УДК 355/359.07 DOI: https://doi.org/10.33099/2304-2745/2022-2-75/47-55)

Сніцаренко П. М., доктор технічних наук, старший науковий співробітник (0000-0002-6525-7064)
Саричев Ю. А., кандидат технічних наук, старший науковий співробітник (0000-0003-1380-4959)
Зубков В. П. (0000-0003-1616-2795)
Піщанський Ю. А. (0000-0003-4392-3318)

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

Методичний підхід до управління ризиками безпеки інформації як складової забезпечення інформаційної безпеки держави

Резюме. У статті розглядається проблема безпеки інформації як складової інформаційної безпеки держави. Висвітлюються основні аспекти безпеки інформації, сутність і характеристики ризиків безпеки інформації. Пропонується методичний підхід до створення системи управління ризиками безпеки інформації, що базується на кібернетичній моделі функціонування такої системи.

Ключові слова: безпека інформації; ризики безпеки інформації; управління ризиками.

Постановка проблеми. Забезпечення національної безпеки держави пов'язане, поряд з іншим, з використанням значного інформаційного ресурсу, що спричиняє підвищену потребу інформаційної безпеки держави. При цьому під *інформаційною безпекою держави* слід розуміти стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через певну сукупність негативних чинників [1], а *забезпечення інформаційної безпеки держави* – це цілеспрямована та узгоджена діяльність органів державного управління, інших визначених суб'єктів інформаційної діяльності щодо розроблення та реалізації комплексу заходів (дій) з метою створення умов отримання і захисту в інформаційному просторі необхідних інформаційних ресурсів для реалізації інформаційного забезпечення процесів управління відповідно до функцій і завдань, визначених законодавством [2]. Забезпечення інформаційної безпеки держави має бути спрямовано на складові, які визначають її рівень – розвиток інформаційної інфраструктури, отримання та використання інформаційних ресурсів, безпеку інформації (інформаційних ресурсів).

У сучасних умовах до інформації, яка циркулює в інформаційному просторі між об'єктами та суб'єктами управління, висуваються особливі вимоги стосовно її основних властивостей: достовірності, доступності, повноти (достатності), цілісності, конфіденційності, порушення яких може становити загрозу інформаційній безпеці держави, реально призвести до нанесення значної шкоди в різних сферах життєдіяльності. Тому проблема безпеки інформації (БІ) як складової забезпечення інформаційної безпеки в загальній системі її забезпечення постає вкрай актуальною. При цьому під *безпекою інформації* розуміється стан захищеності інформації (інформаційних ресурсів) в інформаційній системі, коли стосовно неї (них) унеможливлюється або зменшується здатність скоєння несанкціонованих дій [2].

Одним зі стримуючих чинників у процесі вдосконалення систем управління на основі інформаційно-технологічних рішень є наявність супутніх загроз БІ та відповідних ризиків БІ, що потребує їх ідентифікації, оцінювання та нейтралізації або зменшення до прийнятного рівня.

Аналіз публікацій показує, що більшість дослідників розуміють ризик як кількісну міру безпеки або шкалу, за допомогою якої можна кількісно виміряти збитки, пов'язані з реалізацією загроз, які мають різноманітні джерела походження. За допомогою такої шкали можна порівнювати всі види загроз (ризиків) між собою і відповідно визначати рівень безпеки – міру захищеності [3–9]. Загалом же, під *ризиком* розуміють прогнозовану величину збитку, що може виникати внаслідок ухвалення рішень в умовах невизначеності та реалізації загрози [10]. Управління ризиками розглядається як раціональний захід зменшення величини такого збитку.

Нині методологія управління ризиком ґрунтується на виборі математичної моделі оцінювання ризику, що залежить від кожної конкретної загрози. Як наслідок, існує значна кількість як самих моделей, так і підходів щодо моделювання оцінювання ризику. Наразі, для формалізації ризику використовуються адитивно-мультиплікативні моделі, які пов'язують між собою ймовірність виникнення подій (загроз) і відповідних їм небажаних наслідків, про що йдеться, зокрема, у роботах [10, 11]. Зазначені моделі є складні, громіздкі, потребують відповідної підготовки персоналу, незручні для оперативного користування. Через наявність багатьох непрогнозованих, випадкових, суб'єктивних обставин відбуваються значні відхилення від очікуваного результату.

Зарубіжні дослідники, аналізуючи сучасні загрози БІ, визначили такі причини глобальних ризиків БІ: негативні наслідки технічного прогресу; підвищення вразливості з використання інформаційної інфраструктури та мереж; кібератаки або зловмисне програмне забезпечення; масові випадки шахрайства з використанням дезінформації, крадіжки даних тощо [11]. При цьому під *загрозою БІ* розуміють наміри, дії (бездіяльність) або явища та чинники, прояв яких може нанести шкоду наявній інформації (інформаційним ресурсам).

