Подальші наукові розвідки за темою статті доцільно здійснювати за такими **напрямами**: 1) співвідношення функції кримінального переслідування з діяльністю із притягнення особи до кримінальної відповідальності; 2) дослідження пізнавального елементу діяльності з кримінального переслідування і його співвідношення з процесуальними елементами такої діяльності.

Список літератури: 1. Концепція реформування кримінальної юстиції України / Затв. Указом Президента України від 8 квітня 2008 року № 311/2008 // http://www.president.gov.ua/documents/ 7703.html? PrintVersion. 2. Ларин А. М. Расследование по уголовному делу: процессуальные функции. – М., 1986. 3. Парадеев В. М. О понятии обвинения // Уголовно-процессуальные формы борьбы с правонарушениями. – Свердловск, 1983. 4. Проект Кримінального процесуального кодексу, підготовлений Робочою групою Національної комісії зі зміцнення демократії та утвердження верховенства права. – К., 2007. – 155 с. 5. Строгович М. С. Уголовное преследование в советском уголовном процессе. – М., 1951. 6. Таджиев Х. С. Прокурорский надзор и ведомственный контроль за расследованием преступлений. – Ташкент, 1985. 7. Фаткуллин Ф. Н. Обвинение и его изменение в суде. – Казань, 1963. 8. Фойницкий И. Я. курс уголовного судопроизводства. – СПб., 1912. – Т. 2. 9. Халиулин А. Г. Осуществление функции уголовного преследования прокуратурой России. – Кемерово, 1997. 10. Чеканов В. Я. Прокурорский надзор в уголовном судопроизводстве. – Саратов: Изд-во Саратовского ун-та, 1972. 11. Щегель Н. І. Кримінальне переслідування: зміст та форми: Автореф. дис…. канд. юрид. наук. – К.: КНУВС, 2007. – С. 19.

Надійшла до редколегії 10.11.08

О. В. Бойченко

Інформаційна безпека України: поняття та загрози

Розвиток і впровадження практично в усі сфери діяльності інформаційних технологій суттєво змінює структуру суспільства, а також трансформує міжнародні відносини. Одним із найважливіших напрямків цієї трансформації є реалізація національних інтересів щодо забезпечення національної безпеки.

Починаючи із середини XX ст., триває бурхливий розвиток інформаційних технологій, які набули глобального характеру. Обсяги світової інформаційної індустрії на початку 90-х рр. минулого сторіччя досягли 2 трлн. доларів США, а на початку XXI ст. зросли у кілька разів [1].

Тому можна стверджувати, що у світі відбувається стрімке формування інформаційного суспільства. Головною його особливістю є те, що стратегічним ресурсом стає інформація, яка здатна взаємодіяти не тільки з матеріальним, але й із духовним світом людини. Ось чому у програмі інтеграції України до Європейського союзу розділ «Інформаційне суспільство» був включений як базовий [2].

Метою роботи є визначення основних понять, сутності та рівнів загрози інформаційній безпеці України як невід'ємного складника національної безпеки.

Інформаційне суспільство, як і будь-яка система, складається зі структурних одиниць, до яких належить суб'єкти інформацій-

них процесів; інформація, призначена для використання суб'єктами інформаційного суспільства; інформаційна інфраструктура та суспільні відносини, які утворюються у зв'язку зі створенням, зберіганням, переданням та розповсюдженням інформації [3; 4].

Суб'єкти інформаційної сфери та окремі елементи її інфраструктури можна об'єднати поняттям «інформаційна система». Вона забезпечує одержання й обробку даних, отримання результату або зміну власного зовнішнього стану [5].

Метою існування інформаційних систем, що інтегровані до інформаційного суспільства, є змінення поведінки інших інформаційних систем у своїх інтересах або ж підтримання їх поведінки незмінною. Кожна інформаційна система може розглядатися як об'єкт інформаційного впливу, який реалізується цілеспрямованим переданням інформації, що включає як змістовий (відображення реальної діяльності), так і представницький складники (форму представлення інформації для передання та забезпечення адекватного засвоєння), а також має певну цінність аспектом [6].

За своєю сутністю інформація може формувати матеріальне середовище життя

людини (інноваційні технології, комп'ютерні програми тощо). Водночас вона може використовуватись як основний засіб міжособистісної взаємодії, постійно виникаючи та змінюючись у процесі переходу від однієї інформаційної системи до іншої.

