

Важливим, на нашу думку, є відкритість Державної служби для демократичного цивільного контролю з додержанням вимог законодавства про охорону державної таємниці.

III Висновки

Розглянуті етапи реорганізації служб, що пов'язані з реалізацією спеціального зв'язку та захисту інформації України, свідчать про доцільність проведених керівництвом держави Україна заходів, спрямованих на забезпечення ефективного функціонування, безпеки та розвитку державної системи урядового зв'язку і Національної системи конфіденційного зв'язку, визначення вимог і порядку створення та розвитку систем технічного та криптографічного захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом

Подальша ефективна діяльність, як свідчить досвід провідних країн світу, має проходити шляхом нарощування потужностей структур, на які покладено реалізацію згаданих завдань, шляхом підвищення їхнього значення в системі органів державного управління, створення додаткових важелів впливу на процеси реалізації державної політики у сфері інформаційної безпеки, особливо з позиції її важливості для безпечного та стабільного розвитку суспільства в умовах глобалізації процесів інформаційного обміну.

Література: 1. Конституція України від 28.06.1996 р. // Відомості Верховної Ради України. – 1996. – № 30. – ст. 141 – із змінами, внесеними згідно з Законом N2222-IV від 08.12.2004 р. // Відомості Верховної Ради України. – 2005. – № 2. – ст. 44. 2. Декларація про Державний суверенітет України від 16 липня 1990 року N 55-XII // <http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi>. 3. Закон України «Про Службу безпеки України» від 25 березня 1992 р. // <http://www.portal.rada.gov.ua>. 4. Положення про порядок здійснення криптографічного захисту інформації в Україні, затверджене Указом Президента України від 22 травня 1998 року № 505 // <http://www.president.gov.ua>. 5. Указ Президента України «Про додержання прав людини під час проведення оперативно-технічних заходів» від 7 листопада 2005 р., № 1556/2005 // <http://www.president.gov.ua/documents/3681.html>. 6. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» від 23.02.2006 р. // Відомості Верховної Ради України (ВВР). – 2006. – № 30. – ст. із змінами, внесеними згідно з Законами N879-VI від 15.01.2009 // ВВР – 2009. – № 24. – ст. 296; № 1180-VI від 19.03.2009 // ВВР – 2009. – № 32 – 33. – ст. 485; № 1415-VI від 02.06.2009 // ВВР – 2009. – № 41. – ст. 601.

УДК 681.3:34

ПЕРСПЕКТИВИ ПРОТИДІЇ КРИМІНАЛЬНИМ ЗАГРОЗАМ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ В УМОВАХ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

Дарія Прокоф'єва-Янчиленко

Головне управління по боротьбі з корупцією та організованою злочинністю СБ України

Анотація: Розглянуті питання щодо кримінальних загроз національній безпеці в умовах інформаційного суспільства, а також проблеми інформаційної та кримінологічної безпеки.

Summary: The article represents the research of criminal threat for state security in information world, information & criminology security's problems.

Ключові слова: Національна безпека, злочинність, корупція, загрози безпеці.

I Вступ

У рішенні РНБО України «Про стан злочинності у державі та координацію діяльності органів державної влади у протидії злочинним проявам та корупції», введеному в дію Указом Президента №870/2009 від 27. 10. 2009 р. [1], зазначається, що злочинність, особливо в умовах поглиблення соціально-політичної та фінансово-економічної кризи в державі, становить серйозну загрозу національній безпеці України та є одним із негативних чинників, який серйозно впливає на ефективність діяльності органів державної влади, підриває стабільність і систему правопорядку, захищеність прав, свобод і законних інтересів громадян. Однак в чому саме полягає ця загроза і як протидіяти їй в умовах розвитку інформаційного суспільства – дослідженню вказаних питань і присвячена ця стаття.

