціональних ролей, очікувань та міри відповідальності задіяних суб'єктів включно зі звітністю про події, які несуть потенційні загрози.

Нижче наведено схему трирівневої архітектури безпеки, опрацьовану фахівцями з корпорації Erickson, позначену рисами універсальності, яка може бути успішно перенесена на сферу інформаційної безпеки України.

На вході (на схемі — справа) позначено напади на систему й різноманітні загрози, що стосуються семи вимірів інформаційної сфери (лівіше):

автентичність (справжність) — authentication;
авторизація — authorization;
підзвітність — accountability;
доступність — availability;
вірогідність — confidentiality;
цілісність — integrity;
безвідмовність та приватність — non-repudiation and privacy.

Як особливі виміри серед цих семи іноді виокремлюють ті, що англійською дають абревіатуру CIA (від англомовної назви ЦРУ):

вірогідність — confidentiality;
цілісність — integrity;
доступність — availability.

Звідси у «проекціях» на національну безпеку України маємо сім вимірів безпеки, пов'язаних із реалізацією таких завдань, як:

відповідність конституційним правам і свободам людини й громадянина;
ефективність інформаційного забезпечення державної політики;
доступ до інформації;
використання інформації;
захист інформації;
особиста безпека;
безпека інформаційних та телекомунікаційних засобів.

Нижче пропонується структурна схема поетапного становлення та функціонування системи інформаційної безпеки Української держави, яка виходить із тієї принципової настанови, що забезпечення безперервності та оперативної трансформації цієї системи залежить від її спроможності реагувати на нові виклики й ризики, що передбачає виконання основних стадій нагляду за системою забезпечення інформаційної безпеки держави, а саме:

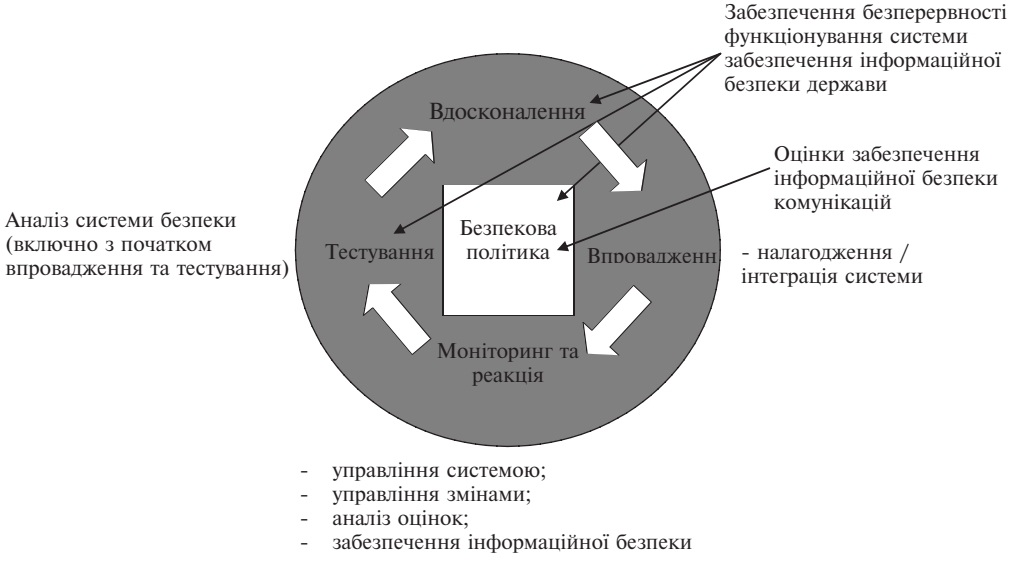
1. Безпосереднє впровадження механізмів забезпечення необхідного рівня безпеки.

2. Моніторинг системи та її реакцій на інциденти (події) і впровадження безпекової політики із використанням ефективних інструментів відстеження різноманітних «вторгнень».

3. Тестування системи безпеки через постійне вдосконалення аудиту.

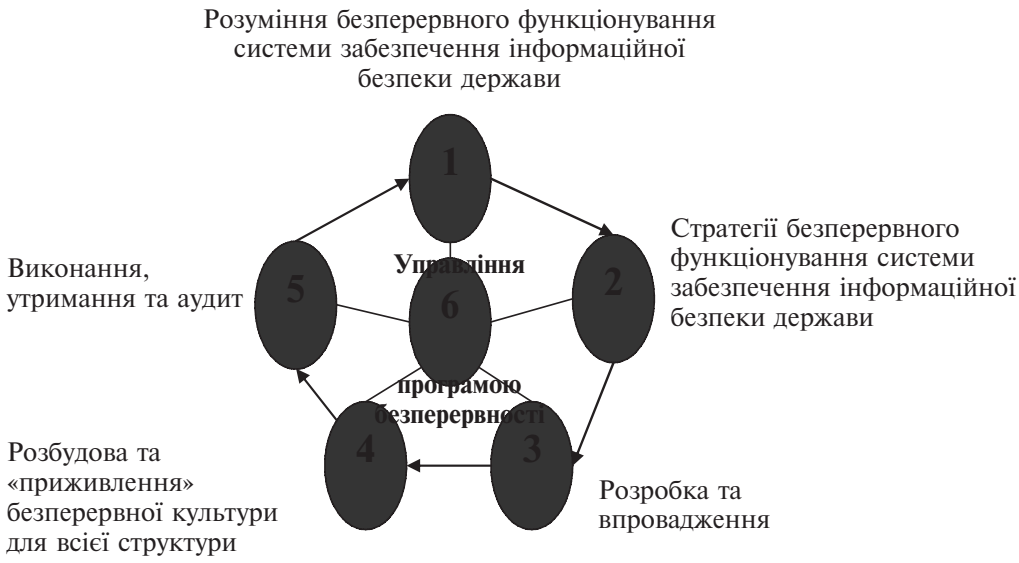
4. Вдосконалення системи — інформація збирається з попередніх етапів для аналізу та використання у подальшому вдосконаленні системи.