Проблематика виникнення загроз та ризиків у різних галузях, зокрема у сфері інформаційної безпеки, розробляється і у працях вітчизняних дослідників інформаційної безпеки (А. Б. Качинського, В. П. Горбуліна, Г. П. Ситника, О. М. Загорки, П. М. Сніцаренка, А. І. Семенченка та ін.), у яких наголошується на необхідності й актуальності системного підходу до захисту інформації, зниження ризиків для забезпечення обґрунтованості та послідовності заходів, запланованих для цього, забезпечення їх максимально ефективної реалізації. Водночас, на сьогодні вченими ще не розроблено уніфікованого підходу до управління ризиками БІ, зокрема у воєнній сфері. Тому пошук найбільш раціональних рішень продовжується.

Метою статті є формування методичного підходу до управління ризиками БІ в інформаційних системах як невід'ємної складової процесу забезпечення інформаційної безпеки держави.

Виклад основного матеріалу. У сучасних умовах практично всі галузі життєдіяльності держави можуть знаходиться під загрозою БІ (прикладами є неодноразові інформаційні атаки на інформаційні системи державних та приватних установ України), що безпосередньо впливає на рівень БІ та спричиняє відповідний ризик.

Можна стверджувати, що під *ризиком БІ* слід уважати прогнозовану величину інформаційного збитку, що може виникати внаслідок реалізації загроз БІ із-за несанкціонованих дій (доступу, зміни, вилучення, знищення). Урахування ризиків БІ (інакше кажучи, управління такими ризиками) забезпечить покращення процедури підтримки процесу прийняття управлінських рішень, дасть змогу підвищити якість реалізації практичних заходів.

У роботі [9] стверджується, що будь-який ризик БІ може бути спричинений сукупністю таких негативних факторів: наявністю та характером джерела загрози БІ, невизначеністю настання небезпечної події, невизначеністю механізму впливу, можливістю та рівнем заподіяння шкоди. Усю сукупність ризиків БІ можна умовно поділити на підставі характеристик їх певних чинників.

Чинниками, з якими пов'язується ризик БІ, є різні впливи на основні характеристики інформації [12] – це достовірність, достатність (повнота), цілісність, конфіденційність, доступність.

Достовірність – це властивість інформації відображати реальні об'єкти (процеси, явища) з необхідною точністю в межах певного рівня ймовірності випадку, що відображається. Ризик порушення достовірності інформації характеризується її можливостями відповідати істинним (безпомилковим) даним.

Достатність (повнота) – мінімальний, але достатній для прийняття рішення склад інформаційного продукту. Ризик порушення достатності інформації пов'язаний з кількістю інформації, достатньої для розуміння та прийняття обґрунтованого рішення користувачем (споживачем).

Доступність – це можливість доступу суб'єкта до інформації за запитом у будь-який час (можливість використання інформації, коли в цьому є необхідність). Ризик порушення доступності інформації залежить як від несправності обладнання і збоїв у програмному забезпеченні, так і від успішно реалізованих мережевих атак на інформаційну систему ззовні. Цей тип ризику залежить від надійності апаратних і програмних компонентів інформаційної системи та від рівня компетенції персоналу, керуючого їх роботою.

Цілісність – це властивість інформації зберігати її точність і повноту в умовах користування. Ризик порушення цілісності інформації характеризується можливостями відмови обладнання або програмного забезпечення, недосконалістю алгоритмів і ступенем надійності засобів доступу користувачів до інформаційної системи.

Конфіденційність – рівень захисту інформації від несанкціонованого доступу. Ризик порушення конфіденційності залежить від рівня алгоритмів автентифікації користувачів, імовірності недокументованих ситуацій під час роботи з інформаційною системою, недосконалості організаційної структури, недотримання керівних документів щодо захисту інформації і людського фактору.

Джерелами впливу на характеристики інформації є середовище виникнення ризиків БІ та стан інформаційних систем [12].

За *середовищем виникнення* такі ризики діляться на зовнішні та внутрішні.

До *зовнішніх ризиків БІ* відносяться ризики, які обумовлені політичною обстановкою навколо країни, відносинами між державами, економічною ситуацією на ринку, соціальним станом громадян тощо. Рівень таких ризиків визначається декількома складовими, які впливають на його загальну величину.

До *внутрішніх ризиків БІ* відносяться ризики, які залежать від безпосередньої діяльності структурного підрозділу (організації) і його персоналу. Серед них визначальними є *організаційні ризики* – це ризики, пов'язані з діяльністю персоналу, що експлуатує і обслуговує інформаційні системи, проблемами системи внутрішнього контролю, нечітко визначеними правилами робіт, – тобто ризики, пов'язані з внутрішньою організацією роботи структурного підрозділу (організації).

За *станом інформаційних систем* (під яким слід розуміти рівень дієздатності складових інформаційних систем) ризики БІ поділяються на апаратні та програмні.

