



МІНІСТЕРСТВО
ВНУТРІШНІХ СПРАВ
УКРАЇНИ
ОДЕСЬКИЙ ДЕРЖАВНИЙ
УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

Наталія СВИРИДЮК

В'ячеслав НЕКРАСОВ

Дмитро АФОНІН

**Оцінювання ризиків
поширення кримінальних
загроз, спроможностей та
прогнозування протидії цим
загрозам**

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ



Одеса

2024

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

**Оцінювання ризиків поширення
кримінальних загроз,
спроможностей та прогнозування
протидії цим загрозам**

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ

УДК: 343.9:343.851(072)(477)
С24

Погоджено на засіданні науково-дослідної лабораторії з актуальних питань кримінального аналізу навчально-наукового інституту підготовки фахівців кримінальної поліції Національної поліції України Одеського державного університету внутрішніх справ.
(Протокол № 12 від 13 грудня 2024 р.)

Схвалено та рекомендовано до друку
Науково-методичною радою
Одеського державного університету внутрішніх справ.
(Протокол № 6 від 23 грудня 2024 р.)

Авторський колектив:

Н.П. Свиридюк доктор юридичних наук, професор, старший науковий співробітник науково-дослідної лабораторії з актуальних питань кримінального аналізу Навчально-науковий інституту підготовки фахівців кримінальної поліції НПУ Одеського державного університету внутрішніх справ;

В.А. Некрасов кандидат юридичних наук, професор, професор кафедри кримінології та кримінально-виконавчого права Національної академії внутрішніх справ;

Д.С. Афонін кандидат юридичних наук, доцент, завідувач науково-дослідної лабораторії з актуальних питань кримінального аналізу Навчально-науковий інституту підготовки фахівців кримінальної поліції НПУ Одеського державного університету внутрішніх справ.

Рецензенти:

О.А. Балтовський – доктор технічних наук, доцент, професор кафедри кримінального аналізу та інформаційних технологій Одеського державного університету внутрішніх справ;

В.Ю. Калугін кандидат юридичних наук, доцент, професор кафедри кримінального аналізу та інформаційних технологій Одеського державного університету внутрішніх справ.

Оцінювання ризиків поширення кримінальних загроз, спроможностей та прогнозування протидії цим загрозам : методичні рекомендації / Н.П. Свиридюк, В.А. Некрасов, Д.С. Афонін,. — Одеса: ОДУВС, 2024.— 40 с.

Методичні рекомендації спрямовані на вдосконалення підходів до аналізу та управління ризиками у правоохоронній діяльності. У методичних рекомендаціях детально розглянуто методологію оцінювання кримінальних загроз, виявлення джерел небезпеки та прогнозування заходів для їх ефективної нейтралізації.

Актуальність теми обумовлена необхідністю формування сучасного правоохоронця (детектива, слідчого, оперативного працівника, аналітика) із глибокими знаннями системного підходу до управління безпекою. Рекомендації враховують впливи людського чинника, надійності системи та зовнішніх факторів небезпеки на загальний рівень безпеки. Основна мета — мінімізація ризиків, людських жертв, матеріальних втрат, а також екологічних і соціальних збитків.

Методичні рекомендації розраховані на правоохоронців, аналітиків та фахівців у сфері забезпечення безпеки. Вони стануть незамінним інструментом у побудові сучасної системи управління ризиками, яка відповідає міжнародним стандартам і сприяє підвищенню інтегрального рівня безпеки суспільства.

ЗМІСТ

Вступ	4
1. Методологічні засади застосування РОП	5
2. Загальні підходи та принципи застосування РОП	7
3. Оцінка ризиків	10
4. Усунення ризиків	11
5. Комплекс заходів з оцінювання ризиків (КЗОР)	14
6. Цикл РОП щодо забезпечення публічної безпеки і порядку, протидії злочинності	15
7. Управління аналізом ризиків	16
7.1. Стратегічний рівень	18
7.2. Оперативний рівень	19
7.3. Тактичний рівень	20
7.4. Етапи виконання аналізу ризиків	20
7.5. Методи ідентифікації ризиків	22
8. Управління ризиками	32
Список використаної літератури	38

ВСТУП

Сучасна правоохоронна діяльність потребує від фахівців глибоких знань та практичних навичок у сфері аналізу ризиків і управління ними. Процес формування компетентного правоохоронця, будь то детектив, слідчий, оперативний працівник чи аналітик, базується на розумінні складної системи взаємодії «правоохоронець – кримінальне явище». Ця система є ключовим інструментом управління безпекою, який враховує впливи людського чинника, надійності правоохоронної системи, а також зовнішніх факторів загроз на інтегральний рівень безпеки.

В основі управління безпекою лежить системний підхід, спрямований на виявлення джерел небезпеки, оцінювання чинників ризику та мінімізацію їхнього впливу. Зведення до мінімуму людських жертв, матеріальних, фінансових, екологічних і соціальних втрат є пріоритетним завданням сучасних правоохоронців.

Методичні рекомендації «Оцінювання ризиків поширення кримінальних загроз, спроможностей та прогнозування протидії цим загрозам» розроблено з метою вдосконалення підходів до виявлення та оцінювання кримінальних ризиків, аналізу їх впливу та прогнозування ефективних заходів протидії. Вони пропонують структурований алгоритм дій для правоохоронців і аналітиків, спрямований на забезпечення високого рівня безпеки у суспільстві.

Актуальність цих рекомендацій визначається зростаючою складністю кримінальних явищ і потребою у побудові сучасної системи управління ризиками, яка відповідає міжнародним стандартам. Документ стане важливим ресурсом для фахівців, що працюють у сфері забезпечення правопорядку та протидії злочинності.

1. МЕТОДОЛОГІЧНІ ЗАСАДИ ЗАСТОСУВАННЯ РОП

Процес формування сучасного правоохоронця (детектива (слідчого, оперативного працівника), аналітика) вимагає глибоких знань методології аналізу ризиків та управління ними, складної системи «правоохоронець – кримінальне явище», як сучасного інструментарію управління безпекою, в якій враховуються впливи людського чинника, надійності системи, зовнішніх факторів небезпек на інтегральний рівень безпеки. В основі управління безпекою лежить системний підхід до виявлення джерел небезпеки і контролю чинників ризику на користь зведення до мінімуму людських жертв, матеріального збитку, а також фінансових, екологічних і соціальних втрат.

Ключовим моментом впровадження **РИЗИК-ОРІЄНТОВАНОГО ПІДХОДУ (далі РОП)** в Україні в питаннях протидії злочинності стало прийняття Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» (п.53 ч.1 ст.1, п.3 ч.1 ст.3, ст.7) [1], а також включення в Закон України «Про Бюро економічної безпеки України» 2021 р. [2] (п.7 ч.1 ст.1, ст.12), положень такого характеру, а видання Указу Президента України «Про запровадження національної системи стійкості» [3], лише посилило актуальність реалізації у правоохоронній практиці такого підходу.

Розглядати злочинність саме як кримінальну загрозу, а діяльність правоохоронних органів та інших суб'єктів контролю через призму спроможності державних інститутів щодо відвернення її проявів, допомагає сформувати принципово інші підходи до системи організації роботи правоохоронного сектору, зокрема в питаннях досудового розслідування, оперативно-розшукової діяльності, аналітичної діяльності та використання штучного інтелекту в правоохоронній практиці. У такому випадку реалізація превентивної функції в діяльності правоохоронних органів, що спрямована на мінімізацію кримінальних ризиків, стає цілком реалістичним проектом.

По-перше, ризик є однією з системоутворюючих складових національної, економічної, публічної безпеки, відповідно аналіз ризиків є інструментом вивчення складних соціально-економічних систем в умовах невизначеності. Ризик – це ймовірність виникнення негативного наслідку конкретної діяльності, загроза понесення певних збитків, результат впливу невизначеності на досягнення поставленої мети;

По-друге, складовими ризику є загроза як потенційна, можлива небезпека, що має намір та можливості заподіяти шкоду національній, економічній, публічній безпеці, котрі характеризуються масштабом (впливом) та ймовірністю її реалізації. Тобто йдеться про сили, явища та чинники, а такою є протиправна діяльність оргзлочинності, сама наявність яких вже передбачає застосування до них заходів з боку правоохоронних

органів, а також інших суб'єктів контролю ще під час формування наміру та визначення можливостей. При цьому ідентифікація уразливостей (проблеми, вади, недоліки) систем національної, економічної, публічної безпеки, які породжують або посилюють піддатливість негативним впливам загроз надає можливість визначити шляхи підвищення спроможності системи;

По-третє, в РОП ми завжди маємо справу з ймовірнісними категоріями, розрахунками можливого впливу та працюємо над тим, щоб не допустити реалізацію загрози, мінімізувати її вплив або мінімізувати наслідки;

По-четверте, виходячи з принципу контрінтуїтивної поведінки Дж. Форрестера (1974, 1978), базуючись на принципах роботи складних систем, якими є національна, економічна, публічна безпеки, дати задовільний прогноз поведінки складної системи на досить великому проміжку часу, спираючись тільки на власний досвід та інтуїцію, практично неможливо. Це пов'язане з тим, що наша інтуїція «вихована» на спілкуванні з простими системами, де зв'язки елементів практично завжди вдається простежити. Контрінтуїтивна поведінка складної системи полягає в тому, що вона реагує на вплив зовсім іншим чином, ніж це нами інтуїтивно очікувалося [4]. Тому інструментарій аналізу ризику яким повинні оперувати працівники правоохоронного органу побудовані на обробці великих масивів інформації саме штучним інтелектом (машиною) із застосуванням спеціальних методик та алгоритмів роботи.

По-п'яте, РОП також оперує інструментами, які надають можливість визначити зону компетенцій кожного суб'єкта контролю у забезпеченні національної, економічної, публічної безпеки, розкриваючи її через наявність або відсутність достатніх оперативних можливостей (людських, технічних ресурсів тощо), юридичних повноважень, компетентностей тощо.