Як товар інформація може користуватися попитом, оскільки має певну цінність, однак її специфіка, пов'язана з перетворенням людських знань, створює складності у визначенні її вартості [7]. Проте, на нашу думку, цінність інформації насамперед визначається її достовірністю, цілісністю та доступністю. Остання робить інформацію найбільш привабливою, оскільки її конфіденційність визначається встановленим режимом доступу й обмежується колом осіб, які мають право володіти нею [8].

Слід відзначити, що в Україні інформація з обмеженим доступом поділяється на два різновиди – таємну і конфіденційну. Відповідно до Закону України «Про інформацію» до таємної інформації відносять такі відомості, розголошення яких завдає шкоди особі, суспільству і державі та яка включає до свого складу державну або іншу визначену законом таємницю [9]. Перелік видів таємної інформації визначається державою і закріплюється законодавчо.

Державна таємниця включає в себе відомості зі сфери оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визначені у встановленому законом порядку державною таємницею і підлягають охороні державою [10].

Таким чином, можна говорити про те, що захист інформації, віднесеної до конфіденційної і, перш за все, до державної таємниці, слід вважати невід'ємним складником національної безпеки України. Іншими словами, можна стверджувати, що інформаційна безпека визначається як захищеність важливих інтересів особи, суспільства та держави в інформаційній сфері, що забезпечує використання інформації в інтересах її суб'єктів, сталий розвиток держави, виявлення, попередження і ліквідаці. загроз національним інтересам.

Категорія національних інтересів в інформаційній сфері повною мірою узгоджується з іншою категорією – національною безпекою і відноситься до неї як частина до цілого. При цьому слід ураховувати, що інформаційний чинник не може існувати поза цілями загальної національної безпеки, так само як і національна безпека не буде всеохоплюючою без інформаційної безпеки [11].

У цілому політика національної безпеки держави спрямована на мінімізацію та, по можливості, уникнення існуючих чи потенційних внутрішніх або зовнішніх загроз розвитку держави відповідно до її цілей [12].

Уперше поняття «національна безпека» та «національні інтереси» на законодавчому рівні були визначені у «Концепції (основах державної політики) національної безпеки України» та знайшли подальший розвиток у Законі України «Про основи національної безпеки України» [13].

У Законі визначається, що захист національної безпеки є однією з найважливіших функцій держави. У цьому контексті інформаційна безпека як невід'ємний складник національної безпеки має бути забезпечена на державному рівні, оскільки протягом усієї історії розвитку людства інформація розглядалася як важливий військовий, політичний, економічний і соціальний фактори, що значною мірою обумовлює розвиток держави, суспільства й особистості в конкретних історичних умовах.

Однією з характерних ознак так званої «інформаційної революції» в цій сфері стало народження електронної комерції, яка розвивається відповідно до законів ринку та вільної конкуренції [14]. Ці обставини збільшили попит на стратегічну інформацію, яка безпосередньо пов'язана з діяльністю держави.

Головною характеристикою стратегічної інформації є спеціальний правовий режим її збору, збереження і використання, тобто режим таємності, який забезпечується силою державного примусу. Ця інформація залишається стратегічною лише доти, поки вона не доступна іншим сторонам, які віднесені до ймовірних противників. Але вдосконалення інформаційних технологій зробило державну таємницю не абсолютним, а відносним поняттям.

Тому, на думку деяких фахівців [15], постійно зменшується кількість часу, протягом якого держава здатна зберігати секретність інформації, зокрема, стратегічної.

Визначені закономірності дозволяють дійти висновку, що в сучасних умовах традиційні підходи щодо забезпечення інформаційної безпеки швидко втрачають свою ефективність і потребують постійного удосконалення.

Одним з основних елементів реалізації державної політики в інформаційній сфері є інформаційна інфраструктура, яку слід вважати невід'ємною частиною стратегічних інформаційних ресурсів і такою, що має значення для обороноздатності держави та її інформаційного ринку.

Так, згідно з Законом України «Про національну програму інформатизації» [16] до інформаційної інфраструктури входять:

– міжнародні та міжміські телекомунікаційні та комп'ютерні мережі;

– системи інформаційно-аналітичних центрів;

– інформаційні ресурси;

– інформаційні технології;

– системи науково-дослідних установ з проблем інформатизації;

– виробництво та обслуговування технічних засобів інформації;

– система підготовки кваліфікованих фахівців у сфері інформатизації.