Апаратні ризики виникають у разі виходу з ладу обладнання інформаційної системи (персональних комп'ютерів, серверів, вимірювальних засобів (сенсорів), мережевих комутаторів, маршрутизаторів тощо) та залежать від способів її експлуатації.

Програмні ризики безпосередньо пов'язані з порушеннями в роботі програмного забезпечення (операційних систем) інформаційної системи, діями шкідливого програмного забезпечення, а також впливом мережевих атак.

Усі види ризиків, як правило, можуть бути об'єктом управління, найкраще – адаптивного управління. Отже, йдеться про певну кібернетичну систему управління ризиками БІ, яка повинна мати у своєму складі орган управління, виконавчий орган, орган моніторингу (рис. 1). Об'єктом управління у такій системі якраз є рівень ризику БІ. Відповідно до основних положень теорії управління [13, 14] саме такий методичний підхід дає змогу найбільш результативно (адаптивно) управляти ризиками БІ як складової забезпечення інформаційної безпеки.

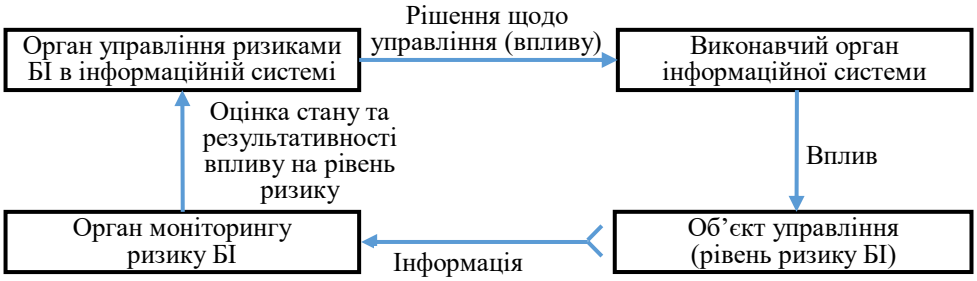

Рис. 1. Кібернетична модель функціонування інформаційної системи управління ризиками БІ

Кібернетична модель функціонування системи управління ризиками БІ базується на реалізації послідовності часткових функцій загального процесу управління ризиками БІ. Управляти ризиком БІ, відповідно до теорії управління [13–15], означає:

моніторити (виявляти, оцінювати джерела ризику);

проводити аналіз та оцінювання ризиків;

прогнозувати сценарії розвитку небезпечних подій;

приймати рішення за результатами аналізу ризиків;

упроваджувати заходи щодо запобігання, локалізації, нейтралізації або зменшення рівня ризиків до припустимої величини;

усувати наслідки небезпечних подій.

Варіант структурної схеми реалізації такого кібернетичного процесу, пов'язаного з управлінням ризиками БІ, складається з 4-х етапів (рис. 2).

Послідовність реалізації процесу управління ризиками БІ, відповідно до схеми на рис. 2, є такою:

1 етап процесу управління ризиками БІ є найбільш складним утворенням логічної послідовності окремих часткових функцій, коли *орган управління* на підставі виявлення, проведеного аналізу та оцінювання прогнозованої величини інформаційного збитку, який може виникати внаслідок реалізації загроз БІ, робить висновок щодо необхідності протидії, вибирає методи та заходи впливу на ризик БІ (підготовку пропозицій) та ухвалює рішення (затверджує висновок) щодо необхідності організації протидії. Розкриємо сутність елементів цього етапу.