Таким чином, метою розроблення методології із застосування РОП є опис системних підходів до оцінки ризиків національної, економічної, публічної безпеки, які базуються на поєднанні об'єктивних кількісних статистичних даних і суб'єктивних якісних експертних оцінок, аналізу агентурно-оперативної інформації правоохоронних органів (співбесіди, опитувальники), результатів розгляду кримінальних проваджень, оперативно-розшукових справ, заходів, які вживаються суб'єктами контролю у сфері забезпечення національної, економічної, публічної безпеки, приватним сектором та інших прикладів міжнародного співробітництва між правоохоронними органами з протидії кримінальним загрозам, а також іншої інформації з відкритих джерел. РОП призначений для структуризації аналізу доступної інформації про загрози, вразливості і можливі наслідки прояву ризиків, пов'язаних із забезпеченням національної, економічної, публічної безпеки, з метою покращення управлінської діяльності, обґрунтованого застосування заходів реагування на ризики та для впровадження основних

результатів міжнародних практичних і методологічних досліджень, а також для врахування національних особливостей застосування РОП у правоохоронній практиці.

Враховуючи вищезазначене, запровадження РОП саме у правоохоронній діяльності матиме значний економічний ефект, сприятиме вирішенню системних проблем, здатне постійно утримувати рівень компетентностей в актуальному стані.

2. ЗАГАЛЬНІ ПІДХОДИ ТА ПРИНЦИПИ ЗАСТОСУВАННЯ РОП

РОП – це визначення (виявлення), оцінка (переоцінка) та розуміння ризиків, а також вжиття відповідних заходів щодо управління виявленими ризиками у спосіб та в обсязі, що забезпечують мінімізацію таких ризиків залежно від їх рівня [2].

Застосування РОП правоохоронними органами, які опікуються питаннями забезпечення національної, економічної, публічної безпеки тощо, здійснюється у порядку, визначеному їх внутрішніми документами, з урахуванням підходів окреслених для центральних органів виконавчої влади, діяльність яких спрямовується і координується Кабінетом Міністрів України. Внутрішні документи повинні, містити програму управління ризиками національної, економічної, публічної безпеки, що враховує визначення ризиковості окремих осіб, груп, юридичних осіб та об'єктів, ризики процесів та діяльності, використання існуючих організаційних форм підприємництва у злочинних цілях, включаючи ризик використання технологічних досягнень, ризик-рішення та ризик-послуги розпорядників бюджетних коштів тощо.

Кінцевою метою застосування РОП є виявлення (актуалізація) кримінальних ризиків (загроз, вразливостей, наслідків) в системі забезпечення національної, економічної, публічної безпеки, визначення елементів управління ними та сприяння у розробці стратегії розвитку системи національної, економічної, публічної безпеки.

Ризик – ймовірність виникнення негативного наслідку конкретної діяльності, загроза понесення певних збитків, результат впливу невизначеності на досягнення поставленої мети. Ризик складається з імовірності реалізації загрози та вразливості об'єкта, якому загрожує загроза та результатів впливу.

Загроза – наявність сили, явищ та чинників, що мають намір та можливості заподіяти шкоду національній, економічній, публічній безпеці, котрі характеризуються масштабом та ймовірністю її реалізації.

Уразливість – наявність проблем, вад, недоліків системи, які породжують або посилюють схильність до порушення функціональності та/або піддатливість негативним впливам загроз національній, економічній, публічній безпеці. При їх оцінці одним із компонентів є негативний вплив, а іншим – механізм контролю.

Вплив – ймовірні (прогнозовані) наслідки реалізації загрози або виникнення інших явищ і чинників, які не становлять загрозу, але можуть вплинути на національну, економічну, публічну безпеку.

Це відображає рівень економічної, емоційної, фізичної, інтелектуальної та політичної шкоди, яка може статися у разі реалізації загрози. Рівень впливу залежить від рівня самої загрози, а також від вразливості об'єкта, що перебуває під загрозою, та його здатності відвернути загрозу.

Ймовірність – показник, який характеризує можливість реалізації певних подій, інцидентів, загроз або їх наслідків.

Компетентність – здатність, аналітика, детектива, керівника ефективно застосувати здобуті ними знання, уміння, навички для реагування на кримінальні загрози економічній безпеці на будь-якому етапі.

Механізм контролю – наявні знання та ресурси, що можуть бути використані для реагування на загрозу, підвищення стійкості та зменшення уразливості.

Можливість – це володіння знаннями та ресурсами, необхідними для реалізації наміру.

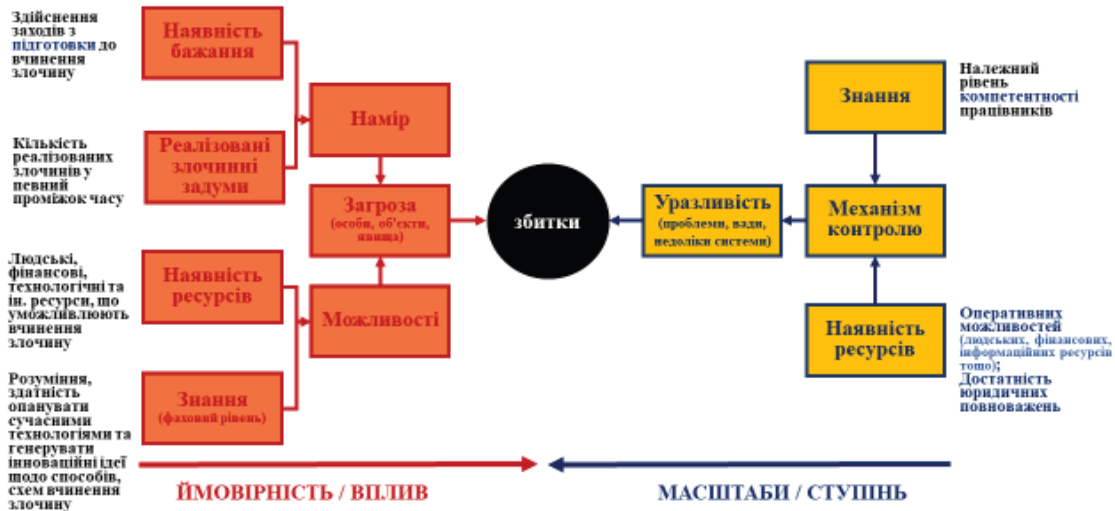
Намір – задум, бажання щось зробити або здійснити, передбачаючи та приймаючи наслідки.

Фактор ризику – це змінна, що підсилює виникнення, реалізацію та наслідки кримінальної загрози.

Принципами, які повинні бути покладені в основу такого підходу є:

- принцип безумовного пріоритету безпеки і збереження життя, здоров'я над будь-якими іншими елементами умов і якості життя членів суспільства;
- принцип прийнятного ризику (небезпеки), відповідно до якого встановлюються нижній (допустимий) і верхній (бажаний) рівні безпеки і в цьому інтервалі – прийнятний рівень ризику і безпеки з урахуванням соціально-економічних чинників;
- принцип мінімальної небезпеки, відповідно до якого рівень ризику встановлюється настільки низьким, наскільки він є реально досяжним;
- принцип послідовного наближення до абсолютної безпеки. [5]

Модель аналізу ризиків



Набір інструментів окреслених РОП правоохоронних органів передбачає встановлення рівня ймовірності вчинення злочинів підслідних ним з огляду на існуючі кримінальні загрози (особа (група осіб), об'єкт або діяльність, що здатні завдати шкоди національній, економічній, публічній безпеці, суспільству) та вразливості (фактори, що створюють умови для виникнення кримінальних загроз) системи протидії злочинам у різних сферах, а саме шляхом:

- а) раннього виявлення кримінальних загроз;
- б) достовірної оцінки можливості їх реалізації;
- в) встановлення вразливостей систем національної, економічної, публічної безпеки до кримінальних загроз;
- г) оцінки наслідків та масштабів реалізації кримінальних загроз у співвідношенні із ідентифікованими вразливостями системи національної, економічної, публічної безпеки;
- г) своєчасного усунення вразливостей системи національної, економічної, публічної безпеки;
- д) запобігання негативним наслідкам прояву кримінальних ризиків;
- е) визначення пріоритетних напрямів діяльності правоохоронних органів та інших інституцій забезпечення національної, економічної, публічної безпеки;
- є) прийняття рішень про найбільш ефективне використання оперативних можливостей (ресурсів) правоохоронних органів.

Застосування показника ризику дозволяє порівнювати дію шкідливих та небезпечних чинників національної, економічної, публічної безпеки різної природи і різного виду, визначати з урахуванням внеску кожного окремого чинника інтегральний ступінь небезпеки будь-якого об'єкту, системи, технології, проекту, діяльності, процесу тощо. Проводячи порівняння ризиків, наприклад, пов'язаних з зайняттям підприємницькою діяльністю у

неконкурентних умовах, з повсякденними кримінальними та корупційними ризиками, слід брати до уваги, що одні небезпеки приймаються суспільством добровільно (наприклад, оптимізація оподаткування), а інші - ні. Вельми важливо, що питання про сприйняття ризику істотно залежить від тих реальних вигод, які надає та або інша діяльність.

3. ОЦІНКА РИЗИКІВ

Правоохоронні органи повинні здійснити оцінку загроз організованої злочинності та тяжких злочинів (**СОСТА**), аналіз ризиків, а також разом з іншими суб'єктами контролю провести КЗОР відповідно до вимог діючого законодавства, особливо у разі якщо відповідно до вимог діючого законодавства вони визначені «національними координаторами». Наприклад, Національне антикорупційне бюро України може виступати «національним координатором» реалізації антикорупційної стратегії, Бюро економічної безпеки України – у забезпеченні економічної безпеки держави, Служба безпеки України – у забезпеченні національної безпеки, відповідно Національна поліція України – публічної безпеки тощо.

КМУ відповідно до діючого законодавства повинен призначити такі органи відповідальним за проведення КЗОР, з визначенням механізму координації такого заходу.

Національні координатори (визначені правоохоронні органи) за напрямом та інші суб'єкти контролю повинні регулярно здійснювати КЗОР з метою оновлення їх результатів.

Національні координатори повинні мати механізми комунікації за результатами проведення КЗОР з усіма суб'єктами контролю, зокрема правоохоронними органами та іншими суб'єктами державного регулювання.

