СЕКЦІЯ 1.
ФОРМУВАННЯ ДЕРЖАВНОЇ ПОЛІТИКИ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ В УМОВАХ ЗБРОЙНОГО КОНФЛІКТУ.

ВОЛОБОЄВ Артур
начальник відділу організації освітнього процесу
Донецького державного університету внутрішніх справ,
доктор філософії в галузі права

МЕХАНІЗМИ ДЕРЖАВНОГО ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ БОРОТЬБИ З ОРГАНІЗОВАНОЮ ЗЛОЧИННІСТЮ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

Збройна агресія російської федерації кардинально змінила природу організованої злочинності в Україні. Якщо раніше вона становила переважно кримінальну проблему, то сьогодні перетворилася на потужний інструмент гібридної війни. Саме тому І. В. Басиста слушно зазначає, що повномасштабне вторгнення вимагає принципово нового підходу до розуміння цієї проблематики. Організована злочинність тепер має розглядатися через призму її інституціоналізованості та тісного зрощення з терористичною діяльністю, яка здійснюється на користь країни-агресора. Особливо небезпечним є її поширення у цифровому просторі, де фактично одночасно ведуться «активні бойові дії» [1, с. 202].

Сучасні гібридні загрози являють собою складне об’єднання усталених злочинних практик, доповнених новітніми формами деструктивного впливу. Організовані злочинні формування вміло поєднують класичні кримінальні схеми з інформаційно-психологічними операціями, масштабними

кібератаками та цілеспрямованою підривною діяльністю проти об'єктів критичної інфраструктури. Умови воєнного стану створили для них додаткові можливості. Наприклад, послаблення державного контролю в окремих сферах дозволило розширити зони впливу та активніше виконувати завдання, спрямовані на підрив обороноздатності України.

Проблема полягає в тому, що існуюча нормативно-правова база виявилася неготовою до таких викликів. Основний документ у цій сфері – Закон України «Про оперативно-розшукову діяльність» [2], розроблявся для протидії традиційній злочинності та не враховує специфіки боротьби з організованими угрупованнями, які фактично стали агентами іноземного впливу. Хоча Стратегія інформаційної безпеки України, затверджена Указом Президента від 28 грудня 2021 року № 685/2021, окреслює концептуальні засади захисту від гібридних загроз [3], проте між стратегічними цілями та реальними операційними можливостями правоохоронних органів утворився значний розрив. У зв’язку з цим, подолання порушеного питання потребує створення якісно нової інтегрованої системи інформаційного забезпечення.

Так, досвід перших місяців повномасштабної війни продемонстрував вразливість централізованих підходів до інформаційного забезпечення. Цілеспрямовані атаки агресора на ключові вузли системи свідчили про необхідність переходу до більш стійкої моделі. Оптимальним рішенням стала децентралізована система, яка об'єднує відомчі інформаційні платформи таким чином, що система зберігає працездатність навіть при виході з ладу окремих її елементів.

В основі нової системи є мережа аналітичних підрозділів, діяльність яких регламентується статтею 8 Закону України «Про оперативно-розшукову діяльність» [2]. При цьому кожен підрозділ має свою спеціалізацію, зосереджуючись на конкретних аспектах гібридних загроз. Така структура дозволяє ефективно аналізувати різнотипні дані, залишаючись у межах визначених законом повноважень.

Технологічною основою системи стали графові бази даних, які дають змогу моделювати надзвичайно складні мережеві зв'язки між учасниками організованої злочинної діяльності. На відміну від облікових баз, вони здатні виявляти не лише звичні ієрархічні структури, але й приховані горизонтальні зв'язки з терористичними організаціями та кібергрупами, де технологія блокчейн забезпечує незмінність даних, ефективно протидіючи спробам дискредитації або фальсифікації доказової бази.

Усі процедури в системі стандартизовані відповідно до Постанови Кабінету Міністрів України № 373 від 29 березня 2006 року [4], однак з урахуванням особливостей функціонування в умовах воєнного стану, що вносить свої корективи в операційну діяльність.

