6. Новини ТСН [Електронний ресурс]. – Режим доступу: http://tsn.ua/ukrayina/shahray-zder-z...

7. Теорія держави і права: навчальний посібник – Ведєрніков Ю.А., Папірна А.В. [Електронний ресурс]. – Режим доступу: http://pidruchniki.com/16400116/pravo...

МАЗУРИК С. В.,
аспірант кафедри конституційного,
адміністративного та фінансового права
*(Тернопільський національний
економічний університет)*

УДК 347.963

ІНФОРМАЦІЙНА БЕЗПЕКА ОРГАНІВ ПРОКУРАТУРИ

У статті автором проаналізовано поняття, сутність та зміст інформаційної безпеки в органах прокуратури України. Автор виокремив правові та технічні засоби забезпечення інформаційної безпеки в органах прокуратури та проаналізував інфраструктуру сучасної інформаційної безпеки прокуратури. За результатами дослідження стану нормативно-правового регулювання безпеки в органах прокуратури автор запропонував виокремити інформаційну безпеку в самостійний напрям прокурорської діяльності.

Ключові слова: *органи прокуратури, інформаційна безпека, загрози інформаційної безпеки, інформаційна інфраструктура, персональні дані, засоби захисту інформації.*

В статье автором проанализированы понятие, сущность и содержание информационной безопасности в органах прокуратуры Украины. Автор выделил правовые и технические средства обеспечения информационной безопасности в органах прокуратуры и проанализировал инфраструктуру современной информационной безопасности прокуратуры. По результатам исследования состояния нормативно-правового регулирования безопасности в органах прокуратуры автор предложил выделить информационную безопасность в самостоятельное направление прокурорской деятельности.

Ключевые слова: *органы прокуратуры, информационная безопасность, угрозы информационной безопасности, информационная инфраструктура, персональные данные, средства защиты информации.*

In the article author researches the concept and content of information security in the Prosecutor's Office of Ukraine. The author defines the legal and technical means of information security of the prosecution and reviews the infrastructure of modern information security prosecutor. The author proposes to distinguish information security in a separate area of prosecution.

Key words: *prosecution, security of information, threats to information security, information infrastructure, personal data protection information.*

Вступ. У зв'язку із прогресивними змінами суспільного життя, пов'язаними із масовим використанням інформаційних технологій під час обробки, зберігання інформації та обміну нею, проблеми інформаційної безпеки виходять на перший план у всіх сферах державно-правового життя. Наприклад, сьогодні на отримання відомостей необхідно у декілька разів менше часу, ніж десять років тому назад. Електронізація інформаційної діяльності, з одного боку, суттєво полегшує реалізацію державно-владних повноважень, а з іншого – може завдати непоправної шкоди інформаційному середовищу публічного адміністрування. З урахуванням цього основне завдання органів державної влади як повноцінних суб'єктів інформаційних відносин проявляється не тільки в усуненні інформаційних загроз, а й у виробленні концепції інформаційної безпеки, метою якої є управління ризиками, що можуть мати місце у процесі інформаційної діяльності.

Інформаційна складова в роботі органів прокуратури насамперед забезпечує прийняття раціональних, правильних та своєчасних управлінських рішень у сфері захисту прав та свобод людини, підтримання державного обвинувачення в суді тощо. А інформаційний простір охоплює діяльність суб'єктів прокуратури на всіх рівнях у відносинах, які виникають при реалізації ними своїх повноважень. Створення правових механізмів захищеності інформаційного простору є першим кроком на шляху до забезпечення безпеки в органах прокуратури.

Загалом питання інформаційної безпеки не є новим для правової доктрини. У системі інформаційного права слід виокремити комплексні праці І.В. Арістової, Ю.П. Бурило, Б.А. Кормича, А.М. Новицького, Ю.Є. Максименко, О.В. Логінова, А.І. Марущака, Т.А. Костецької, О.Г. Марцелюка тощо, які заклали підґрунтя для подальшого дослідження окремих питань інформаційної безпеки.

Постановка проблеми. Концептуально-правові та теоретико-методологічні засади забезпечення безпеки інформаційних відносин в органах прокуратури не були розкриті. До того ж ведення відкритої інформаційної війни проти України вимагає особливої уваги до вироблення стратегії політики інформаційної безпеки, в якій прокуратура повинна зайняти стрижневу позицію щодо захисту прав, свобод, інтересів громадян та держави. Слід наголосити, що із активізацією процесів інформатизації дослідження інформаційної безпеки в органах прокуратури в Україні є не тільки актуальною, а й перспективною темою наукового пізнання. З урахуванням цього метою статті є вивчення феномену інформаційної безпеки органів прокуратури України в практичному та теоретико-правовому аспекті, а також внесення пропозицій щодо удосконалення її концепції.