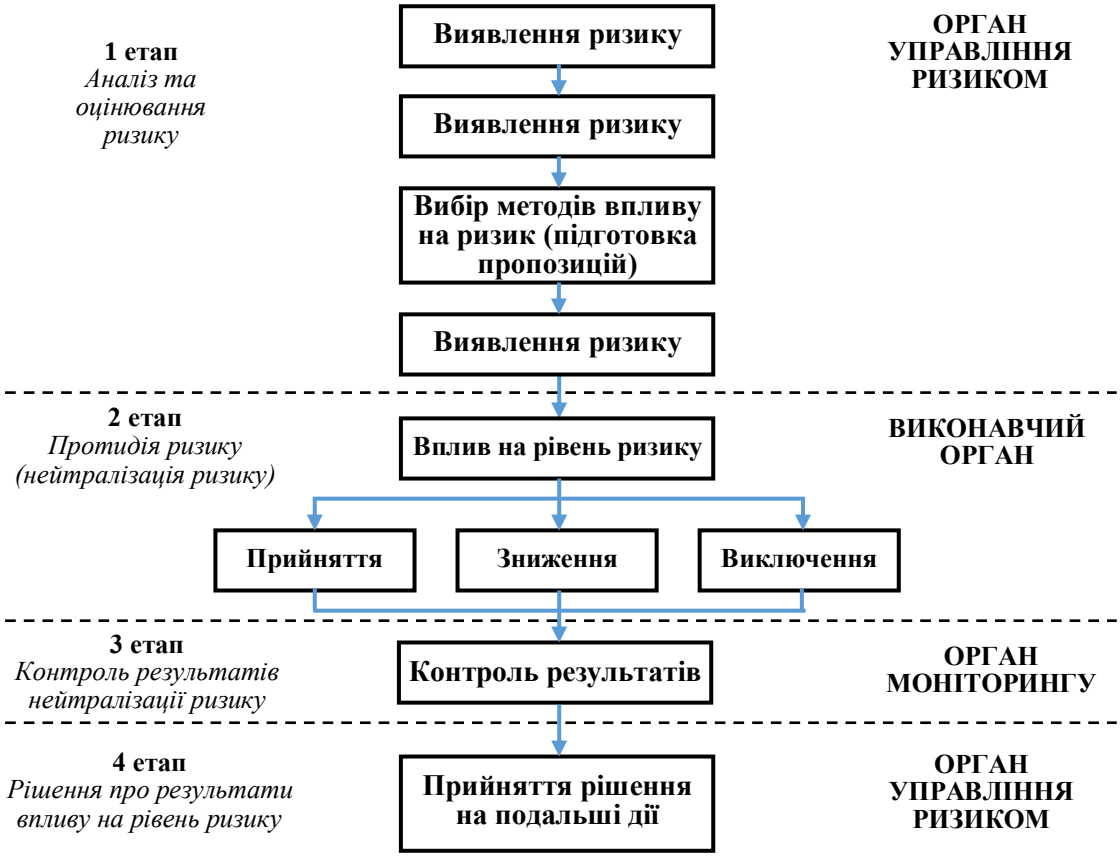

Рис. 2. Структурна схема процесу управління ризиками БІ (варіант)

Виявлення джерел загроз БІ та можливих ризиків БІ. Під час виявлення та ідентифікації джерел загрози БІ (хто чи що є причиною), об'єкта впливу (на який може діяти загроза БІ) та первинного аналізу ризику БІ необхідно оцінити можливість реалізації такої загрози. До того ж слід ураховувати:

частоту появи загрози БІ (як часто вона може виникати згідно зі статистичними, дослідними та іншими даними, якщо такі є);

мотивацію, можливості та інформаційні ресурси, необхідні потенційному порушнику та які, можливо, є в його розпорядженні;

ступінь привабливості та вразливості інформаційних активів з погляду потенційного порушника та джерела навмисної загрози БІ;

непереборні явища (стихійне лихо, епідемія), що можуть впливати на стан і якість інформаційних ресурсів.

Із завершенням цього процесу складається реєстр джерел загроз БІ, який використовується в системі управління ризиком для визначення заходів подальшої протидії, та оцінюється можливість їх реалізації. Також враховується перелік можливих внутрішніх вразливостей (щодо витоку, розголошення, спотворення або втрати інформації), зокрема:

незахищені підключення інформаційної системи до мережі Інтернет, локальних мереж;

недостатньо кваліфікований персонал;

недосконала організація доступу (належного контролю доступу) користувачів до обладнання та інформаційного ресурсу;

відсутність резервних копій даних (інформації) чи програмного забезпечення;

вихід з ладу елементів інформаційної системи тощо.

Оцінювання ризиків БІ здійснюється органом управління ризиком для вибору обґрунтованих методів нейтралізації відповідних загроз (негативного впливу) та забезпечення БІ в інтересах функціонування певної системи управління. Визначення рівня (значення) оцінки має виконуватися з урахуванням досвіду персоналу, вимог нормативно-правових документів, історії попередніх випадків порушення БІ, досвіду інших структурних підрозділів (організацій) тощо. Оцінювання проводиться для всіх видів ризиків БІ та документується у вигляді таблиці *для кожної часткової характеристики інформації*.

За метод оцінювання ризику, відповідно до Держстандарту [16], доцільно вибрати *матрицю наслідків* у зв'язку з її перевагами (порівняно проста в застосуванні та дає змогу швидко ранжувати ризики за різними рівнями важливості). Для побудови самої матриці необхідно сформувати кількісні шкали ранжування. За аналогією з [17–20], пропонуються шкали якості для оцінювання рівня можливості виникнення загроз БІ (Табл. 1) та рівнів їх впливу за умови реалізації на окремі властивості (характеристики) інформації (Табл. 2–6). Таке оцінювання рівнів за 5-ти бальною шкалою попередньо визначають експерти, зважаючи на інформацію про фактор загрози, причини, механізми та заходи щодо запобігання (зниження) ризику БІ.