Аналізуючи державну політику в інформаційній сфері, слід визначити місце питань інформаційної безпеки, які наведені в юридичній літературі й базуються на розумінні інформаційної безпеки як складника національної безпеки України.

Основним завданням заходів забезпечення інформаційної безпеки є мінімізація шкоди через неповноту, несвоєчасність або недостовірність інформації чи негативного інформаційного впливу через наслідки функціонування відповідних інформаційних технологій, а також несанкціоноване поширення інформації [17]. Саме тому інформаційна безпека передбачає наявність певних державних інститутів і умов існування її суб'єктів, що встановлені міжнародним і вітчизняним законодавством [18].

Поняття інформаційної безпеки держави слід також розглядати у контексті забезпечення безпечних умов існування інформаційних технологій, які включають питання захисту інформації, інформаційної інфраструктури держави, інформаційного ринку та створення безпечних умов існування і розвитку інформаційних процесів.

Необхідний рівень інформаційної безпеки забезпечується сукупністю політичних, економічних, організаційних заходів, спрямованих на попередження, виявлення й нейтралізацію тих обставин,

факторів і дій, які можуть завдати збитків чи зашкодити реалізації інформаційних прав, потреб та інтересів країни і її громадян.

Слід зазначити, що поняття «інформаційна безпека держави» розглядали І. Арістова, А. Письменницький, В. Бондаренко, О. Литвиненко, Б. Кормич, В. Остроухов, А. Стрельцов, С. Расторгуєв, А. Баринов, І. Бачило [3, 5, 19–24 та ін.

На наш погляд, інформаційну безпеку держави, у контексті стану її інформаційної захищеності, при якому не завдається суттєвої шкоди національним інтересам, необхідно визначити як комплекс заходів захисту від спеціальних інформаційних операцій, актів зовнішньої інформаційної агресії та негласного зняття інформації (за допомогою спеціальних технічних засобів), інформаційного тероризму та комп'ютерних злочинів.

Тому для розуміння реальних та потенційних загроз інформаційному простору України необхідно дати визначення інформаційних операцій та актів зовнішньої інформаційної агресії, інформаційного тероризму та комп'ютерної злочинності.

Спеціальні інформаційні операції – це сплановані дії, спрямовані на ворожу, дружню або нейтральну аудиторію шляхом впливу на її свідомість і поведінку за допомогою використання певним чином організованої інформації та інформаційних технологій для досягнення певної мети.

Акти зовнішньої інформаційної агресії – легальні або протиправні акції, реалізація яких може мати негативний вплив на безпеку інформаційного простору держави.

Вони поділяються на такі види:

– операції, спрямовані проти суб'єктів, які ухвалюють рішення;

– операції, спрямовані на компрометацію, завдання шкоди опонентам;

– операції, спрямовані на політичну (економічну) дестабілізацію.

Зазначені акції відбуваються на макро- і мікрорівні. Макрорівень характеризується різною агітаційно-пропагандистською й розвідувально-організаційною діяльністю, яка орієнтована на конкретні соціальні групи людей через засоби масової інформації та канали комунікацій.

На мікрорівні застосовується агітаційно-пропагандистська і розвідувально-організаційна діяльність ідеологічного характеру, прицільно персоналізована і здійснювана, переважно, через міжособистісне спілкування. Часто це діяльність, що спрямована на поширення чуток чи на провокування іншими методами негативного поводження населення держави-об'єкта інформаційної війни.

Розглядаючи поняття спеціальних інформаційних операцій та актів зовнішньої інформаційної агресії в контексті заходів політичної розвідки, слід зазначити, що за її допомогою мають вирішува-

тися певні політичні проблеми, досягатися стратегічні цілі суспільства певної держави чи іншого суб'єкта розвідувальної діяльності.

Для об'єкта, на який спрямовані спеціальні інформаційні операції та акти зовнішньої інформаційної агресії, мають настати або ж утворитися загрози чи небезпеки виникнення негативних наслідків. Отже, такий вплив на об'єкт за своєю суттю є також негативним. Вплив як такий застосовується як до окремої особи чи групи осіб, так і на все суспільство в цілому або певний його соціальний прошарок.