Результати дослідження. Витоки інституційних досліджень з інформаційної безпеки як самостійного явища знайшли своє місце в політико-правовій системі завдяки поглибленому гносеологічному вивченню феномену безпеки в цілому, його диференціації на окремі інститути. Необхідність виокремлення та утвердження безпеки у відносинах, предметом яких є інформація, як самостійної ніші з'явилася у зв'язку із цілковитою інтеграцією суб'єктів у інформаційне середовище, набуттям власних інформаційних цінностей, потреб та інтересів. Сьогодні вони є учасниками вже не тільки культурних, політичних, правових, економічних відносин, а й одночасно – інформаційних.

Не секрет, що термін «інформаційна безпека» випливає із категорії «безпека» і в найзагальнішому розумінні означає такий стан, при якому забезпечено захищеність різноманітних систем та процесів обробки, зберігання, передачі відомостей, а також їх конфіденційність (таємність), повноту [2].

У науково-правовій літературі поняття інформаційної безпеки визначалося досить по-різному. Наприклад, на думку Б.А. Кормича, інформаційна безпека являє собою стан захищеності встановлених законодавством норм та параметрів інформаційних процесів та відносин, що забезпечує необхідні умови існування держави, людини та суспільства як суб'єктів цих процесів та відносин [3, с. 34]. Ю.Є. Максименко зазначає, що інформаційна безпека – це результат управління реальними чи (та) потенційними загрозами (небезпеками) з метою задоволення національних інтересів людини, суспільства та держави в інформаційній сфері [5, с. 16]. Я. Малий вважає, що інформаційна безпека означає законодавче

формування державної інформаційної політики, створення відповідно до законів України можливостей досягнення інформаційної достатності для ухвалення рішень органами державної влади, громадянами, гарантування свободи інформаційної діяльності та права доступу до інформації у національному інформаційному просторі України, всебічний розвиток інформаційної структури, підтримку розвитку національних інформаційних ресурсів України, створення і впровадження безпечних інформаційних технологій тощо [6, с. 13]. Із усіма проаналізованими термінами цілком можна погодитися, лише слід зауважити, що автори визначають сутність інформаційної безпеки, виходячи із предмету її функціонування у тій чи іншій сфері публічно-правового життя. А тому у випадку, якщо мова йтиме про висвітлення інформаційної безпеки як елемента національної безпеки, доцільно вдаватись до широкого змісту, а якщо «інформаційна безпека» звучить у контексті діяльності певних суб'єктів, то доцільно використати звужене поняття. Отже, виходячи із того, що забезпечення інформаційної безпеки є однією із функцій прокуратури, вона являє собою систему дій, рішень, методів, процесів у формі правових, технологічних, аналітичних заходів, спрямованих на вироблення механізму виявлення, оцінки, прогнозування та ліквідації загроз в інформаційному середовищі органів прокуратури України на всіх етапах та циклах створення, обробки, зберігання та поширення інформації у процесі здійснення прокурорської діяльності.

Частково питання правового регулювання забезпечення інформаційної безпеки в органах прокуратури України здійснюється: Законами України «Про прокуратуру», «Про інформацію», «Про захист персональних даних», «Про основи національної безпеки», «Про державну таємницю», «Про доступ до публічної інформації», «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних», Типовим порядком обробки персональних даних, затвердженим наказом Уповноваженого Верховної Ради України з прав людини від 8 січня 2014 р. № 1/02-14, Порядком обробки персональних даних працівників органів прокуратури у базі персональних даних «Кадри органів прокуратури України», затвердженим наказом Генерального прокурора України від 26 липня 2014 р. № 77, Наказом Генерального прокурора України № 69 від 17 серпня 2012 р. «Про порядок ведення Єдиного реєстру досудових розслідувань», Наказом Генерального прокурора України від 23 червня 2016 р. № 216 «Про порядок надсилання документів електронною поштою та факсимільним зв'язком», Наказом Генерального прокурора України від 24 лютого 2016 р. «Про затвердження Інструкції з діловодства в органах прокуратури України». Проте місце захисту інформаційної діяльності та середовища в системі функцій прокуратури цілком очевидно випливає із Наказу Генерального прокурора «Про організацію роботи з питань внутрішньої безпеки в органах прокуратури України» від 22 вересня 2014 р. № 17 гн. Зокрема, одним із елементів концепції внутрішньої безпеки зазначено інформаційну безпеку, правові заходи забезпечення якої містять:

1) закріплення за прокурором обласного рівня обов'язку запобігання витоку мовної та видової інформації на об'єктах інформаційної діяльності органів прокуратури, втраті таємних документів тощо;

2) з метою проведення перевірок забезпечення посадовим особам управління внутрішньої безпеки органів прокуратури безперешкодного доступу до службових комп'ютерів та електронних носіїв інформації, інформаційних баз даних тощо;

3) здійснення невідкладних інформаційно-публічних та дисциплінарних заходів за результатами вчинення ганебних вчинків та інших резонансних події за участю працівників прокуратури, своєчасне реагування на публікації такого змісту [9].

Закон України «Про основи національної безпеки України» від 19 червня 2003 р. № 964-IV у ст. 7 наводить перелік загроз, зокрема в інформаційній сфері, які можуть становити суттєву загрозу національній безпеці держави. В одному із пунктів міститься положення про небезпеку розголошення інформації, яка становить державну таємницю, або іншої інформації з обмеженим доступом, спрямованої на задоволення потреб і забезпечення захисту національних інтересів суспільства і держави [11].