Таблиця 1

Шкала ранжування оцінки можливості виникнення загроз БІ

Рівень (ранг) можливості виникнення загроз БІ	Зміст
1	Дуже низька (вкрай мало можлива)
2	Низька (мало можлива, не частіше 1 разу на місяць)
3	Середня (можлива, до 1 разу на тиждень)
4	Висока (достатньо можлива, до 1 разу на добу)
5	Надзвичайно висока (дуже можлива, більше 1 разу на добу)

Таблиця 2

Шкала ранжування наслідків реалізації загроз БІ (впливу) на достовірність інформації

Рівень (ранг) впливу	Зміст наслідків впливу
1 (мінімальний)	Рівень достовірності інформації високий, задовольняє процес управління
2 (незначний)	Рівень достовірності інформації достатній, але може мати несуттєвий негативний вплив на результат процесу управління
3 (середній)	Рівень достовірності інформації середній, що може мати помітний негативний вплив на результат процесу управління
4 (значний)	Рівень достовірності інформації низький, що може мати значний негативний вплив на результат процесу управління
5 (максимальний)	Рівень достовірності інформації дуже низький, що призводить до зупинки процесу управління

Таблиця 3

Шкала ранжування наслідків реалізації загроз БІ (впливу) на повноту інформації

Рівень (ранг) впливу	Зміст наслідків впливу
1 (мінімальний)	Рівень повноти інформації високий, задовольняє процес управління
2 (незначний)	Рівень повноти інформації достатній, але незначною мірою може негативно впливати на результат процесу управління
3 (середній)	Рівень повноти інформації середній, що певною мірою може негативно впливати на результат процесу управління
4 (значний)	Рівень повноти інформації низький, що значною мірою може негативно впливати на результат процесу управління
5 (максимальний)	Рівень повноти інформації дуже низький, що не задовольняє виконанню процесу управління та призводить до його зупинки

Таблиця 4

Шкала ранжування наслідків реалізації загроз БІ (впливу) на цілісність інформації

Рівень (ранг) впливу	Зміст наслідків впливу
1 (мінімальний)	Рівень цілісності інформації високий, задовольняє процес управління
2 (незначний)	Рівень цілісності інформації достатній, але незначною мірою може негативно впливати на результат процесу управління
3 (середній)	Рівень цілісності інформації середній, що певною мірою може негативно впливати на результат процесу управління
4 (значний)	Рівень цілісності інформації низький, що значною мірою може негативно впливати на результат процесу управління
5 (максимальний)	Рівень цілісності інформації дуже низький, що не задовольняє виконанню процесу управління та призводить до його зупинки

Таблиця 5

Шкала ранжування наслідків реалізації загроз БІ (впливу) на конфіденційність інформації

Рівень (ранг) впливу	Зміст наслідків впливу
1 (мінімальний)	Рівень конфіденційності інформації високий, не призводить до розкриття змісту документів з обмеженим доступом та негативних наслідків процесу управління
2 (незначний)	Рівень конфіденційності інформації достатній, але може призвести до часткового розкриття змісту документів з обмеженим доступом та незначного порушення процесу управління
3 (середній)	Рівень конфіденційності інформації середній, що може призвести до опосередкованого розкриття змісту документів з обмеженим доступом та помітного порушення процесу управління
4 (значний)	Рівень конфіденційності інформації низький, що може призвести до значного розкриття змісту документів з обмеженим доступом та порушення процесу управління в цілому
5 (максимальний)	Рівень конфіденційності інформації дуже низький, що призводить до розкриття змісту документів з обмеженим доступом загалом та зриву процесу управління

Таблиця 6

Шкала ранжування наслідків реалізації загроз БІ (впливу) на доступність інформації

Рівень (ранг) впливу	Зміст наслідків впливу
1 (мінімальний)	Рівень доступності інформації високий, задовольняє процес управління
2 (незначний)	Рівень доступності інформації достатній, але незначною мірою може негативно впливати на результат процесу управління
3 (середній)	Рівень доступності інформації середній, що може помітно негативно впливати на результат процесу управління
4 (значний)	Рівень доступності інформації низький, що значною мірою може негативно впливати на результат процесу управління
5 (максимальний)	Рівень доступності інформації дуже низький, що не задовольняє виконанню процесу управління та призводить до його зупинки

Отримані дані оцінювання якісних значень рівнів можливостей виникнення загроз БІ та їх впливу на окремі властивості інформації (шкали ранжування, див. Табл. 1–6) є основою для формування матриці наслідків (оцінювання рівнів ризиків БІ) за кожною з її властивостей. На основі [16], користуючись наведеною 5-ранговою шкалою, формують числову матрицю оцінювання ризику шляхом множення числових значень відповідних рядків і стовпців (рангів), що дає умовне числове значення рівня ризику БІ для кожної властивості інформації в діапазоні від 1 до 25, тобто від найменшого рівня ризику до найвищого. Через кількісні значення матриці виникає можливість якісного оцінювання рівня ризику БІ, зокрема на основі застосування узагальненої функції бажаності Харрінгтона [21, 22]. Шкала бажаності Харрінгтона є універсальною вербально-числовою шкалою (Табл. 7), яка застосовується переважно у випадках, коли оцінки носять суб'єктивний характер.

