Застосування інформаційних технологій організованою злочинністю для впливу на суспільство

Р. А. Калюжний, Р. Л. Колпак

Глобальна інформаційна цивілізація, що формується на рубежі останніх тисячоліть, визначила інформацію своїм базовим параметром – видавнича справа, преса, радіо, телебачення, комп'ютерні технології, інші засоби електронного зв'язку – стали провідними чинниками економіки, виробничої, наукової, освітньої, політичної та інших сфер суспільної діяльності. Звідси випливає, що різні інформаційні системи і мережі телекомунікацій виступають як підсилюючий фактор суспільства і держави. У той же час вони виступають послаблюючим фактором, оскільки стають основним засобом в економічній, політичній, ідеологічній, військовій боротьбі супротивників і опонентів.

Новий виток інформаційної боротьби та її технологій почався у ході інформатизації, її провідної складової комп'ютеризації. Для встановлення нового потенційного плацдарму – Інтернету, електронних цифрових засобів збору, обробки та розповсюдження інформації – створюються всі необхідні умови. Звідси визначається актуальність теми щодо захисту інформації, забезпечення інформаційної безпеки суспільних складових від протиправного використання не тільки технічними, програмно-математичними, а й, здебільшого, організаційними та правовими методами.

В інформаційній цивілізації зростає роль суспільної думки, що також змінює "правила гри" у різних сферах суспільного буття. Сьогодні суспільна думка стала одним із суттєвих факторів, що впливає на процеси прийняття рішень на різних рівнях соціального і державного управління. Природно, що у відповідь породжуються ті чи інші моделі управління цими явищами.

Проблематика технологій інформаційної боротьби цікавить сьогодні багатьох: від технічних спеціалістів у контексті технічного захисту безпеки автоматизованих інформаційних систем до фахівців у галузі соціології, політології, геополітики, військової науки та права – у контексті інформаційної безпеки людини, суспільства, держави, світового співтовариства. Інтеграція їх зусиль у міжгалузевій комплексній інституції науки (науковій дисципліні) – інформаційній безпеці викликає розуміння концептів та інструментарію інформаційної боротьби, яка ще сьогодні недостатньо визначена у всій своїй природі та єдності та не ус-

відомлена як велика інтегрована складна соціальна система, як гіперсистема суспільного буття.

Тому ми розглядаємо окремі положення теорії технологій інформаційної боротьби стосовно практики організації боротьби з організованою злочинністю, протидії її впливу на суспільство у контексті інформаційної безпеки держави.

Інформаційне суспільство, до якого неминуче прямує Україна, змінює не просто статус інформації (відомостей, даних, знань) як каталізатора позитивних зрушень соціального буття, але й розширює можливості застосування інформації з антисоціальною метою злочинними формуваннями. Особливо це простежується в олігархічних кланах, у сфері так званої, "білокомірцевої організованої злочинності", злочинності, що сформувала свій капітал у "тіні", "мутній воді" періоду переходу до ринкової економіки в Україні, а тепер прагне закріпитися на владному "олімпі" держави чи веде боротьбу за нього. У цьому Україна не є оригінальною, подібні тенденції спостерігаються на всьому пострадянському просторі. Аналогічно формувалася владна олігархія переважно в багатьох країнах Заходу і Сходу, про що свідчать історичні джерела та науково-практична література.

Предметом наших наукових розвідок є інформація – універсальний "сильнодіючий засіб", для якого немає межі як у формуванні цивілізованого суспільства, так і в доведенні його до межі соціогенної катастрофи – загрози безпеки країни, а звідси – нації та окремій особі.

Методологія нашого дослідження базується на порівняльному системному аналізі експертних оцінок соціальних явищ у різних країнах, спостереженні та висуванні гіпотез та основ аналогій щодо тенденцій формування громадянських суспільств у державах.

Інформаційна боротьба різної інтенсивності за вплив на суспільство стала відвертою ознакою наших днів.

Наприклад, як зазначають дослідники, Росія визнала, що програла війну в Чечні в першу чергу через програну інформаційну війну [1].

Як зазначив Джордж Стейн у своїй праці "Інформаційна війна", ціль інформаційної війни є розум, особливо розум тих, хто приймає важливі рішення війни і миру,... розум тих, хто приймає ключові рішення і, якщо, коли і як використовувати існуючі сили і можливості стратегічних структур. Можна вважати, що визначні аспекти холодної війни, такі, як Радіо "Вільна Європа"... були генеральною репетицією інформаційної війни [2].

Саме у період холодної війни були відпрацьовані сучасні технології, що активно використовуються злочинними формуваннями для "рекрутування" до своїх рядів соціально нестійких індивідів: дезінформація, створення ореолу романтизму життя у злочинному світі, використання компромату, його фабрикації тощо.