4. УСУНЕННЯ РИЗИКІВ

Ґрунтуючись на власному розумінні своїх ризиків, суб'єкти контролю повинні застосовувати підхід, що ґрунтується на оцінці ризиків, при розподілі ресурсів та впровадженні заходів, спрямованих на запобігання та усунення ризиків національної, економічної, публічної безпеки.

Суб'єкти контролю, які приймають рішення не застосовувати деякі рекомендації КЗОР, у разі визначення їх власниками ризику, повинні продемонструвати, що:

а) доведено низький рівень ризику національної, економічної, публічної безпеки; виняток має місце у суворо обмежених та обґрунтованих обставинах; та він стосується тільки певної категорії юридичних осіб, суб'єктів господарювання, розпорядників бюджетних коштів, отримувачів міжнародної технічної допомоги або діяльності, або

б) фінансова (господарська) діяльність (окрім взаємовідносин з ОГ та ЗО) здійснюється фізичною або юридичною особою не регулярно або обмежено, процедури прийняття рішень та надання послуг суб'єктами контролю та суб'єктами державного регулювання транспарентні (беручи до уваги кількісний та абсолютний критерії), наприклад коли низький рівень ризику розкрадання бюджетних коштів та міжнародної технічної допомоги тощо.

Ознаки спроможності системи: правоохоронні органи та інші суб'єкти контролю належним чином визначають, оцінюють та розуміють свої ризики національної, економічної, публічної безпеки, а також здійснюють координацію заходів на національному рівні, спрямованих на мінімізацію або уникнення ризиків, а у разі неможливості, пом'якшення наслідків або забезпечення відшкодування збитків у разі реалізації загрози. Це включає залучення компетентних органів та інших відповідних органів; використання широкого спектру надійних джерел інформації; застосування оцінки ризиків як основи для розвитку та встановлення пріоритету стратегії та заходів з протидії злочинам; та впровадження цієї стратегії і заходів координованим шляхом через відповідні канали. Відповідні компетентні органи також співпрацюють та координують політику і заходи, спрямовані на діджиталізацію, зокрема системи надання публічних послуг, дозвільної та фіскальної систем тощо. З часом результатом цього стає значне пом'якшення ризиків національної, економічної, публічної безпеки.

Основні питання до розгляду при визначенні, чи досягнуто результат:

- *Наскільки вдало національні координатори та інші суб'єкти контролю усвідомлюють свої ризики національної, економічної, публічної безпеки?*

- *Наскільки вдало ідентифікуються ризики національної, економічної, публічної безпеки, що усуваються загальною стратегією забезпечення національної, економічної, публічної безпеки та заходами з протидії кримінальним загрозам?*

- В якій мірі та чи належним чином використовуються результати аналізу та оцінки ризиків, факторів, що впливають на ризик, для обґрунтування винятків та підтримки застосування посиленних заходів для випадків високого ризику або спрощених заходів для випадків низького ризику?

- В якій мірі цілі та заходи системи національної, економічної, публічної безпеки відповідають стратегіям забезпечення національної, економічної, публічної безпеки та протидії кримінальним загрозам, що розробляються, а також виявленим ризикам національної, економічної, публічної безпеки?

- В якій мірі національні координатори, інші суб'єкти контролю, громадські організації та суб'єкти підприємництва співпрацюють та координують розробку та впровадження стратегії і заходів, спрямованих на забезпечення прозорості фінансування виборчого процесу та політичних партій, оптимізації системи держуправління, а також спрощення процедур надання публічних послуг, детінізацію відносин в економіці та сфері управління публічними фінансами тощо?

- В якій мірі національні координатори та інші суб'єкти контролю забезпечують, щоб відповідні суб'єкти підприємства, суб'єкти державного регулювання та надання публічних послуг, окремі юридичні та фізичні особи, а також інші учасники сектору забезпечення національної, економічної, публічної безпеки, були обізнані про відповідні результати КЗОР?

Основними джерелами первинної інформації правоохоронного органу є бази даних державних органів, зокрема контролюючих та інших правоохоронних органів, результати власної кримінальної розвідки та розслідувань кримінальних проваджень, Європол, OLAF, CARIN тощо. Елементами системи національної, економічної, публічної безпеки, які сприймають перероблену і надану правоохоронним органом інформацію у формі аналітичного продукту як стимул для виконання певної дії, є сукупність суб'єктів контролю (власників ризику), а також західні правоохоронні органи.

Порядок пріоритетів при розробці будь-яких Стратегій розвитку вимагає, щоб вже на перших стадіях їх розробки або побудови системи національної, економічної, публічної безпеки, наскільки це можливо, були включені елементи, що мінімізують ризики вчинення кримінальних, зокрема корупційних, правопорушень. **На жаль, це не завжди можливо. Якщо ідентифіковану загрозу неможливо відвернути повністю, необхідно знизити ймовірність ризику до прийнятного рівня шляхом вибору відповідного рішення. Досягти цієї мети, як правило, в будь-якій системі чи ситуації можна кількома шляхами:**

- усунути джерело ризику, наприклад нейтралізувати вплив організованих груп та злочинних організацій;

- використовувати штучний інтелект з метою моніторингу загроз, прогнозування ризику та превентивного впливу на загрози;

- підвищити спроможність державних інституцій з мінімізації ризиків, розробити концепцію (структури) ризик-менеджменту, процесу управління ризиками, проводити моніторинг виконання необхідних дій, постійно вдосконалювати ризик-менеджмент;

- застосовувати заходи організаційно-управлінського характеру, інтегрувати політику ризик-менеджменту в загальну політику правоохоронного органу, встановити відповідальності та повноваження «власників ризиків» в системі ризик-менеджменту, запровадити протоколи ідентифікації ризику, формувати в такому ключі кадрову політику тощо.

Такий підхід до зменшення ризику зветься управлінням ризиком – це розроблення, на основі оцінювання ризиків, та реалізація управлінських рішень, спрямованих на мінімізацію таких ризиків, а також на підвищення спроможності державних інституцій щодо нейтралізації загроз національної, економічної, публічної безпеки. **З метою підвищення рівня безпеки, інституціональної спроможності суб'єктів контролю зусилля треба спрямовувати за трьома напрямками:**

а) надання достатніх юридичних повноважень та людських ресурсів, удосконалювання технічних систем та оперативних можливостей;

б) підвищення рівня компетентностей (підготовка кадрів);

в) ліквідація наслідків у разі неможливості відвернути загрозу.

Враховуючи вищезазначене можна сформулювати правила ризик-менеджменту національної, економічної, публічної безпеки, що забезпечується в межах компетенції правоохоронним органом:

✓ реагувати на ризики в межах інституціональних можливостей правоохоронного органу, а також інших суб'єктів контролю;

✓ враховувати наслідки ризику будь-якого втручання в систему публічних або суспільних відносин;

✓ втрати у разі реалізації загрози національної, економічної, публічної безпеки повинні співвідноситись з витратами на її додання або мінімізацію. Модель індексу витрат, що очікуються базується на вартості витрат у системі порівняно з вірогідністю втрат. Індекс втрат, що очікуються, у разі свідомого не реагування на ризик або відсутності можливості такого реагування;

✓ мати декілька варіантів впливу на ризики національної, економічної, публічної безпеки: або використовувати інструменти превентивного впливу або кримінального переслідування;

✓ приймати рішення щодо впливу на ризик лише у разі відсутності сумніву.

5. КОМПЛЕКС ЗАХОДІВ З ОЦІНЮВАННЯ РИЗИКІВ (КЗОР)

З метою побудови ефективної системи стратегічного менеджменту в забезпеченні національної, економічної, публічної безпеки на середньострокову перспективу, визначенні місця ОГ та ЗО і способів кримінальних проявів у загальному переліку ідентифікованих загроз, вразливостей / спроможностей системи національної, економічної, публічної безпеки, РОП також супроводжується проведенням КЗОР. Організовує такий захід національний координатор у сфері (уповноважений правоохоронний орган) із залученням державних органів, громадських організацій, бізнесу та інших, що опікуються питаннями національної, економічної, публічної безпеки та інших експертів (у разі потреби). КЗОР повинен проводитись систематично, але не рідше одного разу на три роки. Такий комплекс заходів сприяє визначенню місця кожного суб'єкта контролю, в системі забезпечення національної, економічної, публічної безпеки. У такому випадку уповноважений правоохоронний орган виступає своєрідним «Національним координатором» систем забезпечення національної, економічної, публічної безпеки.

Виходячи із зазначеного вище, та з урахуванням результатів опрацювання перелічених вище методологічних джерел, цілі проведення КЗОР можна конкретизувати через сукупність наступних завдань:

- *зниження ймовірності виникнення ризику національної, економічної, публічної безпеки та ризику вчинення кримінальних правопорушень;*
- *оцінка ступеня загрози реалізації ризику національної, економічної, публічної безпеки та ризику вчинення кримінальних правопорушень;*
- *оцінка ступеня вразливості системи національної, економічної, публічної безпеки відносно актуальних загроз та ризику вчинення кримінальних правопорушень;*
- *співвіднесення ступеня кримінальної загрози реалізації ризику та потенційних наслідків його прояву із обсягом ресурсів, які спрямовуються на зниження відповідного ризику;*
- *мінімізація наслідків за умови реалізації ризику національної, економічної, публічної безпеки та ризику вчинення кримінальних правопорушень.*

Методологія РОП щодо аналізу, оцінки ризиків та управління ними в питаннях протидії кримінальним загрозам та забезпечення національної, економічної, публічної безпеки базується на п'яти принципах, а саме:

- 1) *розуміння загроз і вразливих місць системи національної, економічної, публічної безпеки, а також оцінки кримінальних ризиків;*
- 2) *визначення законодавчої процедури для реалізації підходу;*
- 3) *розроблення базових механізмів роботи національного координатора системи забезпечення національної, економічної, публічної безпеки щодо*

нагляду за способами реагування на ризики суб'єктами контролю, що базується на оцінці ризиків;

4) ефективний розподіл ризиків між власниками ризику (суб'єктами контролю) і забезпечення координації дій між ними в питаннях уніфікації підходів щодо оцінки ризиків та способів (інструментів) реагування на ризики;

5) обмін інформацією між державним сектором, бізнесом та суспільством в частині оцінки ризиків, типологій та оцінки способів протиправного використання різних форм підприємництва та фінансової системи особами, причетними до протиправної діяльності.

