УДК 347.963

А. С. ХОМИЧ,
здобувач
Харківського національного університету внутрішніх справ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ЯК ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ПРОКУРАТУРИ

Виконано дослідження правових питань захисту прокуратури від впливу інформаційних технологій як загрози її інформаційній безпеці, здійснене на підставі аналізу відповідних нормативно-правових актів і поглядів науковців.

Сучасний етап реформування правоохоронної системи України передбачає перехід від екстенсивних до інтенсивних методів здійснення управлінських процесів, що обумовлює підвищену увагу до вдосконалення систем інформаційного забезпечення, від ефективного функціонування яких залежить злагоджена дія всіх правоохоронних органів. Без інформаційних технологій неможливо налагодити ефективну взаємодію між владними структурами, а також належним чином підвищити ефективність та якість вироблення й прийняття рішення, вчасно виявити управлінську помилку. При цьому необхідно зауважити, що, незважаючи на підвищену увагу з боку науковців та практиків до інформаційного забезпечення правоохоронних органів взагалі і органів прокуратури зокрема, на цьому шляху залишається багато невирішених проблем, пов'язаних насамперед із повільним впровадженням в управлінську практику інформаційних технологій та недостатнім використанням усіх можливостей сучасної обчислювальної техніки, засобів зв'язку тощо.

У той же час широке запровадження інформаційних технологій та зростання ролі інформації в діяльності органів прокуратури викликає проблему забезпечення інформаційної безпеки, адже запровадження інформаційних технологій робить більш відкритою роботу органів прокуратури. Це не тільки цілком позитивне явище з точки зору можливості контролю з боку громадського суспільства за діяльністю прокуратури. Стурбованість викликає саме відкритість діяльності прокуратури для несанкціонованого, незаконного доступу до інформації, витоку інформації, створення умов для зменшення ефективності або унеможливлення заходів прокурорського реагування. Зрозумілим є те, що, наприклад, витік інформації про заплановані заходи в рамках розслідування злочинів чи проведення перевірки діяльності відповідних суб'єктів може ставити під загрозу весь хід розслідування чи перевірки, а подекуди призводить до унеможливлення відновлення порушених правових приписів, уникнення винними особами відповідальності та спричинення значних збитків. Такі дії зрештою знижують можливості органів прокуратури щодо належного, ефективного та своєчасного виконання покладених завдань і завдають шкоди інтересам держави та суспільства.

Велика кількість публікацій у вітчизняній і зарубіжній науковій і періодичній літературі [1; 2; 3], що ілюструють небезпеки того або іншого інформаційного впливу, свідчить про актуальність належного правового захисту інтересів особи, суспільства і держави в даній сфері.

Необхідно відзначити, що в правовій науці, зокрема у сфері інформаційного права, окремим аспектам інформаційної безпеки присвятили свої праці як українські, так і російські вчені: А. Б. Агапов, І. В. Арістова, О.А. Баранов, Ю. М. Батурін, І. Л. Бачило, М. М. Биченок, В. М. Брижко, В. Д. Гавловський, В. П. Горбулін, Д. В. Дубов, В. Г. Заблоцький, Р. А. Калюжний, В. А. Копилов, П. У. Кузнецов, В. А. Ліпкан, А. І. Марущак, І. В. Панова, А. О. Рось, В. Я. Рубан, Г. П. Стежка, В. Г. Хахановський, В. С. Цимбалюк, М. Я. Швець, Ю. С. Шемшученко тощо. Проте зазначені дослідження та наукові праці стосувалися лише окремих напрямків у сфері забезпечення інформаційної безпеки, інформаційна ж безпека органів прокуратури залишається поза увагою. Тож **метою** статті є дослідження правових питань захисту прокуратури від впливу інформаційних технологій як загрози її інформаційній безпеці, а завданням – виокремлення проблем здійснення такого захисту та пошук оптимальних шляхів їх подолання.

Інформатизація, розвиток глобальної мережі Інтернет, застосування інформаційно-комп'ютерних технологій як «панацеї» для розвитку суспільства і держави, навпаки, тільки дезорієнтують суспільство. Інтернет та інформаційно-

комп'ютерні технології – це не тільки і не стільки засоби комунікації і новий вид зберігання, поширення та забезпечення широкого доступу до певної інформації. Це передусім активно діючі суб'єкти: індивіди та різні співтовариства (світові корпорації, держави, коаліції держав), що беруть участь у створенні, розвитку, забезпеченні функціонування і використання можливостей глобальної мережі як позитивних, так і негативних [4].