Таблиця 7

Вербально-числова шкала Харрінгтона

Опис градацій імовірності	Числове значення ймовірності
1. Дуже низька	0 – 0,19
2. Низька	0,20 – 0,36
3. Середня	0,37 – 0,63
4. Висока	0,64 – 0,80
5. Дуже висока	0,80 – 1,0

Користуючись шкалою Харрінгтона (Табл. 7), визначаються 5 *якісних рівнів ризику БІ* за такою числовою шкалою (Табл. 8):

"дуже низький" рівень – 1 – 4 (1/25 = 0,04; 4/25 = 0,16);
"низький" рівень – 5 – 9 (5/25 = 0,2; 9/25 = 0,36);
"середній" рівень – 10 – 16 (10/25 = 0,4; 16/25 = 0,64);
"високий" рівень – 20 (20/25 = 0,80);
"критичний" рівень – 25 (25/25 = 1).

Таблиця 8

Матриця якісного оцінювання рівнів ризиків БІ

Рівень (ранг) можливості виникнення загрози БІ						
	Дуже високий (5)	*5 Низький*	*10 Середній*	*15 Середній*	*20 Високий*	*25 Критичний*
	Високий (4)	*4 Дуже низький*	*8 Низький*	*12 Середній*	*16 Середній*	*20 Високий*
	Середній (3)	*3 Дуже низький*	*6 Низький*	*9 Низький*	*12 Середній*	*15 Середній*
	Низький (2)	*2 Дуже низький*	*4 Дуже низький*	*6 Низький*	*8 Низький*	*10 Середній*
	Дуже Низький (1)	*1 Дуже низький*	*2 Дуже низький*	*3 Дуже низький*	*4 Дуже низький*	*5 Низький*
		Мінімальний (1)	Незначний (2)	Середній (3)	Значний (4)	Максимальний (5)
		Рівень (ранг) впливу на характеристики (властивості) інформації				

Таким чином, цією матрицею (див. Табл. 8) формується *набір значень якісних оцінок рівня ризику БІ*, справедливий для застосування до будь-якої з характеристик (властивостей) інформації, і вона дає змогу оперативно з відносною якістю оцінювати "вагомість" ризиків стосовно кожної властивості інформації для прийняття відповідного рішення.

Слід зауважити, що наявність неприпустимого рівня ризику БІ (наприклад, "високий" чи "критичний"), принаймні за однією властивістю інформації, потребує відповідного реагування. Тому для рішення щодо реагування достатньо обмежитися розрахунком матриці стосовно кожної властивості інформації окремо і не ускладнювати процес оцінювання до інтегрального (за усіма властивостями сукупно).

Результатом оцінювання ризиків БІ є реєстр таких ризиків для кожного можливого випадку порушення достовірності, повноти, цілісності, конфіденційності, доступності інформації в діючій системі управління. Цей реєстр використовується як підстава для формування висновків у процесі вибору комплексу заходів забезпечення БІ під час виконання етапів реалізації процесу управління, пов'язаного з протидією ризикам БІ.

Вибір методів (заходів) впливу на ризик БІ орган управління здійснює відповідно до висновку щодо рівня ризику БІ для забезпечення стійкого функціонування усієї інформаційної системи та підвищення її надійності.

Якщо на підставі аналізу та оцінювання ризику БІ прийнято рішення про необхідність зниження його рівня, то готуються пропозиції про вжиття комплексу заходів для доведення рівня такого ризику до необхідного значення ("низького" на практиці). Зазначені пропозиції розробляються фахівцями експертної групи. Розроблення цього комплексу заходів потребує вивчення можливості зниження рівня ризику БІ за умови прийняття всіх доступних методів. До того ж вплив на зменшення ризику БІ здійснюється через різні сфери: фізичне навколишнє середовище; апаратні засоби (програмне забезпечення); елементи інформаційної інфраструктури (засоби забезпечення комунікації); обслуговуючий персонал (адміністрацію).

Для визначення заходів впливу на рівень ризику БІ необхідно розглянути вразливості системи (інформаційних активів), що потребують захисту, та види загроз, які можуть реалізуватися за наявності цих вразливостей, а також економічну складову (вартість, витрати матеріальних ресурсів та ін.) того чи іншого заходу.

До напрямів зниження рівня ризиків БІ належать:

уникнення ризику;

зниження рівня загроз;

зниження ступеня вразливості інформаційної системи (інформаційних ресурсів);

зниження можливого впливу непереборних подій (стихійного лиха, зухвалої агресії тощо).

Заходи за напрямами можуть бути організаційні та технічні.