Ранжування принципів КЗОР здійснюється наступним чином:

1) Узгодження цілей і масштабів КЗОР;

2) Комплексність КЗОР;

Комплексність передбачає наявність єдиного підходу до застосування РОП та КЗОР, використання єдиної інформаційної бази (єдиної бази статистичних показників), системний підхід до збору кількісних даних щодо протидії кримінальним правопорушенням.

3) Політична воля, зобов'язання виконавчої та законодавчої влади щодо РОП та КЗОР;

4) Організація взаємодії органів, залучених до проведення КЗОР;

5) Наявність координуючого органу з питань проведення КЗОР;

6) Гнучкість (актуалізація, розвиток) системи РОП та КЗОР;

7) Поєднання кількісної і якісної вхідної інформації, її достатність і різнобічність;

8) Документальне оформлення інструментарію і результатів КЗОР.

6. ЦИКЛ РОП ЩОДО ЗАБЕЗПЕЧЕННЯ ПУБЛІЧНОЇ БЕЗПЕКИ І ПОРЯДКУ, ПРОТИДІЇ ЗЛОЧИННОСТІ

Побудова концептуальної моделі забезпечення національної, економічної та публічної безпеки можлива лише на основі вибору науково обґрунтованого переліку кількісних показників, які є індикаторами ризиків і сигналізують про посилення вірогідності (наближення часу) виходу криміногенної ситуації за межі контрольованої. При цьому мають значення не самі показники, а їх відхилення від порогових рівнів. Порогові значення індикаторів ризиків – це такі граничні величини, наближення до яких сигналізує про зниження рівня національної, економічної та публічної безпеки, збільшення кількості вчинення кримінальних правопорушень, а перевищення граничних, або порогових, значень – про настання неконтрольованої ситуації. Вибір показників залежить від тривалості періоду, протягом якого потрібно оцінити ризики та виявити загрози національної, економічної та публічної безпеки. В контексті зазначеного потребує зміни підходів до вивчення явищ, зокрема шляхом його

оцифровування у спосіб, що забезпечує можливість його аналізу за допомогою штучного інтелекту.

З тим щоб досягти мети з мінімізації ризику правоохоронний орган розробляє шкалу ризиків, яка містить відповідні фактори ризику. Отже, самі ризики, їх аналіз та оцінка, заходи з реагування на ризики повинні переглядатися та оновлюватися правоохоронним органом у випадках зміни факторів ризику.

Цикл РОП щодо забезпечення національної, економічної та публічної безпеки включає наступні дії:

1) виявлення джерел ризику та факторів впливу за яких виникає ризик, ідентифікація всіх можливих ризиків національної, економічної та публічної безпеки;

2) оцінка рівня окремих ризиків національної, економічної та публічної безпеки та втрат (шкоди), що очікуються, у разі не реагування на ризик або відсутності можливості такого реагування;

3) визначення прийняттого рівня ризику;

4) розробка та вжиття заходів з мінімізації ризику;

5) оцінка підходів та заходів з мінімізації ризику.

Мінімізація окреслених вище загальних загроз і вразливостей може стати вагомим підґрунтям підвищення дієвості, результативності та ефективності системи забезпечення національної, економічної та публічної безпеки, а також запорукою розробки, впровадження й подальшого поширення цілісного комплексу заходів аналітичного, оперативно-розшукового, кримінально-процесуального, кримінологічного характеру, який сприятиме переходу від традиційної протидії й боротьби з наслідками (симптомами) суспільно-небезпечних протиправних діянь до стратегії проактивного запобігання і системної нейтралізації факторів (причин) криміналізації суспільних відносин, національної економіки та сфери управління публічними фінансами.

7. УПРАВЛІННЯ АНАЛІЗОМ РИЗИКІВ

Запровадження ризик-орієнтованого підходу, з ключовою його складовою аналізом ризиків, у правоохоронну практику, для уможливлення превентивного впливу на процеси криміналізації суспільних відносин, з метою забезпечення національної, економічної та публічної безпеки, є більш ефективним способом захисту суспільства від шкоди, аніж кримінальні переслідування осіб причетних до протиправних дій після їх вчинення.

Діяльність уповноважених суб'єктів контролю відіграє важливу роль в системі захисту суспільства від процесів його криміналізації, зокрема шляхом:

1) підвищення рівня поінформованості суб'єктів регулювання та їхнього розуміння ризиків національної, економічної та публічної безпеки;

встановлення регулятивних зобов'язань та підтримки й сприяння сучасним практикам реагування на ризики;

2) усунення загрози, забезпечення виконання та моніторингу дотримання обов'язків із забезпечення правопорядку, а також

3) вжиття відповідних заходів у разі виявлення недоліків системи.

АНАЛІЗ РИЗИКІВ – це сукупність процедур і методів обробки інформації щодо оцінки загроз національної, економічної та публічної безпеки, діяльності окремих осіб чи груп, підприємств, установ, організацій, причетними до злочинної діяльності, видів злочинів у певній сфері або їх наслідками, рівня негативного впливу на суспільство, підприємницьку діяльність, оцінки ступеню вразливості органів влади, зокрема судової системи, правоохоронних та контролюючих органів.

Аналіз ризиків використовується на інституційному рівні, на трьох основних компонентах аналізу інформації, відповідно стратегічному, оперативному та тактичному. Цей тип аналітичного продукту має використовуватись в активній фазі діяльності правоохоронного органу в тому сенсі, що він орієнтує діяльність на виявлення, оцінювання та визначення ризиків вчинення кримінальних правопорушень, а також вжиття відповідних заходів щодо управління ризиками у спосіб та в обсязі, що забезпечують мінімізацію таких ризиків залежно від їх рівня, а також документування фактів протиправної діяльності до реєстрації інциденту / події / правопорушення на інституційному рівні. Це не виключає проведення аналізу ризиків у реактивному сегменті, у такому випадку, як правило, визначається поведінка, якої слід дотримуватись детективам у конкретних ситуаціях.

Система аналізу ризиків представлена трьома основними компонентами аналізу інформації: **стратегічний; оперативний; тактичний.**

Залежно від результатів проведення аналізу ризиків встановлюються рівні ризиків, зокрема для трирівневого підходу:

низький – за незначних рівнях загрози або коли рівень загрози переважає рівень уразливості, за незначного або помірного рівня впливу,

середній – за низького або помірного рівня впливу, коли рівень уразливості відповідає рівню загрози,

високий – за помірного або високого рівня впливу, коли рівень уразливості переважає рівень загрози.

3 рівні ризику:	5 рівнів ризику:
– низький	– дуже низький
– середній	– помірний
– високий	– допустимий
	– високий
	– катастрофічний

7.1. СТРАТЕГІЧНИЙ РІВЕНЬ

Аналіз ризику стратегічного рівня включає оцінку кримінального явища, діяльності організованих груп та злочинних організацій, криміногенної ситуації чи типу інцидентів, пов'язаних із зонами їх походження, часовими інтервалами та частотою, на середній та довгостроковій перспективі, на основі заздалегідь визначених критеріїв (показників).

Метою аналізу ризиків на стратегічному рівні, як першочергового кроку діяльності правоохоронного органу, повинно бути вивчення кримінального/криміногенного явища з метою оцінки його впливу на національної, економічної та публічної безпеки та управління ризиками з метою мінімізації ризиків та кращого забезпечення управління інституційними ресурсами. При цьому зосереджуються зусилля на господарських/виробничих, бюджетних, фіскальних процесах, інструментах вчинення злочинів, часових інтервалах (частоти застосування) та визначенні причинно-наслідкових зв'язків, втягуваності.

Аналіз ризиків стратегічного компоненту забезпечується на центральному рівні шляхом визначення ризиків, пов'язаних із кримінальними злочинами підслідними правоохоронному органу, криміногенними явищами чи деякими типами інцидентів, для обґрунтування управлінських рішень щодо певних напрямків та інструментів реагування. У такому випадку звіт щодо такого аналізу з визначенням прогнозованих наслідків охоплює проміжок часу, що перевищує один рік.

Замовниками стратегічного аналізу ризиків можуть бути:

- а) керівництво правоохоронного органу;*
- б) керівники територіальних управлінь правоохоронного органу;*
- в) центральні органи виконавчої влади чи інші державні, зокрема інші правоохоронні органи, в межах інституціональної компетенції із забезпечення національної, економічної та публічної безпеки, а також профільні комітети Верховної Ради України.*

Користувачами аналізу ризику стратегічного рівня можуть бути:

- керівники середньої ланки правоохоронного органу або окремі працівники відповідно до функціональних обов'язків;*
- установи, організації з якими правоохоронним органом підписані відповідні угоди;*
- інші установи, організації відповідно до їх запиту у разі згоди на це керівництва правоохоронного органу.*

У разі, якщо звіт містить відомості з обмеженим доступом, керівництвом правоохоронного органу на свій розсуд можуть бути прийняте одне із наступних рішень:

- направити звіт замовнику (користувачу) відповідно до правил секретного діловодства;*
- відмовити у наданні матеріалів звіту;*
- надати усічений звіт.*

Звіт про аналіз ризиків готується уповноваженими аналітиками відповідно до посадових обов'язків або на підставі запиту/розпорядження керівника, який вказує на явище, часовий проміжок, а також інші показники, що становлять інтерес для аналізу.

7.2. ОПЕРАТИВНИЙ РІВЕНЬ

Аналіз ризику оперативного рівня представляється як продукт, який готується аналітиком, відповідно до запиту уповноваженої особи щодо ризиків вчинення певного виду злочинів у різних сферах суспільних відносин та галузях економіки, або пов'язаних з розпорядженням бюджетними коштами, а також з отриманням та використанням міжнародної технічної допомоги. Він може складатися у разі прийняття рішень щодо: превентивного оперативно-розшукового втручання в процеси, що відбуваються у кримінальному середовищі; руйнування кримінальної інфраструктури; розслідування кримінальних проваджень; нейтралізації впливу організованих груп та злочинних організацій тощо. Замовниками та користувачами такого аналізу можуть бути детективи правоохоронного органу, незалежно від їх рівня.