Графічно загальну схему створення ефективної системи інформаційної безпеки держави можна подати так:



Забезпечення безперервності функціонування системи інформаційної безпеки держави є одним із основних завдань державної політики у сфері як національної безпеки загалом і забезпечення інформаційної безпеки держави зокрема.

Процес забезпечення такої безперервності можна поділити на шість основних стадій, що схематично виглядає так:



1. Розуміння безперервності функціонування системи забезпечення інформаційної безпеки держави. Ця фаза пов'язана з ідентифікацією критично важливих точок (об'єктів) захисту. Йдеться також про виокремлення основних зовнішніх та внутрішніх загроз, що можуть стати критичними для системи.

2. Стратегії забезпечення безперервності функціонування системи: завдання зосереджуються на визначенні та доборі альтернативних рішень щодо відновлення системи з метою мінімізації загроз основних точок захисту. Пошук рішень балансує між собівартістю систем захисту та їхньою ефективністю.

3. Розробка та впровадження. На цій фазі зусилля зосереджуються на структуруванні та документуванні Програми безперервності державного управління

4. Розбудова та «приживлення» безперервної культури інформаційної безпеки держави. На цій стадії йдеться про запуск власне самого процесу розбудови інтегральної системи забезпечення інформаційної безпеки держави.

5. Виконання, підтримання та аудит праць із впровадження точного регулювання (поліпшення, трансформації) Стратегії безперервного функціонування системи інформаційної безпеки держави за умов різноманітних криз.

6. Управління програмою інформаційної безпеки держави шляхом розподілу та перерозподілу статусів та ролей, що передбачає відповідальність, підзвітність, страхування (гарантії) та керування у контексті реалізації загального плану безперервності функціонування системи забезпечення інформаційної безпеки держави. Ця стадія необхідна для чіткого визначення безперервної координації та управління всіма завданнями, пов'язаними із функціонуванням системи забезпечення інформаційної безпеки держави.

Повноцінний аналіз загроз національній безпеці України в інформаційній сфері можливий лише з урахуванням подальшого синтезу показників усіх вищезазначених індикаторів і передбачає можливість створення комплексної моделі загроз Україні в інформаційній сфері та комплексної стратегії їх нейтралізації.

Отже, фрагментарний підхід до проблеми забезпечення інформаційної безпеки держави створює загрозливу ситуацію, оскільки надає змогу ворожим щодо цієї держави суб'єктам здійснювати її послідовну «віртуальну десуверенізацію» (передусім через медіа-поле), що може призвести до істотних втрат держави у сферах реальної політики й економіки через погіршення інвестиційної привабливості, іміджу держави, численні інформаційні війни тощо.

Відповідно, критично важливою є необхідність практичної реалізації наведеної вище схеми створення ефективної системи інформаційної безпеки держави. З цією метою доцільне опрацювання «Доктрини національної інформаційної безпеки України» з чітким визначенням зон (сфер) відповідальності органів виконавчої влади щодо забезпечення кожного з етапів функціонування інформаційної безпеки держави згідно з наведеною схемою. Предметом постійної уваги в межах визначеного доктриною часового проміжку має стати перегляд списку «Загрози національній безпеці України в інформаційній сфері» як щодо нових загроз, так і усунення наявних із визначенням ступеня можливих наслідків та рівнів інтенсивності.

З огляду на те, що проблема забезпечення безперервності функціонування системи забезпечення інформаційної безпеки держави є ключовою, пріоритетним є також створення стратегії безперервного функціонування системи забезпечення інформаційної безпеки держави, основною метою якої має бути визначення та добір альтернативних рішень щодо створення/відновлення основних точок захисту системи національної безпеки в інформаційній сфері. Пошук рішень має бути продиктований балансом собівартості подібної системи захисту та її ефективності. З метою практичної реалізації зазначеної стратегії слід створити інтегрований у вертикаль виконавчої влади спеціальний орган, який здійснював би її практичну реалізацію і на який, окрім функції впровадження, були покладені обов'язки запуску власне самого процесу розбудови інтегральної системи забезпечення інформаційної безпеки держави, контролю за її виконанням та формулювання нових редакційних версій стратегії з урахуванням кардинальних змін у геостратегічній ситуації України.

Джерела

1. *Бек У.* От индустриального общества к обществу риска / Пер. А. Д. Ковалева // THESIS. — 1994. — № 5. — С. 161 — 168.
2. *Beck U.* World Risk Society. — Polity Press, Malden, 1999. — P. 3 — 4, 44, 51, 72.
3. *Гидденс Э.* Судьба, риск и безопасность // THESIS. — 1994. — Вып. 5. — С. 107 — 134.
4. *Giddens A.* The Consequences of Modernity. — Cambridge: Polity Press, 1991.
5. *Kaniell M. H.* World of Risk: Next Generation Strategy For A Volatile Era. John Wiley & Sons (Asia). — Singapore, 2000. — P. 10, 12, 18.
6. *Луман Н.* Понятие риска / Пер. А. Ф. Филиппова // THESIS. — 1994. — № 5. — С. 149.
7. *Катастрофическое* сознание в современном мире в конце XX века / Ред.: Шляпентох В. Э., Шубкин В. Н., Ядов В. А. — М.: Московский общественный научный фонд, Издательский центр научных и учебных программ, 2002.
8. *Ковалева М. С.* Эволюция понятия «риск» // Социологическое обозрение. — 2002. — № 1. — Декабрь.