Організаційні заходи передбачають наявність контрольованих методів розроблення та впровадження прикладних програм, процедур оброблення інцидентів під час порушення в інформаційній системі, контролю за роботою персоналу, його

навчання, інструкції щодо захисту від ризиків БІ, безпечні способи ведення документації.

Технічні заходи передбачають всебічний захист елементів інформаційної системи: апаратних засобів, програмного забезпечення та засобів забезпечення системи зв'язку (комунікації).

Ухвалення рішення щодо необхідності організації протидії по кожному ризику БІ приймається органом управління за бінарним принципом:

а) оцінений ризик *несуттєвий* (значення індексу ризику потрапляє в діапазон рівня прийнятних ризиків), ним можна знехтувати і не слід розробляти заходів щодо його зниження;

б) оцінений ризик *суттєвий* (неприйнятний) і необхідно визначити та здійснити заходи для його зниження і подальшого контролю його рівня.

2 етап процесу управління здійснюється *виконавчим органом* та спрямований на реалізацію заходів протидії ризику БІ (*вплив на рівень ризику БІ*), сутність яких полягає у нейтралізації (зменшені) оціненого рівня ризику БІ шляхом застосування попередньо визначеного (на 1-му етапі) комплексу заходів.

Основними напрямами впливу на рівень ризику БІ є:

прийняття оціненого ризику (підготовка фінансових, матеріальних та інших ресурсів на випадок появи небезпечних ситуацій);

зниження оціненого ризику (проведення заходів щодо запобігання небезпечним ситуаціям, розроблення систем їх локалізації);

виключення оціненого ризику (використання більш безпечних технологій, удосконалення захисних програм, дублювання (резервування) елементів інформаційної системи і т. ін.).

3 етап процесу управління (*контроль результатів нейтралізації ризику БІ*) виконується *органом моніторингу*, який постійно контролює результативність впливу на рівень ризику БІ. Сутність виконання 3-го етапу полягає в оцінюванні результатів зменшення (нейтралізації) ризику БІ та наданні об'єктивної інформації про цей стан органу управління ризиком.

4 етап – *орган управління* на підставі даних, отриманих від органу моніторингу щодо результатів зменшення (нейтралізації) рівня ризику БІ, приймає *рішення про результати впливу на рівень ризику БІ* та робить висновок щодо необхідності подальших управлінських дій.

Таким чином, запропонована 4-етапна схема дозволяє реалізувати адаптивну систему управління ризиками БІ на основі якісної оцінки ризиків БІ з метою вибору обґрунтованих шляхів протидії цьому ризику у певній інформаційній системі, чим забезпечується послідовність системних заходів його нейтралізації.

Висновки

1. Дестабілізуючі зовнішні та внутрішні чинники можуть викликати ризики БІ в інформаційній системі (інформаційних ресурсах) по основних характеристиках інформації (достовірність, повнота, цілісність, конфіденційність, доступність), тому управління такими ризиками є важливою складовою забезпечення інформаційної безпеки держави.

2. Запропонований методичний підхід, який базується на кібернетичному принципі управління, дає змогу створити систему адаптивного управління ризиками БІ як важливий елемент забезпечення інформаційної безпеки певної інформаційної системи. Вона повинна мати у своєму складі орган управління, виконавчий орган, орган моніторингу та об'єкт управління – рівень ризику БІ. Така система базується на алгоритмі формування набору значень (матриці) якісних рівнів ризику БІ (за основними характеристиками інформації) з метою вибору обґрунтованих рішень протидії таким ризикам.

3. Реалізація запропонованого процесу управління ризиками БІ забезпечить покращення підтримки прийняття рішень щодо нейтралізації (зменшені) ризику в будь-яких інформаційних системах, що дасть змогу підвищити рівень забезпечення інформаційної безпеки держави загалом.

4. Подальші дослідження слід зосередити на визначенні переліку та сутності комплексу заходів щодо реалізації протидії ризикам БІ за кібернетичним принципом управління.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : Закон України від 09.01.2007 р. № 537-V. URL: http://zakon.rada.gov.ua/ laws/show/537/2007 (дата звернення: 04.06.2022).
2. ВСТ 01.004.004 – 2014 (01). Інформаційна безпека держави у воєнній сфері. Терміни та визначення. Чинний від 2014-02-28. Київ : МОУ, 2014. 24 с.
3. Мінцберг Г. Зліт і падіння стратегічного планування. Київ : Видавництво Олексія Капусти, 2008. 412 с.
4. Семенченко А. І. Методологія стратегічного планування у сфері державного управління забезпеченням національної безпеки України. Київ : НАДУ, 2008. 429 с.