II Основна частина

Передусім слід звернутися до законодавчого підгунтя забезпечення національної безпеки України. Так, відповідно до ст. 2 Закону України «Про Службу безпеки України» [2], до завдань СБ України входить захист державного суверенітету, конституційного ладу, територіальної цілісності, економічного, науково-технічного і оборонного потенціалу України, законних інтересів держави та прав громадян від посягань з боку окремих організацій, груп та осіб, а також попередження, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, тероризму, корупції та організованої злочинної діяльності в сфері управління і економіки та інших протиправних дій, які безпосередньо створюють загрозу життєво важливим інтересам України. У вказаній статті, окрім конкретно-визначених протиправних проявів, мова йде про протиправні посягання на законні інтереси держави та права громадян та інші протиправні дії, які створюють загрозу життєво-важливим інтересам України. Перелік цих протиправних дій є невичерпним, однак законодавець наголошує на їх значній суспільній небезпеці, що дозволяє припустити, що йдеться передусім про злочинні прояви.

Аналізуючи зміст ст. 7 Закону України «Про основи національної безпеки України» [3] та зіставляючи зміст визначених в нормах закону загроз з положеннями Особливої частини Кримінального кодексу України (далі – КК України) [4], слід дійти висновку, що на сучасному етапі до основних загроз національній безпеці України у сфері державної безпеки належать діяння (та загроза вчинення відповідних діянь), передбачені *ст. 109-434, 447 КК України, статтями розділів XVII – XVIII КК України, ст.255–257, ст.258 – 258-5, ст.265–266 КК України, статтями розділу XX КК України, ст. 201, 260, 262–263, 267, 269, 410, 414, 305–308, 311–313, 320 КК України*. До основних загроз національній безпеці України у інших сферах належать діяння (та загроза вчинення відповідних діянь), передбачені *ст. 176, 177, 229, ст. 305–320 КК України, ст. 332, 439–440 КК України, статтями розділів V, XVII, XVIII КК України, окремі статті розділів II, III, VI КК України (в частині вчинення злочинів спеціальним суб'єктом), розділу VII КК України, ст. 113, 201, 237, 258 – 258-5, 268, 236, 333, 441, 442 КК України*, а також низка діянь, безпосередньо пов'язаних з інформаційною сферою, які наведемо докладніше:

прояви обмеження свободи слова та доступу громадян до інформації (*ст. 171, 232-2, 351, 238 КК України*);

поширення засобами масової інформації культу насильства, жорстокості, порнографії (*ст. 300, 301 КК України*);

комп'ютерна злочинність та комп'ютерний тероризм (*розділ XVI КК України*);

розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави (*ст. 111, 114, 328, 329, 422, 132, 145, 163, 168, 231-232, 381, 387, 397 148-6, 148-7, 182, 231, 232, 330 КК України*);

намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації (*ч.1 ст. 209-1, 221, ч.3 ст. 243, 285, 396, 351, 383, 384, ч.1 ст. 209-1, 218, ст. 220, 222, 259 КК України та деякі інші*).

Отже, значну питому вагу в системі загроз національній безпеці України становлять прояви діяльності, що визначена як злочинна за кримінальним законодавством України, а також інші види правопорушень та девіантної поведінки, які поки що не отримали належної кримінально-правової оцінки (наприклад, комп'ютерний тероризм), однак опосередковують злочинні прояви або зумовлюють їх як фонові явища. Таким чином, слід дійти остаточного висновку, що злочинність (не лише організована або транснаціональна) становить суттєву внутрішню загрозу національній безпеці України. При цьому з точки зору забезпечення безпеки доцільно розглядати реальні та потенційні прояви злочинності, які створюють загрозу життєво важливим інтересам України, а також її фонові явища як кримінальні загрози національній безпеці або її окремим складовим.