Звіт за результатами аналізу ризиків є аналітичною підтримкою роботи детективів та переслідує мету виявлення потенційних ризиків, про які раніше не було відомо, але які становлять ризик вчинення злочинів або створюють підґрунтя для останнього.

Цілі звіту за результатами аналізу ризиків щодо превентивного втручання у криміногенні процеси, визначаються на основі показників ризику, попередньо встановлених аналітиком, залежно від кримінального злочину, що розглядається.

Для ідентифікації окремих джерел ризику вчинення злочинів або обґрунтованої підозри щодо цього, використовуються всі бази даних, зокрема автоматизована система аналізу та управління ризиками, а також відкриті джерела. За необхідності, за результатами аналізу ризиків, цей великий обсяг даних відображається у змісті звіту у структурованій, пояснювальній формі на основі виявлених або заздалегідь визначених показників ризику.

Виявлені ризики, висновки та рекомендації, що знайшли відображення у змісті звіту про результати аналізу ризиків, надаються детективам кримінальної розвідки для оцінки можливості превентивного втручання у криміногенні процеси. Матеріали, що мають достатню кількість даних, інформації, версій, гіпотез та висновків та підтверджуються результатами проведених спеціальних операцій, зокрема із застосуванням оперативно-технічних заходів, а також контрольно-перевірочною діяльністю, з метою одержання доказової бази, можуть бути підставою для відкриття кримінального провадження.

7.3. ТАКТИЧНИЙ РІВЕНЬ

Аналіз ризику тактичного рівня включає оцінку видів злочинів або серії інцидентів у районах їх виникнення, за часовими інтервалами та частотою, за короткий та середньостроковий проміжок часу (до одного року), відповідно до сфери аналізу ризиків та рівню латентності злочинів.

Аналіз ризику тактичного рівня може бути складений на місцевому рівні для обмежених територій, наприклад, на рівні населеного пункту, області або регіону, залежно від компетенції територіальних підрозділів правоохоронного органу, шляхом аналізу інформації, даних та відомостей, доступних протягом 24-годин. У такому разі типи звіту розрізняють РТ24 (24-годинний тактичний ризик), РТ30 (30-денний тактичний ризик) та за запитом в ТАРЗ (тактичний аналіз ризиків за запитом).

Звіти про результати аналізу ризиків тактичного рівня можуть готуватися на вимогу керівників територіальних управлінь правоохоронного органу в регіоні, області, місті або за запитом уповноваженої особи та лише типу РТ24 та РТ30.

Аналіз ризиків тактичного рівня є способом виявлення латентних злочинів, віднесених до компетенції правоохоронного органу, тобто тих, які не стали предметом реагування з боку останнього, шляхом моніторингу інших, пов'язаних з ними правопорушень, інцидентів.

Тип звіту обирається залежно від наявних даних або часового інтервалу, що підлягає аналізу.

Звіти про результати аналізу ризиків тактичного рівня надаються замовнику/користувачу для забезпечення об'єктивного уявлення про реальний стан злочинності.

7.4. ЕТАПИ ВИКОНАННЯ АНАЛІЗУ РИЗИКІВ:

1. Визначення мети та кола завдань, які потребують вирішення.

Передбачає: визначення виконавця та оформлення запиту на проведення аналізу, при цьому орієнтовний план визначає вид необхідних даних, їхнє джерело, аналітичні техніки, методи аналізу, термін реалізації та форми розповсюдження.

2. Визначення об'єкту аналізу (особи, групи, явища) та теми аналізу.

Передбачає: збирання даних та інформації, дії відповідно до плану.

3. Оцінка інформації. Передбачає: оцінку надійності джерел інформації та її достовірності, що робить подальшу інтерпретацію інформації більш обґрунтованою.

4. Впорядкування. Передбачає: відсіювання неправдивих, несуттєвих даних, впорядкування решти інформації з метою встановлення взаємозв'язків між її складовими.

5. Аналіз. Передбачає: ґрунтовну інтерпретацію інформації; опрацювання максимально точних висновків та прогнозів, трендів і закономірностей; надання рекомендацій; інформування про факти щодо діяльності окремих ОГ та ЗО, їхній потенціал та слабкі сторони.

6. Представлення результатів. Передбачає: підсумовування результатів процесу накопичення та аналізу інформації, а також представлення результатів оперативного процесу; визначення виразних зв'язків між фактами та оцінками, висновками та прогнозами; часто вимагає додаткового навчання у сфері написання текстів або використання програмного забезпечення для візуалізації матеріалу.

7. Розповсюдження. Передбачає: постачання звіту зовнішнім та внутрішнім замовникам/користувачам та, у разі потреби, особам, які надали дані та інформацію у якості допомоги та власного внеску в побудову якісної системи національної, економічної та публічної безпеки.

8. Оцінювання результатів (здійснюється після завершення аналізу). Передбачає дві форми: одна спрямовується на вивчення рівня виконаної роботи аналітичним підрозділом (аналітиками), а також з'ясування, що саме вплинуло на якість їхньої роботи (знання, досвід); друга концентрується на результативності, тобто оцінці, чи був продукт аналізу корисним у роботі замовника, який рівень підтримки він забезпечив та чи був він, на думку замовника, достовірним і своєчасним.

ВИМОГИ, ЩО ВИСУВАЮТЬСЯ ДО КОЖНОГО ЕТАПУ ПРОВЕДЕННЯ АНАЛІЗУ РИЗИКІВ:

1. Визначення мети, кола завдань та теми аналізу може бути встановлена як на прохання замовника, так і аналітиком самостійно відповідно до функціональних обов'язків. Якщо це відбувається за бажанням замовника, запит повинен бути сформульований ним письмово у довільній формі за формою визначеною відомчим нормативним актом, як це передбачено в угоді про співпрацю.

На цьому етапі аналітик повинен враховувати наступні критерії:

- а) тема та мета повинні бути чітко визначені;*
- б) забезпечити доступ до даних та інформації, що є предметом аналізу;*
- в) вимоги клієнта не перевищуватиме матеріально-технічні та інші ресурсні можливості;*
- г) розумні умови, залежно від наявних даних та інформації;*

Технічне завдання щодо проведення аналізу ризиків стратегічного, тактичного та операційного рівнів, що окреслене у цій методології, повинне співвідноситись з іншими затвердженими методиками або процедурами аналізу інформації, а також наказами та положеннями, що врегульовують питання збору інформації.

У разі виникнення обставин, зазначених у нормативних документах як таких що унеможливають проведення аналізу ризиків, аналітик має право відмовити замовнику в проведенні аналізу ризиків про що письмово доповідає керівникові, який доручив останньому проведення такого аналізу, про що також інформується замовник.

2. Збір інформації з метою проведення аналізу ризиків здійснюється з усіх доступних джерел (закритих та відкритих).

Збір інформації для аналізу ризиків повинен виконуватись відповідно до існуючих процедур / методик для кожного компоненту аналізу інформації.

3. Оцінка інформації. На цьому етапі аналітик використовуватиме наступні методики:

а) **Фільтрування інформації** – відмова від інформації, яка не є релевантною, щоб зосередитись на важливому;

б) **Категоризація інформації** – це відбір / класифікація даних за категоріями та логічними критеріями;

в) **Пріоритетність** – сортування зібраної інформації та упорядкування її за важливістю та актуальністю;

г) **Оцінка інформації** – це процес перевірки надійності джерела та достовірності інформації, отриманої з різних джерел;

д) **Агрегація інформації** – передбачає підрахунок даних, їх комбінування та обчислення середнього показника, зосередження уваги на найважливішому;

е) **Порівняння** – це зіставлення окремих елементів / інцидентів, щоб з'ясувати наявність чи відсутності взаємозв'язку між ними;

є) **Кореляція** – статистичний прийом, який допомагає встановити взаємозв'язок між одним набором даних та іншим;

ж) **Причинність та пояснення** – продовжує техніку кореляції, яка визначає причинно-наслідковий зв'язок між окремими факторами.

Аналіз та інтерпретація дозволять виявити існуючі умови, які впливають на досліджувану проблему та отримання відповіді на поставлені питання. Він описує та аналізує контекст, в якому знаходиться проблема, та забезпечує основу для порівняння джерел загрози та рівнів їх наслідків, одночасно надаючи можливість виявити інформаційні прогалини.

Аналіз ризиків та їх інтерпретація для кожного компонента (стратегічного, оперативного та тактичного) проводитимуться у відповідності з діючими методологіями, методиками чи процедурами.

Ідентифікація ризику проводиться на етапі його аналізу, враховуючи результати кримінального аналізу, шляхом виділення генеруючих елементів ризику та загрози.

7.5. МЕТОДИ ІДЕНТИФІКАЦІЇ РИЗИКІВ

Карта перевірки (чек-лист) – використання певного сформованого переліку питань, для перевірки стану виконання процесу;

Аналіз блок-схем – послідовний аналіз виконуваного процесу, послідовність виконання якого відображено у графічний спосіб;

Порівняння з еталонними критеріями (бенчмаркінг) – систематичний пошук і впровадження найкращих практик роботи правоохоронних органів або структурно-функціональної та правозастосовної моделі протидії економічним злочинам для порівняння із власною системою організації роботи та переймання найбільш вдалих методів роботи;

Сценарне планування дослідження зовнішнього середовища, що впливає на діяльність правоохоронного органу, стосовно наявності визначених елементів (*predetermined elements*) і ключових невизначеностей (*key uncertainties*) та їх комбінування для формулювання альтернативних сценаріїв майбутнього.

Кожен із зазначених методів можна використовувати на практиці, що допоможе керівництву правоохоронного органу ідентифікувати ризики, зокрема під час: опитувань; мозкових штурмів; засідань робочих груп (з управління ризиками) / робочих (оперативних) нарад.

В залежності від конкретної ситуації, виявлення ризику здійснюється шляхом аналізу загальних або конкретних заздалегідь визначених показників об'єкту, що підлягає аналізу.

Показники ризику визначаються шляхом аналізу даних із офіційних джерел (власні бази даних правоохоронного органу або тих, до яких останній має доступ, статистичні матеріали тощо), які підтверджені іншими даними з відкритих джерел.