5. Вишняков Я. Д., Радаев Н. Н. Общая теория рисков. Москва : Академия, 2008. 368 с.
6. Цуркан В. В. Функціональний підхід до моделювання процесу менеджування ризику безпеки інформації // Информационные технологии и безопасность. Оценка состояния : материалы Междунар. конф. ИТБ-2013. Киев : ИПРИ НАН Украины, 2013. С. 193–194.
7. Качинський А. Б. Безпека, загрози та ризик. Київ : ІПНБ РНБО; НА СБ України, 2004. 472 с.
8. The Global Risks Report 2018 13th Edition. URL: http://www3.weforum.org/docs/WEF_GRR18 _Report.pdf (дата звернення: 07.06.2022).
9. Хмелевський Р. М. Дослідження оцінки загроз інформаційній безпеці об'єктів інформаційної діяльності // Сучасний захист інформації. 2016. № 4. С. 65–70.
10. Горбулін В. П., Качинський А. Б. Стратегічне планування: вирішення проблем національної безпеки : монографія. Київ : НІСД, 2010. 288 с.
11. Кравченко М. О., Бояринова К. О., Копішинська К. О. Управління ризиками : навч. посіб. Київ : НТУУ "КПІ ім. Ігоря Сікорського", 2021. 432 с.
12. Грінченко Є. М., Колмик О. О. Методи управління інформаційними ризиками // Комп'ютерна інженерія і кібербезпека: досягнення та інновації : матеріали Всеукр. наук.-практ. конф. здобувачів вищої освіти й молодих учених (м. Кропивницький, 27–29 листопада 2018 р.) / М-во освіти і науки України, Держ. наук. установа "Інститут модернізації змісту освіти", Центральноукраїн. нац. техн. ун-т. Кропивницький : ЦНТУ, 2018.
13. Винер Н. Кибернетика или управление и связь в животном и машине. Москва : Сов. Радио, 1968. 328 с.
14. Глушков В. М. Кибернетика. Вопросы теории и практики. Москва : Наука, 1986. 488 с.
15. Єжова Л. Ф. Економічні аспекти ризиків інформаційної безпеки // Сучасна спеціальна техніка. 2011. № 3 (26). С. 80–91.
16. ДСТУ IEC/ISO 31010:2013. Керування ризиком. Методи загального оцінювання ризику. Національний стандарт України. Київ : Мінекономрозвитку України, 2015. 80 с.
17. Методика управління ризиками : затв. розпорядж. Криворізького міського голови 02.03.2015 р. № 75-р. URL: Режим доступу: https://so.kr.gov.ua ›osxfile (дата звернення: 05.06.2022).
18. Про затвердження методики системи управління якістю виконавчих органів Бердянської міської ради "Порядок управління ризиками та можливостями" : розпорядж. міського голови міста Бердянськ Запорізької обл. від 12.06.2018 р. № 225-р.
19. Методика управління ризиками для системи управління якістю при виготовленні виробів різного призначення / А. М. Денисенко, Г. С. Грінченко, Ю. С. Лис, В. М. Бурдейна // Системи управління, навігації та зв'язку. 2019. Вип. 3 (55). С. 25–30.
20. Нефьодова Л. Я. Застосування засад проектного управління в оборонному менеджменті : лекція // Проєктний офіс реформ Міністерства оборони України. Київ : МОУ, 2019.
21. Ахназарова С. Л., Гордеев Л. С. Использование функции желательности Харрингтона при решении оптимизационных задач химической технологии : учеб.-мет. пособ. Москва : РХТУ им. Д.И. Менделеева, 2003. 76 с.
22. Пичкалев А. В. Обобщенная функция желательности Харрингтона для сравнительного анализа технических средств // Исследования наукограда. 2012. № 1. С. 25–28.

Стаття надійшла до редакційної колегії 05.07.2022

The methodical approach to information security risk management as a component the state information security ensuring

Annotation

Ensuring the state national security is connected, among other things, with the use of a significant information resource, which entails an increased need for information security of the state. In modern conditions, special requirements are imposed on the information circulating in the information space between the objects and subjects of management regarding its basic properties: reliability, accessibility, completeness (sufficiency), integrity, confidentiality, the violation of which may pose a threat to the information security of the state, and actually lead to significant damage in various spheres of life. Therefore, the problem of information security (IS) as a component of information security in the overall system of its provision is extremely relevant.

The purpose of the article is to form a methodological approach to managing IS risks in information systems as an integral part of the process of ensuring the information security of the state.

The proposed methodological approach, based on the cybernetic principle of management, allows creating a system of adaptive IS risk management as an important element of ensuring the information security of a particular information system. It should include a governing body, an executive body, a monitoring body and a management object – the level of IS risk. Such a system is based on an algorithm for forming a set of values (matrix) of qualitative levels of IS risk (according to the main characteristics of information) in order to select reasonable solutions to counteract such risks.

The implementation of the proposed IS risk management process will provide better decision-making support for neutralizing (reducing) risks in any information systems, which will increase the level of information security of the state as a whole.

Further research is planned to focus on determining the list and essence of a set of measures to implement counteraction to IS risks based on the cybernetic management principle.

Keywords: information security; information security risks; management of risks.