Спираючись на визначення національної безпеки, наведене у ст. 1 Закону України «Про основи національної безпеки України», необхідно констатувати, що від кримінальних загроз потерпають всі сфери реалізації національних інтересів (сфери правоохоронної діяльності, боротьби з корупцією, прикордонної діяльності та оборони, міграційної політики, охорони здоров'я, освіти та науки, науково-технічної та інноваційної політики, культурного розвитку населення, забезпечення свободи слова та інформаційної безпеки, соціальної політики та пенсійного забезпечення, житлово-комунального господарства, ринку фінансових послуг, захисту прав власності, фондів ринків і обігу цінних паперів, податково-бюджетної та митної політики, торгівлі та підприємницької діяльності, ринку банківських послуг, інвестиційної політики, ревізійної діяльності, монетарної та валютної політики, захисту інформації, ліцензування, промисловості та сільського господарства, транспорту та зв'язку, інформаційних технологій, енергетики та енергозбереження,

функціонування природних монополій, використання надр, земельних та водних ресурсів, корисних копалин, захисту екології і навколишнього природного середовища та інші сфери державного управління) та, відповідно, всі складові національної безпеки України. В свою чергу, це підводить до висновку про існування загального «крізу», «середовища» або «виміру» національної безпеки (в усіх її складових), в якому має забезпечуватись безпека від кримінальних загроз за рахунок протидії останнім та їх ефективній нейтралізації, а також здійснюватись правоохоронна діяльність органів державної влади та діяльність спецслужб щодо забезпечення державної безпеки. Останнє дозволяє вести мову не лише про загальний вимір національної безпеки, присутній в усіх її складових, але й про самостійну кримінологічну (або ж антикримінальну) складову національної безпеки [5–7].

В умовах бурхливого розвитку інформаційного суспільства протидія кримінальним загрозам та, відповідно, забезпечення кримінологічної безпеки неможливі без врахування специфіки інформаційної сфери та можливостей інформаційного простору як щодо продукування кримінальних загроз, так і щодо підвищення результативності протидії таким загрозам.

Інформаційне суспільство, основу якого складає світовий інформаційний простір, будується на досягненнях інформаційної сфери, яка утворюється сукупністю: суб'єктів інформаційних процесів (механічні, біологічні та соціальні інформаційні системи); інформації, призначеної для використання суб'єктами інформаційної сфери; інформаційної інфраструктури; суспільних відносин, що складаються у зв'язку з формуванням, зберіганням, передачею та розповсюдженням інформації. Чим активніше вона розвивається, тим більше від неї залежать політична, економічна, оборонна та інші складові національної безпеки, і ця залежність надалі зростатиме в ході розвитку технічного прогресу адже інформаційна сфера одночасно існує на двох рівнях: самостійно і у взаємозв'язку з іншими сферами життєдіяльності суспільства шляхом проникнення в них для здійснення інформаційного обслуговування та забезпечення їх взаємодії за допомогою інформації. Інформація завжди втілює певне змістовне навантаження, а отже, інформаційна сфера має своїм змістом достовірне або прогностичне знання – інформацію – про інші сфери життєдіяльності суспільства, що забезпечується формуванням інформаційних моделей інших сфер життєдіяльності суспільства, їх інфраструктури, суб'єктів та взаємодії останніх. При цьому всі взаємини між суб'єктами інформаційного суспільства ґрунтуються на споживанні й обміні інформацією, тому у соціальних системах залежність має інформаційну природу, яка слугує підставою для визначення завдання моделювання й оцінки стану національної безпеки [8–18].

Відповідно, інформаційна сфера в цілому та її окремі елементи стають привабливим об'єктом для численних протиправних посягань передусім внаслідок можливості справити опосередкований вплив на соціальну, економічну, політичну, духовну та інші сфери життєдіяльності. При цьому мова йде не лише про так звану комп'ютерну злочинність, але й про актуалізацію принципово новітніх суспільно небезпечних явищ, окремі з яких поки що взагалі не охоплені увагою законодавця в аспекті їх криміналізації [19–25].