Далі ризик повинен оцінюватися на основі деяких загальних показників:

- еволюція загальної кількості інцидентів, що підлягають аналізу, зафіксованих за певний проміжок часу, порівняно з аналогічними періодами попередніх років;

- динаміка спричинених збитків, втрат бюджету (податкових надходжень та/або освоєння бюджетних коштів), кількості жертв / інцидентів за аналізований період;

- сфери, географічне розташування, місце виникнення інцидентів та / або жертв, секторів та місць втрат бюджету;

- середнє значення інцидентів та / або жертв, сум втрат бюджету у визначений проміжок, а також за сферою та місцем виникнення;

- часові інтервали, в яких відбуваються інциденти;

- існування та вплив зовнішніх економічних, соціальних та географічних факторів;

- встановлення взаємозв'язку між інцидентами, що аналізуються, та діями осіб (фізичних, юридичних), які знаходяться на оперативному обліку або відносно яких є інформація про причетність до протиправної діяльності.

Під час аналізу, на стадії саме оцінки загрози, аналітик повинен визначити, що саме спричиняє загрозу, в якій формі вона може бути реалізована, у разі якщо буде втілена, які наслідки матиме для держави, суспільства, економіки, бюджету, на які сфери суспільних відносин, сектори економіки або роботи державних органів вплине. При оцінці загрози може бути зроблений висновок про її відсутність або зменшення її рівня. Такий висновок є також важливим, його треба розглядати рівнозначним, як і у випадках оцінки загрози з високим рівнем впливу.

Аналітик під час аналізу ризиків повинен враховувати наступне:

- що загроза, як сила, яка має намір та можливості заподіяти шкоду, не вважається ризиком, якщо у нас відсутні вразливості, тобто слабкі місця системи, які може використати потенційний правопорушник;
- загроза завжди повинна сприйматися як ймовірнісна категорія, тому у разі її реалізації вона вже виступатиме як ситуація або стан речей;
- у зв'язку з тим, що рисою, яка притаманна загрозі є негативний вплив (шкідливі наслідки), у разі його відсутності, треба говорити не про загрозу, а швидше за все про фактор впливу.

Під час ідентифікації, опису та оцінки загрози необхідно враховувати дві загальні характеристики, що її визначають це ймовірність та вплив.

Рівень загрози розраховується на основі матриць 3×3 або 5×5, при цьому імпліцитно (неявний, прихований, такий, що (на відміну від експліцитного) може бути виявлений тільки через свої зв'язки з іншими об'єктами чи процесами) присвоюється значення як для впливу, так і для ймовірності за шкалою від 1 до 3 (ймовірність/вплив):

1 – низька/низький;

2 – середня/помірний;

3 – висока/високий;

або шкалою від 1 до 5 (ймовірність/вплив):

1 – дуже низька/дуже низький;

2 – низька/помірний;

3 – помірна/допустимий;

4 – висока/високий;

5 – дуже висока / катастрофічний.

Результат, отриманий на перетині між двома осями, представляє рівень загрози (у матриці 3×3 максимальний рівень досягає значення 9, а в типі 5×5 максимальне значення становить 25, тобто значення рівня загрози обчислюється шляхом множення значень ймовірності та впливу).

Залежно від отриманого результату, аналітик встановлює такі рівні загрози:

1-3	низька загроза	1	дуже низький рівень загрози
3-6	середня загроза	2, 3	помірний рівень загрози
6-9	висока загроза	4, 5, 6	допустимий рівень загрози
		8, 9, 10, 12	високий рівень загрози
		15, 16, 20, 25	катастрофічний рівень загрози

Для кращого графічного відображення рівнів загрози / ризику рекомендується включати кольорову схему до змісту звіту про результати аналізу, наступним чином:

А. Оцінка за матрицею 3×3

- а. Високий рівень – червоний колір;

- б. Середній рівень – жовтий колір;
в. Низький рівень – зелений колір.

В. Оцінка за матрицею 5×5

- а. Дуже низький рівень – темно-зелений колір;
б. Помірний рівень – світло-зелений колір;
в. Допустимий рівень – жовтий колір;
г. Високий рівень – червоний колір;
е. Катастрофічний рівень – темно-червоний колір.

Якісна оцінка рівня загрози

	ІМОВІРНІСТЬ	ВПЛИВ
	опис	
низька / низький	➤ Виходячи з аналізу попередніх періодів, спостерігається стійка позитивна динаміка на зменшення випадків/масштабів негативних явищ, ресурсів на їх реалізацію, не відбувається інтелектуалізація протиправної діяльності, незмінність способів досягнення кримінальних цілей; ➤ Існують несприятливі внутрішні та зовнішні фактори для реалізації загрози; ➤ П/о володіє інформацією (A1, B2) з інших закритих та відкритих джерел, яка підтверджує протилежне.	➤ Наслідки: буде завдана незначна шкода або, як правило, не буде заподіяно шкоди національній, економічній та публічній безпеці (регіональній безпеці), а також системі функціонування державних інституцій, веденню господарської діяльності та соціальній сфері; ➤ Вони впливатимуть на невеликі території / сектори економіки / явища і жодним чином не впливатимуть на сфери життєдіяльності/економіку.
середня / помірний	➤ Присутня динаміка коливань щодо кількості/масштабів розповсюдження негативних явищ, задіяння ресурсів на їх реалізацію, кількості суб'єктів кримінальних пропозицій у попередні періоди, відбувається незначна інтелектуалізація протиправної діяльності, частково змінюються способи досягнення кримінальних цілей; ➤ Відсутність відповідних внутрішніх та зовнішніх каталітичних факторів; ➤ Часткове підтвердження або відсутність інформації.	➤ Наслідки: буде завдана помірна шкода національній, економічній та публічній безпеці (регіональній безпеці), та соціальній сфері; ➤ Вона впливатимуть на конкретні обмежені території / сфери (наприклад, на регіональному, місцевому рівні, певних галузях, секторах економіки), окремі напрями освоєння бюджетних коштів, а також міжнародної технічної допомоги або на частини деяких областей / явищ
висока/високий	➤ Виходячи з аналізу попередніх періодів, спостерігається динаміка на збільшення кількості/масштабів	➤ Наслідки: буде заподіяно значної шкоди національній, економічній та публічній безпеці (регіональній безпеці), а також

	розповсюдження негативних явищ, ресурсів на їх реалізацію, кількості суб'єктів кримінальних пропозицій, відбувається значна інтелектуалізація протиправної діяльності, суттєво змінюються способи досягнення кримінальних цілей; ➤ Існують внутрішні та зовнішні каталітичні фактори; ➤ Достовірність інформації підтверджується з інших закритих та відкритих джерел	соціалній сфері; ➤ Вони впливатимуть на значні території (наприклад, на національному або регіональному рівні) або на області вцілому / явища
--	---	--

Послідовність оцінки ризику:

1) виявлення джерел і причин ризику, етапів і характеру дій, при проходженні та виконанні яких виникає ризик;

2) ідентифікація всіх можливих ризиків, властивих даній галузі, сфері економіки, розподілу бюджетних коштів;

3) оцінка рівня окремих секторальних ризиків і ризиків в цілому у різних сферах життєдіяльності, а також бюджетній, податковій, митній, грошово-кредитній та інвестиційній сферах, що визначає механізми та інструменти їх мінімізації;

4) визначення допустимого рівня ризику;

5) розробка заходів щодо зниження ризику, виходячи з інституціональної спроможності.

Оцінка ризику:

- має на меті виявити та дослідити вразливі сфери національної, економічної та публічної безпеки вцілому, а також вразливі місця до кримінальних загроз бюджетної, податкової, митної, грошово-кредитної та інвестиційної сфер, які використовуються або якими можуть скористатися, щоб надати рекомендації із зазначенням інструментів та механізмів їх усунення;

- при цьому враховується не тільки характер вразливого сектору, але й характер потенційних джерел (суб'єктів) загрози (наприклад ОГ та ЗО, корумпованих можновладців тощо), та рівень складності режиму їх роботи;

- комбінація з поєднання передбачуваного рівня ймовірності та передбачуваного рівня впливу загрози є ризиком, на основі якого складається профіль ризику;

Оцінка ризику проводиться за трирівневою шкалою, а саме:

1. Оцінка ймовірності матеріалізації виявленого ризику полягає у визначенні вірогідності настання конкретного результату і здійснюється шляхом:

а) спостереження за матеріалізацією подібних ризиків у минулому;
б) аналізу обставин (причин), які сприяли/сприяють виникненню ризиків;

в) використання шкал для оцінки ймовірності матеріалізації ризику, відповідно трьох або п'яти рівнів ймовірності, як зазначено у таблицях нижче:

2. Оцінка впливу на економічну безпеку (об'єкт) у випадку матеріалізації ризиків являє собою наслідки для об'єкту впливу, які можуть бути

3. Оцінка впливу ризику – це наслідки, поєднання ймовірності та впливу, які може відчувати система національної, економічної та публічної безпеки (об'єкт впливу) у випадку матеріалізації ризику.

1. Оцінка ймовірності матеріалізації виявленого ризику полягає у визначенні вірогідності настання конкретного результату і здійснюється шляхом:

а) спостереження за матеріалізацією подібних ризиків у минулому;
б) аналізу обставин (причин), які сприяли/сприяють виникненню ризиків;

в) використання шкал для оцінки ймовірності матеріалізації ризику, відповідно трьох або п'яти рівнів ймовірності, як зазначено у таблицях нижче:

3 рівні ймовірності

Рівень ймовірності		Пояснення
1.	Низька (0% - 19%) (можливо)	навіть чи це станеться у довгостроковій перспективі; цього ще не траплялося.
2.	Середня (20% - 79%) (Ймовірно)	ймовірно, це станеться у середньостроковій перспективі; це траплялося періодично кілька разів за останній рік / роки.
3.	Висока (80% - 100%) (Майже впевнений)	дуже ймовірно, що це станеться найближчим часом; це траплялося системно багато разів за останній рік.