Якщо за методом аналогії прослідкувати деякі події у нашій країні, то можна висунути гіпотезу, що інформаційна боротьба нерідко має характер інформаційної громадянської війни. Наприклад, "оксамитова революція у Верховній Раді" була програна прихильниками ідеології О. Ткаченка задовго до його усунення з посади Голови парламенту, адже вона базувалася на авторитаризмі, ідеях минулого та ігнорування потреб сучасності. Він залишився у полоні комплексу "колгоспної ідеї", що сформувала "тіньову" економіку в агропромисловому секторі України. Ця ідеологія віджила свій час, а її адепти не бажали пристосовуватися до нових економічних суспільних відносин та нового геопорядку інтеграції України, до нових міжнародних регіональних структур, новацій, що сформували у громадській думці переважної більшості населення нашої держави бажання жити у незалежній країні.

Наведемо й інший приклад з нашого політичного життя. Відсутність достатньої інформації, що мали надати правоохоронні органи вчасно, викликали рішення Президента України та Прем'єр-міністра стосовно призначення деяких членів Уряду з числа олігархів Паливно-енергетичному комплексу країни, капітал яких сформований був у "тіньовому" секторі економіки. Наслідки такого стану відомі.

Існує тенденція, – коли правоохоронні органи України починають активізувати боротьбу з організованою злочинністю і корупцією у вищих ланках державного управління, реалізовувати оперативно-розшукову інформацію для суду на організовані злочинні формування "білих комірців", відразу активізується інформаційна боротьба з публічною владою. При цьому "опонентами" застосовуються різні інформаційні технології, у тому числі новітні, для здійснення інформаційної агресії. Основні зусилля спрямовуються на перших керівників державних структур, що зобов'язані вести безпосередньо боротьбу зі злочинністю. За таких умов спостерігається тенденція до зростання темпів удосконалення інформаційної зброї організованих злочинних формувань "білих комірців", що перевищують розвиток адекватних технологій захисту. Перші особи в Уряді, в міністерствах і відомствах, які не усвідомлюють це, змушені йти у відставку під тиском замовленої "громадської думки".

У контексті організації боротьби з організованою злочинністю і корупцією в державі напрошується висновок, що при плануванні заходів щодо виявлення та розкриття протиправної діяльності організованих злочинних формувань необхідно передбачати заходи щодо ведення інформаційної боротьби з ними, у тому числі захисту від негативного інформаційного впливу на суспільство: протидії формуванню негативного іміджу працівників правоохоронних органів, паніки у суспільстві, кризи влади тощо. Образно це можна виразити народною мудрістю – "клин

клином треба вибивати". Застосування правоохоронними органами адміністративних заходів в інформаційній боротьбі з організованою злочинністю і корупцією подібно до "підливання масла у вогонь".

На цих прикладах продемонстровано, що інформаційні технології "сильних" роблять сильнішими, а "слабких" слабкішими. Цю аксіому слід пам'ятати тим, над ким гойдається "Домоклов меч" публічної влади, у тому числі керівникам правоохоронних органів. В Україні, як і в усіх країнах світу, війна компроматів стала звичайною справою. Інформаційні технології дають нові можливості тим, хто знає їх, володіє ними, вміє ними користуватися і вміє від них адекватно захищатися.

Наведемо висловлювання заступника Генерального директора Федерального агентства урядового зв'язку та інформації (ФАПСІ) при Президентові Російської Федерації у 1997 році В. Маркоменка, що кожна людина, військовий чи цивільний, бере участь в "інформаційній" війні у тій чи іншій формі [3].

Правоохоронні органи мають свою ділянку у цій війні – інформаційну боротьбу зі злочинністю як з фактором соціогенної загрози безпеці людини, суспільству, державі, світовому співтовариству. Для того, щоб захищати інших від негативного інформаційного впливу правопорушників, їх угруповань на суспільство, вони мають навчитися захищати і себе адекватними інформаційними технологіями захисту.

Дослідження свідчать, що сучасні держави добре розуміють значення інформації, особливо у кризових ситуаціях. В урядових органах багатьох країн сформовано спеціальні структури щодо ведення інформаційної боротьби, захисту від інформаційної агресії, у тому числі з боку організованих злочинних формувань. Ці структури також активно досліджують технології ведення боротьби з антисоціальними проявами у сфері суспільних інформаційних відносин.

На наш погляд, необхідно ввести до навчальних дисциплін "Інформаційне право" та "Теорія організації інформаційної безпеки", що запроваджуються до навчальних планів вищих закладів освіти МВС України, тематики стосовно технологій ведення інформаційного захисту: інформаційних відносин працівників правоохоронних органів із мас-медіа, журналістами; контрзаходи інформаційного впливу з боку злочинних угруповань на формування негативного ставлення громадської думки до правомірної діяльності правоохоронних органів.

1. *Почепцов П.* Информационные войны. – М.: Рефл-бук; 2000. – С. 10.

2. *Там само.*

3. Див.: *Известия.* – 1997. – 12 авг.