Враховуючи, що злочинність являє собою конкретно-історичне явище, зміст і характер якого змінюється залежно від умов того чи іншого етапу розвитку суспільства, перебуваючи у системно-структурному взаємозв'язку з іншими соціальними системами (суспільні відносини, девіації, правопорушення тощо) та пристосовуючись до змін середовища, негативні соціальні відхилення – прояви становлення інформаційного суспільства, набувають рис криміногенних детермінант. Так, джерелом кримінальних загроз для суспільства і держави стає розширення каналів міждержавного інформаційного обміну, яке генерує умови для збирання іноземними спецслужбами розвідувальної інформації про Україну, а також впливу на формування національних інформаційних ресурсів шляхом цілеспрямованого наповнення інформаційного простору України власною (не завжди корисною або безпечною) інформацією. В таких умовах становлення суспільної свідомості значною мірою відбувається в напрямку, вигідному іноземним замовникам, під впливом проведення так званих спеціальних інформаційних операцій.

Відсутність географічних кордонів, важко визначальна національна належність об'єктів глобальних інформаційних мереж, анонімний доступ до їх ресурсів, маніпулювання свідомістю людини внаслідок інформаційних впливів та за допомогою технологій віртуальної реальності, поширення недостовірної та образливої для суспільної моралі інформації – все це робить вразливою систему захисту інформаційного простору України. Суспільство постійно потерпає від інформаційних впливів, що безпосередньо загрожують фізичному або психічному здоров'ю, формують морально-психічну атмосферу в суспільстві, підготовують кримінальне середовище та сприяють зростанню психічних захворювань [9–25]. Переважна більшість цих різнопланових негативних проявів становлення та розвитку інформаційного суспільства, в т.ч. досліджуваних в рамках проблеми інформаційної війни, за ступенем суспільної небезпеки потенційно припадає саме на злочини. Інформаційні мережі також стають зручним майданчиком для поширення пропагандистських матеріалів злочинних угруповань, готування та вчинення різноманітних злочинів, не лише пов'язаних з використанням комп'ютерної техніки, але й інших, зокрема, шахрайств, незаконного

збуту підконтрольних речовин, терористичних актів, замовних вбивств та інших загально-кримінальних злочинів тощо. Адаптуючись до умов інформаційного суспільства, злочинність (передусім організована та транснаціональна, адже в умовах інформаційного суспільства нівелюються кордони між внутрішніми та зовнішніми загрозами) отримує значний потенціал якісних змін та подальшого кількісного зростання внаслідок скрутного економічного становища, низької ефективності роботи правоохоронних органів, вад чинного законодавства, а також здатності інформаційної сфери справляти вплив на інші сфери життєдіяльності суспільства.

Все це вимагає не лише адекватного посилення кримінально-правового захисту інформаційної сфери за рахунок усунення прогалин кримінального закону та вдосконалення механізмів нейтралізації кримінальних загроз, джерелом яких є інформаційний простір, тобто, кримінально-правового, кримінологічного, кримінально-процесуального, оперативного-розшукового та контррозвідального забезпечення інформаційної безпеки, але й використання інформаційного простору та закономірностей розвитку інформаційної сфери в забезпеченні кримінологічної безпеки.

По-перше, інформаційна сфера є однією з самостійних сфер життєдіяльності об'єктів антикримінальної безпеки, що потенційно потерпає від кримінальних загроз, причому забезпечення інформаційної безпеки справляє позитивний вплив на забезпечення кримінологічної безпеки об'єктів в інших сферах їх життєдіяльності.

По-друге, власне вже визначення кримінологічної безпеки включає інформаційний фактор – усвідомлення захищеності від кримінальних загроз.

По-третє, з точки зору теорії інформації діяльність державних органів з викриття, знешкодження та прогнозування кримінальних загроз передусім носить інформаційний характер (являє собою процес збирання, аналізу та використання інформації), так само, як і власне процес вчинення злочину, як пов'язаного, так і не пов'язаного з використанням механічних інформаційних систем (особа, яка має намір вчинити злочин, оцінює інформацію щодо потенційного потерпілого, предмету або об'єкту злочину, можливі результати своїх дій тощо, займається інформаційним пошуком в процесі готування до злочину, здійснює безпосередній інформаційний вплив на потерпілого шляхом погроз, шантажу тощо; навіть у випадках вчинення злочинів без попередньої підготовки має місце отримання від зовнішнього середовища інформації, в т. ч. опосередкованої, яка спонукає до певних дій, та реакція на неї, яка в свою чергу змінює об'єктивну реальність та, відповідно, лишає по собі інформаційний слід. Тобто, процес підготовки та вчинення злочину супроводжується певною інформаційною взаємодією і відбивається зрештою в низці інформаційних моделей.