5 рівнів ймовірності

Рівень ймовірності		Пояснення
1.	Дуже низька (0% - 10%) (Незначна)	це виключено, щоб це відбувалося у довгостроковій перспективі; цього ще не траплялося.
2.	Низька (10% - 19%) (можливо)	це може статися у довгостроковій перспективі; цього ще не траплялося.
3.	Середня (20% - 39%) (Ймовірно)	ймовірно, це станеться у середньостроковій перспективі; це траплялося періодично кілька разів за останній рік / роки.
4.	Висока (40% - 79%) (Майже впевнений)	це майже напевно станеться протягом у середньостроковій перспективі або найближчим часом; це траплялося кілька разів за останній рік / роки.
5.	Дуже висока (80% - 100%) (Неминуче)	Немає сумнівів, що це відбудеться найближчим часом; це регулярно траплялося багато разів за останній рік.

2. Оцінка впливу на економічну безпеку (об'єкт) у випадку матеріалізації ризиків являє собою наслідки для об'єкту впливу, які можуть бути, залежно від характеру ризику, негативними чи позитивними і проводяться згідно з таблицею:

Рівень впливу / наслідки		Пояснення
1.	низький	З дуже низьким впливом на сфери або діяльність структури та досягнення цілей.
2.	середній	З середнім впливом на сфери або діяльність структури та досягнення цілей.
3.	високий	Зі значним впливом на сфери або діяльність структури та досягнення цілей.

3. Оцінка впливу ризику – це наслідки, поєднання ймовірності та впливу, які може відчувати система національної, економічної та публічної безпеки (об'єкт впливу) у випадку матеріалізації ризику. Рівень ризику обчислюється на основі матриці 3x3 або 5x5, представленої вище, у разі чого кожному типу аналізованого факту надається оцінка, як для впливу, так і для ймовірності за шкалами від 1 до 3 або від 1 до 5, наступним чином:

- а) через матрицю 3×3: 1 – низький, 2 – середній, 3 – високий;
- б) через матрицю 5×5: 1 – низький, 2 – помірний, 3 – допустимий, 4 – високий і 5 – катастрофічний.

Оцінка впливу ризику визначається наступним чином: ймовірність × вплив ($X \times Y$):

- а) Шкала оцінки ризику за допомогою матриці “3×3” представлена графічно наступним чином:

ВПЛИВ (Y)	Високий - 3	3	6	9
	Середній - 2	2	4	6
	Низький - 1	1	2	3
		низька	середня	висока
		ЙМОВІРНІСТЬ (X)		

ПРИМІТКА: Рядки матриці описують варіацію ймовірності, а стовпці - варіацію впливу. Схильність до ризику відбувається при перетині рядків із стовпцями.

Приклад вирішення матриці оцінки ризику типу 3×3.

ВПЛИВ (Y)	Високий - 3	3	6	9
	Середній - 2	2	4	6
	Низький - 1	1	2	3
		низька	середня	висока
		ЙМОВІРНІСТЬ (X)		

Якщо ми реєструємо значення удару 2, а значення ймовірності 2, результат оцінки ризику дорівнює 4, що означає, що ми маємо середній рівень ризику (жовтий колір).

б) Шкала оцінки ризику через матрицю “5×5” представлена графічно наступним чином:

ВПЛИВ (Y)	катастрофічний-5	5	10	15	20	25
	високий-4	4	8	12	16	20
	допустимий-3	3	6	9	12	15
	помірний-2	2	4	6	8	10
	низький -1	1	2	3	4	5
		дуже низька -1	низька-2	середня-3	висока-4	дуже висока-5
		ЙМОВІРНІСТЬ (X)				

Приклад вирішення матриці оцінки ризику типу 5×5.

ВПЛИВ (Y)	катастрофічний-5	5	10	15	20	25
	високий-4	4	8	12	16	20
	допустимий-3	3	6	9	12	15
	помірний-2	2	4	6	8	10
	низький -1	1	2	3	4	5
		дуже низька -1	низька-2	середня-3	висока-4	дуже висока-5
		ЙМОВІРНІСТЬ (X)				

Якщо ми реєструємо значення впливу 5 і значення ймовірності 5, результат оцінки ризику становить 25, що означає, що ми маємо дуже високий рівень ризику (червоний).

Залежно від отриманого результату, аналітик у звіті визначить такі рівні ризику:

1-3	низький ризик	1	Низький ризик
3-4	середній ризик	2, 3	помірний ризик
6-9	високий ризик	4, 5, 6	допустимий ризик
		8, 9, 10, 12	високий ризик
		15, 16, 20, 25	катастрофічний ризик

Встановлення відповідності й співвідношення між оцінкою загрози та оцінкою ризику і є метою оцінки. На першій фазі ціллю є загроза, а на другій фазі увага зосереджується на сфері життєдіяльності або об'єкті можливого впливу, які/який є вразлив(и)-им і може стати ціллю загрози. Сфера життєдіяльності (об'єкт впливу) може бути вразливим, навіть якщо відсутні загрози.

Якщо неможливо визначити ризики кількісно або їм не можуть бути присвоєні певні значення, вони оцінюються відповідно до: кількості попереджень; частоти, масштабів (географії) прояву; сум збитків та кількості вразливостей або у співвідношенні з іншими факторами ризику. Вони також класифікуються за 3 або 5 рівневою шкалою ризику, залежно від наявних даних та інформації.

8. УПРАВЛІННЯ РИЗИКАМИ

Природа ризику така, що, якщо його не обмежувати і не проводити превентивні заходи, він подібно газу може заповнити собою весь вільний від перешкод простір. Тоді вірогідність реалізації ризиків і об'єм їхнього кумулятивного негативного економічного (фінансового) ефекту з часом зростатиме.

За допомогою сучасних методів AI (штучного інтелекту) та ML (машинного навчання), а також сил, засобів і методів кримінальної розвідки (далі КР) можна з достатньою повнотою простежити, як виникає злочинний задум, у яких конкретних діяннях він реалізується на різних етапах підготовки та скоєння злочинів, які фактори зумовили його виникнення в конкретних умовах місця та часу, які простежуються тенденції та прояви злочинності, сфери її найінтенсивнішого поширення тощо.

Базова модель управління ризиками національної, економічної та публічної безпеки правоохоронного органу включає трирівневу систему реагування на ризики та фактори, що їх обумовлюють:

Перший рівень, належить детективам, що проводять досудове розслідування, уповноваженим особам, які застосовують заходи превентивного впливу та проводять аналітичні дослідження, тобто організаторам будь-яких процедур та процесів в правоохоронному органі – керівникам середньої ланки, детективам та аналітикам, які стикаються з факторами ризику щодня і мають всіляко попереджати поточні інциденти, а у разі потреби інформувати про виникнення загроз або виявлення інциденту керівництво правоохоронного органу або інших суб'єктів контролю.

Другий рівень, належить спеціально уповноваженим підрозділам внутрішнього контролю (власної безпеки), кібербезпеки правоохоронного органу, а також аналітиками, які спеціалізуються на проведенні аналізу ризиків в їхніх різних варіантах і формах. Сюди належать усі підрозділи, основною сферою діяльності яких є процедури внутрішнього контролю. І які спільно з керівниками середньої ланки, детективами/аналітиками беруть участь в розробці та подальшому впровадженні в практику методик кримінального аналізу, аналізу ризиків та розслідування злочинів, схем, регламентів і внутрішніх нормативів як виключно організаційно-розпорядчого, так і операційно-технічного характеру. Цей рівень починає формуватися при переході від стадії повторюваності до стадії регламентованості й формує ланцюг зворотного зв'язку, з якого керівники правоохоронного органу та інших суб'єктів контролю починають отримувати перші відомості про неочевидні для них ризики, а також інциденти в системі забезпечення національної, економічної та публічної безпеки в цілому та про інституціональні уразливості суб'єктів контролю зокрема. На такому етапі керівництву правоохоронного органу необхідно усвідомлювати дві базові істини: кожен впроваджуваний регламент не є остаточним, його варто періодично переглядати на предмет відповідності вимогам сьогодення;

належною реакцією на кожен новий виявлений ризик є оцінка його можливих наслідків. І тільки після цього (при необхідності) — розробка заходів з його усунення і мінімізації.

Третій рівень передбачає застосування групи внутрішнього аудиту (ГВА), яка може складатися з власних постійних співробітників або залучених зовні фахівців, представників Ради громадського контролю та ін., ключовою характеристикою яких є незалежність в оцінці процесів і систем правоохоронного органу, а основне завдання — оцінка адекватності й ефективності системи внутрішнього контролю й управління ризиками. Внутрішній аудит — це незалежна діяльність з перевірки і оцінки роботи правоохоронного органу в його ж інтересах. Внутрішній аудит допомагає правоохоронному органу досягти поставлених цілей, використовуючи систематизований і послідовний підхід до оцінки і підвищення ефективності процесів управління ризиками, контролю і корпоративного управління. У діяльність ГВА, що, як правило, здійснюється на плановій основі, входить оцінка стану внутрішнього середовища правоохоронного органу, методик розслідування окремих видів злочинів, адекватності застосування та ефективності превентивних заходів впливу, наявності сертифікації у використовуваних аналітичних платформ для кримінального аналізу та аналізу ризиків, відповідності існуючих внутрішніх процедур ІЛР-моделі правоохоронного органу, й впроваджених в них засобів внутрішнього контролю, окремих фактів і аспектів оцінки ефективності роботи органу, систем управління ризиками. Одним з ключових завдань ГВА є оцінка корупційних ризиків, оскільки виключна монополія на боротьбу з окремими видами злочину породжує формування різних форм підкупу з боку учасників кримінального середовища, тіньового ринку. Репутаційний ризик від функціонування корупційних схем можна порівняти з наслідками реалізації критичного ризику, він здатний значно похитнути легітимність правоохоронного органу та довіру до нього з боку суспільства, бізнесу, донорів та інших зарубіжних правоохоронних інституцій.

Виходячи з інституціональних можливостей правоохоронного органу одним із інструментів мінімізації ризиків є застосування глибоких, спеціальних, тривалих (в ідеалі постійних) агентурних операцій, а саме виконання спеціального завдання, агентурне спостереження (стратегічні агентурні операції) та контроль за вчиненням злочину, зокрема контрольоване постачання. Але це зовсім не означає, що інші заходи кримінальної розвідки не мають жодного потенціалу до системи управління ризиками.