Справді, глобалізація, сучасний етап розвитку суспільства пов'язані з якісно новими інформаційними технологіями взаємодії з навколишнім світом та новими можливостями формування і коригування інформаційної атмосфери в суспільстві. Глобальні мережі, інформаційні технології – це засоби (інструментарій), що дозволяють більш активно й успішно вирішувати завдання. Ці засоби (інструментарій) можуть дати очікувані позитивні результати тільки за наявності розвиненої соціально-економічної та науково-технологічно-промислової бази й ефективних заходів щодо формування і використання в національних інтересах інформаційних ресурсів і знань. Тільки на основі широкого соціально-економічного і політико-правового розуміння глобалізаційних інформаційних процесів можна коректно ставити і вирішувати проблеми розроблення і впровадження методологічних основ системи інформаційної безпеки як важливої умови функціонування і прогресивного розвитку соціальної системи з додержанням балансу інтересів особистості, суспільства і держави [4].

На думку В. О. Шамрай, інформаційна безпека суспільства, держави характеризується ступенем їх захищеності та, як наслідок, стійкістю головних сфер життєдіяльності у відношенні до небезпечних інформаційних впливів. Інформаційна безпека визначається здатністю нейтралізувати такі впливи. Загальноприйнятим є таке визначення інформаційної безпеки, як стан захищеності життєво важливих інтересів громадян, суспільства та держави в інформаційній сфері [5].

Натомість О. В. Логінов та А. О. Рось зазначають, що інформаційна безпека не може розглядатися лише як окремий стан. Вона має враховувати майбутнє, отже, є не станом, а процесом [6]. Варто підтримати позицію, згідно з якою інформаційну безпеку слід розглядати через органічну єдність ознак, таких, як стан, властивість, а також управління загрозами і небезпеками, за допомогою якого забезпечується обрання оптимального шляху їх усунення і мінімізації впливу негативних наслідків. Одним із механізмів гарантування даного процесу є система органів прокуратури, яка ефективно функціонує і є суб'єктом та об'єктом забезпечення інформаційної безпеки одночасно.

Для вирішення проблем інформаційного забезпечення діяльності органів прокуратури України комп'ютерною службою Генеральної прокуратури розроблена і поступово впроваджується Концепція створення корпоративної інформаційної системи органів прокуратури України. Концепція реалізується в рамках національної програми інформатизації, при цьому враховується можливість інтеграції корпоративної інформаційно-обчислювальної мережі органів прокуратури України в загальну інформаційну систему правоохоронних органів України, а також інтеграцію в загальнодержавну інформаційно-обчислювальну мережу України [7].

Варто підтримати пропозицію щодо впровадження комплексної система захисту інформації від несанкціонованого доступу, що значно покращить діяльність інформаційно-аналітичних служб на всіх рівнях правоохоронної системи, зменшить дублювання численних форм державної і відомчої звітності, допоможе ефективно координувати та обмінювати інформацію між різними відомствами. До того ж, розроблення, узгодження та уточнення стандартів обміну інформацією між правоохоронними відомствами, сумісних зі стандартами, рекомендованими ООН та Радою Європи, сприятиме ефективності інформаційного забезпечення діяльності органів прокуратури [7].

Слід зауважити, що О. А. Баранов вважає не зовсім коректним твердження про зв'язок проблеми інформаційної безпеки тільки з інформатизацією. На його думку, існує два аспекти вивчення інформаційної безпеки в контексті національної безпеки. Це самостійний елемент національної безпеки будь-якої країни і водночас інтегрована складова будь-якої іншої безпеки: військової, економічної, політичної тощо. У цьому складність розгляду проблематики інформаційної безпеки. Часто предметом аналізу стає одна галузь, наприклад сфера масової інформації. Дослідник надає таке визначення інформаційної безпеки: «Під інформаційною безпекою слід розуміти такий стан захищеності життєво важливих інтересів особистості, суспільства і держави, при якому зводиться до мінімуму завдання збитку через неповноту, невчасність і недостовірність інформації, негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації» [1]. На переконання О. А. Баранова,

таке визначення тією чи іншою мірою охоплює практично всі сфери інформаційної взаємодії суб'єктів у суспільстві, державі й у всіх соціальних утвореннях. При цьому під інформаційною взаємодією він розуміє весь процес створення інформації, накопичення, опрацювання, збереження і поширення. Важливого значення набувають визначення понять інформаційного простору та інформаційної інфраструктури. Вони несуть, як і перший термін, методологічне навантаження з погляду побудови політики інформаційної безпеки держави [6].