Це дозволяє вести мову про доцільність досліджень, спрямованих на розкриття відповідних закономірностей інформаційної сфери та врахування в діяльності щодо забезпечення антикримінальної безпеки факторів інформаційної причинності у злочинній діяльності та інформаційних характеристик кримінальних загроз.

Передусім це стосується необхідності підвищення ефективності використання оперативної інформації та диференціації шляхів її отримання, вдосконалення інформаційно-аналітичного забезпечення кримінологічної безпеки за рахунок розширення перспектив інформаційного моделювання та прогнозування, оскільки основа функціонування управлінського механізму забезпечення національної безпеки в цілому та його ефективність безпосередньо залежить від ефективності функціонування підсистеми інформаційного забезпечення. Адже не випадково, наприклад, п. 1 ч. 1 ст. 24 Закону України «Про Службу безпеки України» визначає пріоритетним обов'язком СБ України здійснення інформаційно-аналітичної роботи в інтересах ефективного проведення органами державної влади та управління України внутрішньої і зовнішньої діяльності, вирішення проблем оборони, соціально-економічного будівництва, науково-технічного прогресу, екології та інших питань, пов'язаних з національною безпекою України. Саме цей напрямок службової діяльності набуває особливої актуальності в умовах інформаційного суспільства. Так, п. 4.1 Стратегії національної безпеки України передбачає, що розвиток системи управління національною безпекою України має здійснюватися, зокрема, у напрямках: посилення прогностичної функції системи управління національною безпекою; підвищення ефективності діяльності суб'єктів забезпечення національної безпеки з упереджувального отримання інформації для своєчасного виявлення існуючих і нових типів внутрішніх і зовнішніх загроз, розробка дієвих заходів щодо їх запобігання та нейтралізації; інформаційно-аналітичної підтримки діяльності органів державної влади.

III Висновки

Таким чином, з урахуванням того, що у п. 1 резолютивної частини Рішення РНБО України «Про стан злочинності у державі та координацію діяльності органів державної влади у протидії злочинним проявам та корупції», введеного в дію Указом Президента № 870/2009 від 27. 10. 2009 р., визначено, що: «незважаючи

на певний прогрес у законодавчій та інституційній сферах, масштаби поширення злочинності та корупції сьогодні загрожують національній безпеці та конституційному ладу України. Діяльність органів виконавчої влади, координація їх зусиль щодо протидії кримінальним проявам є малоефективною, не повною мірою відповідає державним інтересам і вимогам національної безпеки України, не забезпечує ефективного захисту конституційних прав і свобод людини і громадянина, правопорядку в державі», а п. 2 резолютивної частини вказаного Рішення передбачає необхідність належного наукового супроводження процесів подолання відповідних істотних недоліків; подальше дослідження проблем кримінальних загроз національній безпеці та інформаційного аспекту протидії вказаним загрозам є перспективним та актуальним напрямком наукової роботи у сфері забезпечення національної безпеки.