По-перше, навіть при проведенні разового заходу можна отримати інформацію, по заздалегідь визначеному профілю ризиків, для проведення аналізу ризиків або кримінального аналізу.

По-друге, під час проведення суто заходів кримінальної розвідки працівники правоохоронного органу отримують значний обсяг так званої попутної інформації. Причому далеко не вся інформація виявляється

оперативним шляхом, оскільки на її отримання порівняно рідко орієнтувалися оперативні джерела інформації. Тим часом, можливості оперативних джерел інформації, зокрема детективів, які працюють під прикриттям у зборі такої інформації досить значні.

По-третє, сконцентрована, систематизована та збагачена оперативна інформація, яка отримана та внесена до баз правоохоронного органу для аналітичного дослідження, за результатами проведення всіх заходів КР (незалежно від їх поділу за ступенем значимості), є якісно іншим змістом (порівняно з розрізненими даними) і при грамотному використанні штучного інтелекту може стати незамінним джерелом емпіричних даних, необхідних для цілей кримінального аналізу (аналізу ризиків). КР, що скеровується аналітикою сама є джерелом інформації для кримінального аналізу та аналізу ризиків. Для вивчення злочинності та протидії її проявам виникає потреба в оцінюванні способів впливу різних загроз на систему суспільних відносин, наприклад:

SOCTA – Методологія «Оцінка загрози з боку особливо небезпечних форм організованої злочинності», є продуктом системного аналізу інформації правоохоронців про кримінальну діяльність і групи, що становлять загрозу для ЄС, щоб допомогти керівникам у визначенні пріоритетів серед загроз організованої злочинності;

ЮСТА – “Оцінка загроз від організованої злочинності в Інтернеті”, є усталеною практикою країн-членів ЄС та залишається важливим інструментом управління та ухвалення політичних рішень, що використовуються фахівцями з протидії кіберзлочинності, у тому числі й транснаціональній, для розробки державних програм на стратегічному рівні, визначення пріоритетів та розподілу ресурсів на операційному рівні;

TE-SAT щорічний звіт Європолу про ситуацію з тероризмом і тенденції в ЄС, містить огляд явища тероризму в ЄС за певний рік. Він пропонує співробітникам правоохоронних органів, політикам і широкій громадськості факти та цифри про тероризм в ЄС, а також визначає тенденції розвитку злочинності терористичного спрямування, на основі інформації, яку країни-члени надають Європолу.

Відповідно до діючого законодавства переважна кількість завдань правоохоронних органів, пов'язана з реалізацією превентивної функції у забезпеченні національної, економічної та публічної безпеки.

Суттєвою ознакою поняття «превенція» є наявність певної низки дій чи подій (правопорушення, інциденти), одні з яких передують іншим і випереджають очікувані наслідки від попередніх. Мова йде про випередження в чому-небудь, дій чи подій котрі передують настанню певних подій чи явищ.

На відміну від попередження, запобігання та припинення результат превенції є кращим, оскільки він не обтяжений наслідками дій і не потребує інших заходів. Поняття «превенція» в аспекті кримінальної розвідки та в контексті забезпечення національної, економічної та публічної безпеки, а також використання її за логікою РОП, розглядається як врегульований нормами оперативно-розшукового та кримінального процесуального законодавства випереджувальний вплив на джерела загроз та фактори, що сприяють криміналізації суспільних відносин.

Ризик – це ймовірна подія, яка може виникнути в майбутньому, якщо зазначена подія все ж таки відбудеться – це може стати проблемою. Тобто ризик виникає в майбутньому, несе певну невизначеність та може відбутися/або не відбутися в якийсь час.

Водночас проблема/проблемне питання – це відома, існуюча або встановлена обставина, яка є або спричинила виникнення певних питань чи обмежень, що потребують вирішення. Іншими словами проблема – це обставина, що вимагає активних дій для усунення негативних наслідків, запобігання їх виникненню та потребує вивчення, дослідження і розв'язання.

Виходячи з цього, тактика кримінальної розвідки за логікою РОП, визначає спосіб реагування на кримінальну загрозу, зокрема яких заходів КР доцільно вжити, зумовлюючи їх зміст, послідовність, місце, час та інтенсивність проведення. Вона також передбачає вміння визначати напрям і характер дій у певній ситуації та раціонально здійснювати їх з огляду на їх особливості і поставлені завдання.

Через певні особливості деяких елементів тактики: оперативній комбінації, тактичним прийомам, утаємниченості самої діяльності, набором особливих прихованих інструментів впливу на фігурантів та процеси, що відбуваються у кримінальному середовищі, зашифрованого спостереження за ризиковими фігурантами та процесами тощо, може бути досягнуто реалізація одного із видів реагування на ризики це його мінімізація. Завдяки поєднанню тактики КР, системи аналізу ризиків, кримінального аналізу досягається синергія в управлінні ризиками, що значно підвищує результативність реалізації превентивної функції правоохоронного органу, а також сприяє підвищенню ефективності протидії кримінальним загрозам в економіці.

Превентивна тактика в контексті застосування РОП або управління ризиками по суті є інституціональним фрагментом, який характеризує логіку використання сил, засобів та методів ОРД з метою мінімізації ризиків.

До основних принципів, необхідних при розробці та реалізації загальної стратегії управління кримінальними ризиками, відносять: системність, безперервність, баланс відповідальності та ініціативи, поєднання аналітики і ризикової евристики, багатоваріантність, проактивність.



впливу, визначити власника ризику або запропонувати заходи, що компенсують ризики, простежити за динамікою криміногенних процесів і, нарешті, прискорити їхню зміну в бік декриміналізації суспільних відносин, зокрема детінізації економіки, транспарентності системи управління публічними фінансами. Метою управління ризиками національної, економічної та публічної безпеки є не тільки сприяння поглибленому аналізу факторів, що впливають на процес криміналізації суспільних відносин, але й підвищення ефективності управлінських рішень.

Методи управління ризиками національної, економічної та публічної безпеки можуть і повинні стати засобом ефективної реалізації концепції її забезпечення на всіх рівнях управління – національному та регіональному. Якісне управління ризиком підвищує шанси системи управління безпекою домогтися успіху в довгостроковій перспективі, значно зменшує небезпеку неефективної реалізації самої концепції.

Важливо не тільки виявити потенційні ризики національної, економічної та публічної безпеки, але й оцінити їхній вплив на різні сфери життєдіяльності, вчасно ухвалити рішення щодо зниження ризиків, причому здійснювати управління ризиками на всіх стадіях кримінального циклу, а також реалізації концепції й адекватно задокументувати процеси управління ризиками для наступного використання цих знань у подальшій практиці управління аналогічними процесами.

Основними цілями превентивного впливу на процес криміналізації суспільних відносин в результаті застосування РОП є:

1. Зниження рівня криміналізації суспільних відносин, зокрема тінізації економіки;
2. Зниження кількості кримінальних правопорушень в певній сфері;

3. Зниження масштабів втягуваності законослухняних громадян у сферу відносин з високими кримінальними ризиками (географічний фактор (охоплення регіонів), кількісний фактор (кількість суб'єктів, що використовують типові способи вчинення злочину в галузі чи виді діяльності тощо);

4. Зниження збитків, шкоди, зокрема сум втрат бюджету та об'єму розкрадань міжнародної технічної допомоги;

5. Розподіл зон компетенцій між суб'єктами контролю (власниками ризику) в процесі детінізації економіки;

6. Удосконалення механізмів і алгоритмів аналізу ризиків, а також форм, способів та інструментів реагування на ризик;

7. Забезпечення зростання індексу якості оперативного контролю за криміногенною ситуацією.

Як нами вже зазначалося раніше, процес управління ризиками припускає проведення певних кроків, у тому числі:

- виявлення передбачуваних кримінальних ризиків у певній галузі, видах діяльності, діяльності державних установ тощо;

- аналіз і оцінка галузевих та об'єктових ризиків, ризик-послуг та ризик-рішень розпорядників бюджетних коштів, а також ризик-рішень суб'єктів контролю;

- вибір способів реагування на ризик та методів управління ризиками;

- застосування обраних методів;

- оцінку результатів управління ризиками.

Управління ризиком здійснюється на всіх стадіях кримінального циклу протиправної діяльності за допомогою моніторингу, контролю та необхідних коригуючих дій. Здійснює це відповідний аналітичний підрозділ правоохоронного органу у тісній взаємодії з його іншими підрозділами, а також з іншими суб'єктами контролю (власниками ризику), що мають оперативні можливості, юридичні повноваження та компетентності щодо реагування на ризики.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення: Закон України від 06 груд. 2019 р. № 361-IX.
2. Про Бюро економічної безпеки України: Закон України від 28 січ. 2021 р. № 1150-IX.
3. Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року «Про запровадження національної системи стійкості»: Указ Президента України від 27 верес. 2021 р. №479/2021.
3. Forrester, Jay W. (1973). *World Dynamics* (sec. ed.). Cambridge, Massachusetts. Wright-Allen Press, INC.
4. Ризик. Застосування ризик-орієнтованого підходу для побудови імовірнісних структурно-логічних моделей виникнення та розвитку. URL: https://pidru4niki.com/1800010250884/bzhd/rizik_zastosuvannya_rizikoriyentovano_pidhodu_dlya_pobudovi_imovirnisnih_strukturno-logichnih_modeley
5. Беккариа Чезаре. О преступлениях и наказаниях: пер. с итал. Киев: Ин Юре, 2014. 240 с.

Науково-методичне видання

СВИРИДЮК Наталія Петрівна
НЕКРАСОВ В'ячеслав Анатольович
АФОНІН Дмитро Сергійович

**Оцінювання ризиків поширення кримінальних загроз,
спроможностей та прогнозування протидії цим загрозам**

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ

Підписано до друку 23.12.2024. .Формат 60x84/16 Папір офсетний.

Гарн. «Times New Roman». Друк цифровий. Ум. друк .арк. 1,16.

Надруковано з готового оригінал-макета.

Наклад 30 прим.

Видавництво ОДУВС

м. Одеса, вул. Успенська, 1

Свідоцтво суб'єкта видавничої справи ДК № 3507 від 25.06.2009 р.