Таким чином, спеціальні інформаційні операції та акти зовнішньої інформаційної агресії мають бути діяльністю, яка проводиться спеціальними органами іноземних держав чи транснаціональних структур, які уповноважені суб'єктом інформаційної війни здійснювати таку діяльність. Тобто основним суб'єктом спеціальних інформаційних операцій та актів зовнішньої інформаційної агресії є спецслужби іноземних держав для здійснення таємних операцій та акцій негативного, деструктивного ідеологічного, ідейно-політичного та соціального впливу на особу, групу осіб або суспільство в цілому з метою їх переорієнтації на інші цінності та ідеали, підштовхнути до вчинення протиправних дій, щоб підірвати і послабити державний та суспільно-політичний лад для здійснення вигідного впливу.

Основою їх діяльності є розповсюдження певної інформації (правдивої чи фальшивої) через використання комунікаційних технологій із впливу на масову свідомість із довготривалими чи короткотривалими цілями. Необхідно підкреслити, що спеціальні інформаційні операції та акти зовнішньої інформаційної агресії створюють загрозу не стільки як явище взагалі, скільки тим, що вона «вмикає» та контролює речово-енергетичні процеси, результатом чого є збудження процесів, масштаби яких у багато разів більші за саму операцію.

Саме цей вид інформаційної боротьби, як правило, скерований на переорієнтацію окремих осіб, їх груп чи суспільства в цілому на інші цінності та ідеали для послаблення політичного і соціально-політичного устрою. Коли заходи безпосереднього інформаційного підриву є інструментом політичної розвідки, їхня мета також має політичний характер.

Отже, спеціальні інформаційні операції та акти зовнішньої інформаційної агресії передбачають заплановане спричинення шкоди життєво важливим інтересам у політичній, економічній, науково-технічній, соціальній чи будь-якій іншій суспільній сферах життя держави-супротивника та здійснення на цій основі вигідного впливу для отримання переваг у тій чи іншій галузі.

Іншим, не менш небезпечним джерелом загроз інформаційній безпеці держави є інформаційний тероризм, що визначається як

небезпечні діяння з інформаційного впливу на соціальні групи осіб, державні органи влади й управління, пов'язані з розповсюдженням інформації, яка містить погрози переслідуванням, розправою, вбивствами, а також викривлення об'єктивної інформації, що спричиняє виникнення кризових ситуацій в державі, нагнітання страху і напруги в суспільстві.

Порівнюючи інформаційний тероризм зі спеціальними інформаційними операціями та актами зовнішньої інформаційної агресії, слід відзначити його характерні ознаки. По-перше, це короткочасність впливу, по-друге, суб'єктами інформаційного тероризму є менш кваліфіковані організації (суб'єктами можуть бути сторонні особи, які мають відповідну підготовку до застосування інструментів інформаційного тероризму). Та, по-третє, об'єктами впливу є менш широка аудиторія. Таким чином, інформаційний тероризм може бути визначено як другий (менш небезпечний) рівень загроз інформаційній безпеці держави.

Третій рівень загроз інформаційній безпеці створюють комп'ютерні злочини – протиправні діяння у сфері використання електронних обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж. Відповідальність за скоєння зазначених злочинів передбачена чинним Кримінальним кодексом України.

Підводячи підсумок, можна стверджувати, що інформаційна безпека передбачає можливість безперешкодної реалізації суспільством та окремими його членами своїх конституційних прав, пов'язаних із можливістю вільного одержання, створення й розповсюдження інформації.

Крім цього, інформаційна безпека повинна забезпечуватися проведенням цілісної державної програми відповідно до Конституції, чинного законодавства України та норм міжнародного права шляхом реалізації відповідних доктрин, стратегій, концепцій і програм, що стосуються національної інформаційної політики України.

Список літератури: 1. Якушев М. В. Информационное общество и правовое регулирование: новые проблемы теории и практики // Информационное общество. – 1999. – № 1. – С. 40-43. 2. Указ Президента України «Про Програму інтеграції України до Європейського Союзу»: від від 14.09.2000, № 1072/2000 (зі змінами, внесеними згідно з Указом Президента № 1411/2004 від 16.11.2004) / [Електронний ресурс]. – Режим доступу: http://search.liga.kiev.ua. 3. Стрельцов А. А. Направление совершенствования правового обеспечения информационной безопасности Российской Федерации // Информационное общество. – 1999. – № 6. – С. 15–21. 4. Шерстюк В. П. Информационная безопасность в системе обеспечения национальной безопасности России: федеральный и региональный аспекты обеспечения информационной безопасности // Информационное общество. – 1999. – № 5. – С. 3–5. 5. Расторгуев С. П. Информационная война. – М.: Радио и связь, 1998. – 415 с. 6. Беляков К. И. Управление и право в период информатизации. – К.: КВШ, 2001. – 308 с. 7. Снытников А. А., Туманова Л. В. Обеспечение и защита права на информацию. – М.: Городец-издат, 2001. – 344 с. 8. Термінологічний словник з питань технічно-