Література: 1. Рішення РНБО України «Про стан злочинності у державі та координацію діяльності органів державної влади у протидії злочинним проявам та корупції», введене в дію Указом Президента №870/2009 від 27. 10. 2009 р.; 2. Закон України «Про Службу безпеки України» від 25. 03. 1992 р.; 3. Закон України «Про основи національної безпеки України» від 19. 06. 2003 р.; 4. Кримінальний кодекс України від 05. 04. 2001 р.; 5. Горшеников Г. Г. Антикримінальная безопасность личности: Дис. ... д-ра юрид. наук : 12. 00. 08 : Ставрополь, 2009. 447 с.; 6. Плеваков В. А., Нечевина Н. Д. Криминологическая безопасность в системе общественной безопасности // Предупреждение преступности и обеспечение безопасности в городах: Материалы международной науч.-практ. конф. (7–8 апреля 1999 г.) / Моск. юрид. ин-т МВД России. -М., 1999. -С. 135–144; 7. Бабаев М. М., Плеваков В. А. Криминологическая безопасность в системе национальной безопасности (опыт структурного анализа) // Криминологический журнал, 2005, № 7; 8. Доктрина інформаційної безпеки України; 9. Емельянов Г. В., Стрельцов А. А. Проблемы обеспечения безопасности информационного общества // Информационное общество. 1999. №2. - С. 15–18.; 10. Красноступ М. Д. Інформаційна безпека України: сутність та проблеми // Інформаційні технології та захист інформації. – 1999. - №1. - С. 108–110; 11. Баранов А. А. Концептуальные вопросы информационной безопасности Украины // Нормативно-правовая база защиты информации: Сб-к материалов. - К., 1997. - С. 53–58; 12. Рубан В. Я. Інформаційна безпека України: сутність та проблеми // Стратегічна панорама. - 1998. - № 3. - С. 174; 13. Лопатин В. Н. Информационная безопасность России: Автореф. дис...докт. юрид. наук.– СПб., 2000. – 28 с.; 14. Шамрай В. О. (п.д./2002). Інформаційна безпека як складова національної безпеки України [WWW документ]. URL [http:// www.crime-research.org/ articles.html](http://www.crime-research.org/articles.html) (08 листопада 2004 року); 15. Васенин В. А., Галатенко А. В. Компьютерный терроризм и проблемы информационной безопасности в Интернет // Высотехнологичный терроризм. Материалы российско-американского семинара РАН в сотрудничестве с Национальными академиями США. Москва, 4–6 июня 2001 г. - М., 2002. - С. 211–225; 16. Литвиненко О. В. Інформаційний простір як чинник забезпечення національних інтересів України. - К., 1998. - 50 с.; 17. Ліпкан В. Націобезпекознавча парадигма //Право України 2003 рік, №2; 18. Данильян О. Г., Дзьобань О. П., Панов М. І. Національна безпека України: структура та напрямки реалізації: Навчальний посібник. - Х.: Фоліо, 2002–285 с.; 19. Расторгуев С. П. Информационная война. - М.: Радио и связь, 1998. - 415 с.; 20. Почепцов Г. Г. Информационные войны. - М.: «Рефл-бук», К.: «Ваклер», 2000. - 567 с.; 21. Емельянов Г. В., Ленский В. Е., Стрельцов А. А. Проблемы обеспечения информационно-психологической безопасности России // Информационное общество. - 1999. - № 3. - С. 47–51; 22. Крылов В. В. Информация как элемент криминальной деятельности // Вестник Московского университета, Серия № 11 (Право). - 1998. - № 4. - С. 59–63; 23. Хананашивили М. М. Информационные неврозы. - М.: Медицина, 1986. – 310 с.; 24. Дремин В. Н. Глобализация информационных систем как фактор глобализации преступности // Інформаційні технології та безпека. - Вип. 1. – К., 2002. - С. 56–59; 25. Мальцев В. В. Категория «общественно-опасное поведение» и ее уголовно-правовое значение // Государство и право. - 1995. - № 9. - С. 58–60.

УДК 621.391

СТРУКТУРА ТА МОДЕЛЬ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В РАМКАХ ПРОЦЕСНОГО ПІДХОДУ

Олександр Потій, Анатолій Леншин, Дмитро Пилипенко

Інститут інформаційних технологій

Анотація: Запропонована модель управління процесами захисту інформації, що дозволяє впроваджувати у практику захисту інформації вимоги стандарту ISO/IEC 27001. Визначено два контури управління – контур управління за результативністю та контур управління за зрілістю.