А. В. Анісімов акцентує увагу на тому факті, що аспект одержання й аналізу інформації для забезпечення власної безпеки і прийняття адекватних рішень також слід включати до розгляду концепції інформаційної безпеки. Що ж до технологічного аспекту захисту інформації, то поняття інформаційної безпеки є старшим за поняття інформатики. Інформаційні технології активно застосовуються для вирішення завдань захисту інформації, але існує також дуже сильний зворотний зв'язок – від проблем захисту інформації до розвитку нових інформаційних технологій. Цей зв'язок не завжди видно, проте вплив його незаперечний [6].

О. Г. Додонов доречно зауважує, що інформаційна безпека – це стан захищеності. Учений зазначає: «Можна також сказати, що це є властивістю системи мінімізувати інформаційні загрози. При розгляді проблеми інформаційної безпеки слід спочатку говорити про загрози і вже потому – про захищеність від цих загроз. Первинною є саме інформаційна загроза. Для окремої особистості існують одні інформаційні загрози, для суспільства – інші, для держави – ще інші. І якщо говорити про інформаційну безпеку як про властивість мінімізувати загрози для певних об'єктів і суб'єктів інформаційної діяльності, то це вбачається правильним. Використовуючи такий підхід, можна розглядати не загальнометодологічні питання інформаційної безпеки, а різні рівні інформаційної взаємодії, інформаційних відносин, виділити методологічні і теоретичні проблеми інформаційної безпеки, які необхідно вирішувати. А тоді вже можна шукати засоби, методи протидії інформаційним загрозам, закладати ці методи у відповідні інформаційні системи для адекватного реагування на загрози» [6].

На сучасному етапі основними реальними та потенційними загрозами інформаційній безпеці прокуратури можна назвати:

– несанкціонований доступ до інформаційних ресурсів прокуратури, зокрема: розкриття інформаційних ресурсів; порушення цілісності інформаційних ресурсів; збій у роботі обладнання тощо;

– негативні інформаційні впливи з використанням засобів масової інформації, а також мережі Інтернет, спрямовані на підрив авторитету органів прокуратури;

– розголошення інформації, яка становить державну та іншу передбачену законодавством таємницю, а також конфіденційної інформації, що є власністю держави.

Найбільшу небезпеку становить несанкціонований доступ до інформаційних ресурсів. Зокрема, загроза розкриття інформаційних ресурсів прокуратури полягає в тому, що інформація стає відомою необмеженій кількості осіб. Це можуть бути як відкриті ресурси, так і ресурси з обмеженим доступом. Дані ресурси мають передаватися один одному і зберігаються в єдиній інформаційній системі.

Загроза порушення цілісності інформаційних ресурсів прокуратури полягає в умисному впливі (модифікація, видалення, зниження) даних, які зберігаються в інформаційній системі органів прокуратури, а також передаються від даної інформаційної системи до інших. Систему органів прокуратури становлять: Генеральна прокуратура України, прокуратури Автономної Республіки Крим, областей, міст Київ і Севастополь (на правах обласних), Дніпровська екологічна прокуратура (на правах обласної), регіональні військові прокуратури, міські, районні, міжрайонні, районні в містах, і якщо на рівні Генеральної прокуратури та прокуратур обласного значення така єдність є організованою, то зв'язки районних, міжрайонних, районних в містах залишаються не налагодженими на відповідному рівні.

Загроза збою в роботі самого обладнання може виникнути при блокуванні доступу до одного або декількох ресурсів інформаційної системи. Насправді блокування може бути постійним, коли ресурс, що запитується, не може бути отриманим або виникають затримки в його отриманні, що є достатнім для того, щоб він став некорисним.

Найбільш частими і небезпечними є ненавмисні помилки користувачів, операторів, системних адміністраторів та інших осіб, що обслуговують інформаційні системи. Іноді такі помилки є загрозами (неправильно введені дані, помилки в програмі, котрі викликають колапс системи), іноді вони створюють ситуації, якими можуть скористатися зловмисники. Як свідчать фахівці, понад 65 % шкоди, що завдається інформаційним ресурсам, – наслідки ненавмисних помилок [8, с. 274].