Слід зауважити, що розроблена система захисту поєднує кілька рівнів безпеки. Квантово-стійкі алгоритми шифрування забезпечили захист даних від можливих загроз, а динамічна автентифікація та детальний рольовий контроль доступу створили додаткові бар'єри для зловмисників.

Крім того, доречно та своєчасно було створено для забезпечення надійності даних багаторівневу систему резервування з географічно розподіленими центрами обробки інформації. Така структура мінімізувала ризики втрати критично важливої інформації внаслідок фізичного знищення інфраструктури, так і через масштабні кібератаки.

У такому контексті, М. В. Калатур справедливо зазначає, що інформаційне забезпечення діяльності правоохоронних органів – це складна частина механізму організації діяльності, що в адміністративно-правовому плані передбачає одержання, збирання, реєстрацію, обробку, передачу, збереження та надання інформації шляхом створення інформаційних ресурсів, баз і систем, автоматизованих робочих місць із використанням новітніх методів і технологій [5, с. 62]. Цей механізм має забезпечувати максимальну оперативність без порушення фундаментальних правових принципів. Обробка персональних даних здійснюється виключно в інтересах національної безпеки, спираючись на положення частини 6 статті 6 Закону України «Про захист

персональних даних» [6]. Автоматизовані засоби контролю мають гарантувати дотримання принципів пропорційності та необхідності навіть при масштабному аналізі великих масивів інформації.

Вважаємо, що перспективні технологічні рішення вже активно впроваджуються у практичну діяльність. Зокрема, квантові обчислювальні системи змінили підхід до аналізу складних мереж злочинних організацій, оскільки дозволяють швидко опрацьовувати великі масиви взаємопов'язаної інформації. Водночас нейроморфні процесори нового покоління відкрили можливість обробки терабайтів даних у режимі реального часу, а технології доповненої та віртуальної реальності сформували нові інструменти для тривимірної візуалізації загроз і створення максимально наближених до необхідних умов підготовки аналітиків. Завдяки подальшій автоматизації операційної діяльності з'являється можливість спрямувати інтелектуальний потенціал правоохоронних органів на вирішення завдань стратегічного планування та ефективне реагування на непередбачувані ситуації.

Отже, проведене дослідження механізмів державного інформаційного забезпечення протидії організованій злочинності в умовах гібридних загроз виявило необхідність системної трансформації всієї правоохоронної діяльності. Гібридна війна кардинально змінила природу організованої злочинності, перетворивши її з кримінального явища на потужний інструмент державної агресії. Ця трансформація вимагає своєчасні відповіді через розробку принципово нових підходів до протидії.

На нашу думку, подальший розвиток системи протидії гібридним загрозам має охоплювати такі пріоритетні напрями, як:

- створення державної платформи збору та обробки даних про гібридні загрози з використанням технологій розподіленого реєстру, що забезпечить надійність та прозорість інформаційних процесів;
- розробка спеціалізованих алгоритмів штучного інтелекту, здатних виявляти складні патерни координованих гібридних операцій на ранніх стадіях їх підготовки;

– впровадження квантово-стійких технологій для захисту каналів обміну інформацією від потенційних загроз;

– створення дієвих механізмів державного контролю за використанням розширених аналітичних можливостей для запобігання зловживанням та захисту прав громадян.

Список використаних джерел:

1. Басиста І. В. Організована злочинність: сучасні українські реалії та кроки до протидії. *Науково-інформаційний вісник Івано-Франківського університету імені Короля Данила Галицького.* Вип. 15 (27). Том 2. С. 202–217. DOI: 10.33098/2078-6670.2023.15.27.2.202-217.

2. Про оперативно-розшукову діяльність. Закон України від 18.02.1992 № 2135-XII. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text.

3. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки». Указ Президента України від 28.12.2021 № 685/2021. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text.

4. Правила забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах. Постанова Кабінету Міністрів України від 29.03.2006 № 373. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text.

5. Калатур М. В. До проблеми визначення поняття інформаційного забезпечення діяльності слідчих органів України. *Актуальні проблеми держави і права.* Вип. 87. С. 59–64.

6. Про захист персональних даних. Закон України від 01.06.2010 № 2297-VI. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.