го захисту інформації / За ред. проф. В. О. Хорошка – 3-є видання. – К.: Поліграф Колсалтинг, 2003. – 268 с. 9. Закон України «Про інформацію»: від 02.10.1992 р., №2658-XII/92-ВР (зі змінами і доповненнями, внесеними Законами України № 1642-III від 6.04. 2000 р., № 3047-III від 7.02.2002 р., № 676-IV від 3.04.2003 р., № 1268-IV від 18.11.2003 р., № 1703-IV від 11.05.2004 р., № 2707-IV від 23.06.2005 р.) // ВВР України. – 1992. – № 48. – Ст. 650. 10. Закон України «Про державну таємницю»: від 21.01.1994 р., № 34/94-ВР // ВВР України. – 1994. – № 16. – Ст. 93. 11. Політологічний енциклопедичний словник. – К.: Генеза, 1997. – С. 34. 12. Гелей С., Рутар С. Політологія. – К.: Знання, 1999. – С. 13. 13. Закон України «Про основи національної безпеки України»: від 19.06.2003 р. №964-IV/2003-ВР (зі змінами і доповненнями, внесеними Законом України № 3200-IV від 15.12.2005 р.) // ВВР України. – 2003. – № 39. – Ст. 351. 14. Соболев В. Информация и переходная инфраструктуры // Бизнес. Информ. – 1999 – № 3-4. – С. 36. 15. Cleveland. The knowledge executive. Leadership in an information society/ – New York: Truman Telley books, 1989. – P. 32. 16. Закон України «Про Національну програму інформатизації»: від 04.02. № 74/98-ВР (із змінами, внесеними згідно із Законом № 2684-III від 13.09.2001 р.) // ВВР. – 2002. – № 1. – Ст. 3. 17. Баринов А. Информационный суверенитет или информационная безопасность? // Національна безпека і оборона. – 2001. – № 1. – С. 70–76. 18. Бачило И. Л. Информационное право: основы практической информации. – М., 2001 – С. 253. 19. Бондаренко В. О., Литвиненко О. В. Інформаційна безпека сучасної держави: концептуальні роздуми // Стратегическая панорама. – 1999. – № 1–2. – С. 127–133. 20. Бондаренко В. О., Литвиненко О. В. Інформаційні впливи і операції // Стратегическая панорама. – 1999. – № 4. – С. 134-140. 21. Інформаційна безпека України. Проблеми і шляхи вирішення. Заочний круглий стіл // Національна безпека і оборона. – 2001. – № 1. – С. 24–29. 22. Кормич Б. А. Інформаційна безпека: організаційно-правові основи: Навч. посібник. – К.: Кондор, 2004. – 384 с. 23. Петрик В. М., Остроухов В. В. та ін. Сучасні технології та засоби маніпулювання свідомістю, ведення інформаційних війн і спеціальних інформаційних операцій: Навч. посібник. – К.: Росава, 2006. – 208 с. 24. Баринов А. Информационный суверенитет или информационная безопасность? // Національна безпека і оборона. – 2001. – № 1. – С. 70–76.

О. І. Опанасенков

Критерії та показники якості, що висуваються до кримінально-виконавчого законодавства

Будь-яке законодавство створюється правниками, а діє в реальному житті на основі існуючих правовідносин. Право повинно бути взаємопов'язаним із різними сторонами суспільного життя і визначати ті умови, що забезпечують якість останнього. У свою чергу, відповідність права суспільним відносинам сьогодення, соціальній структурі суспільства, ідеології та менталітету – основна умова його якості та ефективності.

На думку Ю. І. Бірченка, у визначенні умов ефективності дії права необхідно використовувати системний підхід, тобто враховувати, що ефективність залежить від усіх елементів системи: від правової надбудови в цілому; від суспільних відносин; від культури суспільства, його традицій, звичаїв, історичної спадщини; від діяльності державних установ, громадських організацій тощо [1].

Складовою частиною кримінально-виконавчого права є Кримінально-виконавчий кодекс України (далі – КВК). Від того, наскільки якісним є кримінально-виконавче законодавство, наскільки