Наступними за розміром шкоди можна назвати фальсифікації (пошкодження обладнання; вбудовування логічної бомби, яка з часом руйнує програми і дані; введення неправильних даних; знищення даних; зміну даних; модифікацію даних; надання доступу до даних із обмеженим доступом тощо). У більшості випадків суб'єктами вчинення даних дій є штатні працівники структурних підрозділів органів прокуратури, які добре обізнані з роботою інформаційної системи, а також заходів безпеки. Це можуть бути співробітники, які незадоволені або не поділяють цінностей правоохоронної діяльності.

Невдоволені своїм становищем співробітники створюють реальну загрозу інформаційній безпеці прокуратури. Необхідно слідкувати за тим, щоб при звільненні співробітника його права доступу до інформаційних ресурсів були повністю обмежені, а після його звільнення змінені всі паролі доступу до внутрішньої мережі. Більш того, слід обмежити його спілкування з особами, що мають доступ до важливої інформації.

Серйозною загрозою можуть бути програмні віруси. Водночас дотримання правил користування комп'ютерною технікою, а також наявність у штаті співробітників органів прокуратури відповідного фахівця з даних питань значно полегшить вирішення зазначених завдань.

У той же час загрози інформаційній безпеці, з одного боку, є організаційним компонентом системи органів прокуратури, а з іншого – індикатором ефективності її функціонування, адже реалізація загроз і переростання їх у небезпеки свідчить про неефективність функціонування даної системи і навпаки. На сьогодні розглядати будь-які загрози в інформаційній сфері необхідно з урахуванням того контексту, в якому вони виникають і знаходять свій прояв. У той же час на державному рівні з метою забезпечення інформаційної безпеки прокуратури необхідно частіше залучати засоби масової інформації до забезпечення неухильного додержання конституційних прав і свобод людини і громадянина, захисту конституційного устрою, вдосконалення системи політичної влади з метою зміцнення демократії, духовних та моральних засад суспільства; підвищення ефективності функціонування правоохоронних органів.

Вчасним має бути також розвиток національної інформаційної інфраструктури на засадах стимулювання вітчизняних виробників і користувачів новітніми інформаційно-телекомунікаційними засобами і технологіями, комп'ютерними системами і мережами.

Список використаної літератури

1. Баранов А. Информационный суверенитет или информационная безопасность? / А. Баранов // Національна безпека і оборона. – 2001. – № 1. – С. 70–76.

2. Биченок М. М. Основи інформатизації управління регіональною безпекою / М. М. Биченок. – К. : ПоліграфКонсалтинг, 2005. – 196 с.

3. Е-боротьба в інформаційних війнах та інформаційне право : [монографія] / В. М. Брижко, М. Я. Швець, В. С. Цимбалюк. – К. : Акад. прав. наук України, 2007. – 233 с.

4. Олійник О. В. До питання формування системи інформаційної безпеки України [Електронний ресурс] / О. В. Олійник // Наукові записки інституту законодавства Верховної Ради України. – 2011. – Вип. 3 (6). – Режим доступу: http://www.nbuv.gov.ua/portal/Soc_Gum/Nzizvru/2011_3/index.html.

5. Шамрай В. О. Інформаційна безпека як складова національної безпеки України [Електронний ресурс] / В. О. Шамрай. – Режим доступу: http://www.crime-research.ru/library/Shamray.htm.

6. Інформаційна безпека України: сутність та проблеми [Електронний ресурс] : матеріали круглого столу. – Режим доступу: http://old.niss.gov.ua/book/panorama/kr_stil.htm.

7. Інформаційні системи і технології в юридичній діяльності [Електронний ресурс]. – Режим доступу: http://ubooks.com.ua/books/000166/inx44.php.

8. Ярочкин В. И. Информационная безопасность : учеб. для студ. вузов, обуч. по гуманит. и соц.-экон. спец. / В. И. Ярочкин. – М. : Мир, 2003. – 640 с.

Надійшла до редколегії 25.05.2012

ХОМИЧ А. С. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ КАК УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОКУРАТУРЫ

Выполнено исследование правовых вопросов защиты прокуратуры от воздействия информационных технологий как угрозы её информационной безопасности, осуществленное на основании анализа соответствующих нормативно-правовых актов и взглядов ученых.

KHOMYCH A. INFORMATION TECHNOLOGIES AS A THREAT OF INFORMATIVE SAFETY OF PUBLIC PROSECUTOR

Research of legal questions of protection of prosecutor's office from influence of information technologies as threat of its informative safety, carried out on the basis of the analysis of the relevant normative and legal acts and views of scientists is made.