Виходячи із того, що у своїй службовій діяльності органи прокуратури оперують службовою та таємною інформацією, отриманою у ході досудового розслідування, судового

процесу, можна говорити, що вони разом із іншими правоохоронними органами являються стратегічним суб'єктом забезпечення не тільки інформаційної, а й національної безпеки в масштабах держави. Існування систем захисту інформації із обмеженим доступом цілком закономірно породжує специфічний статус працівників прокуратури (зокрема накладає на них певні обтяження), що пов'язано із забезпеченням режиму секретності.

Загалом, найбільш широко загрози інформаційним ресурсам системи органів прокуратури можна розглядати як потенційно можливі випадки природного, технічного або антропогенного характеру, які можуть спричинити небажаний вплив на інформаційну систему, а також на інформацію, що зберігається в ній [4, с. 98].

До інших загроз інформаційної безпеки в органах прокуратури слід віднести:

1) незаконне проникнення в інформаційне середовище системи органів прокуратури (хакерство);

2) діяльність громадян, установ, організацій у вигляді цілеспрямованих акцій, спрямованих на підрив ділової репутації, авторитету органів прокуратури у суспільстві, поширення неправдивих відомостей про діяльність прокурорів;

3) несанкціонований витік інформації про хід або результати прокурорської діяльності, зокрема у потоках міжвідомчих інформаційно-аналітичних систем;

4) дезорганізацію або пошкодження зведених інформаційних масивів, автоматизованих робочих місць, збої в їх роботі;

5) ризик інформаційного терору (можливості організованих злочинних угрупувань, використовуючи власні технічні можливості або ресурси інших установ, здобувати конфіденційну або таємну інформацію, змінювати, підроблювати чи використовувати її у власних інтересах) [1, с. 16];

6) низькій рівень зворотного зв'язку, неналагодженість комунікації із органами державної влади, підприємствами, установами, організаціями, тощо.

Слід погодитися із позицією О.В. Логінова, що загрози інформаційній безпеці, з одного боку, є організаційним компонентом системи органів виконавчої влади, а з іншого – слугують індикатором ефективності її функціонування [4, с. 90]. Незважаючи на те що до певної міри загрози властиві всій системі прокуратури, їх рівень все ж коливається в залежності від зовнішніх та внутрішніх чинників, урахування яких може суттєво зменшити ризик виникнення самих загроз.

Метою заходів інформаційної безпеки є забезпечення безперебійного функціонування, розміщення, обміну та захисту інформації, а також безпека використання інформаційних баз даних.

Наступним питанням, яке потребує з'ясування, є зміст інформації, що потребує захисту в органах прокуратури України. У цьому випадку мова йтиме не просто про види такої інформації. У комплексному аспекті необхідно говорити про інформаційну інфраструктуру, яка може стати об'єктом інформаційних загроз. На наш погляд, внутрішню сторону інформаційної інфраструктури охоплюють персональні дані та службова інформація з обмеженим доступом.

Здебільшого об'єктом інформаційної діяльності органів прокуратури є персональні дані, які згідно із Законом України «Про захист персональних даних» від 1 червня 2010 р. № 2297-VI можуть бути віднесені до конфіденційної інформації, незаконне розголошення якої карається законом. Механізм захисту персональних даних в органах прокуратури містить два складники. По-перше, захист відомостей про осіб, що фігурують у процесуальних актах-документах, управлінських рішеннях, зведених інтегрованих інформаційних масивах. Наприклад, такі відомості можуть зберігатися в інформаційній (автоматизованій) системі «Єдиний реєстр досудових розслідувань» (далі – ЄРДР), адміністратором якого є, власне, Генеральна прокуратура України. Згідно із Наказом Генерального прокурора України «Про затвердження Порядків обробки персональних даних в органах прокуратури України» від 26 липня 2014 р. № 77 кожен працівник прокуратури дає підписку про зобов'язання не допускати розголошення у будь-який спосіб персональних даних, зокрема відомостей із ЄРДР, які йому довірені або стали відомі у зв'язку із виконанням службових обов'язків [8].

На відміну від персональних даних, які можуть міститися в деяких управлінських рішеннях, в ЄРДР такі відомості централізовані та структуровані. З метою протидії перевищенням службових повноважень працівниками прокуратури адміністрування відомостей, їх перегляд надається лише прокурору відповідного рівня [12].

Більше того, Порядком ведення Єдиного реєстру досудових розслідувань передбачено комплекс програмних, технологічних та організаційних заходів щодо захисту відомостей, що містяться в ЄРДР, від несанкціонованого доступу [12].

По-друге, безпека персональної інформації про співробітників прокуратури. Загалом обробка персональних даних здійснюється виключно з метою забезпечення реалізації визначених законодавством прав і обов'язків у сфері трудових правовідносин та соціального захисту громадян, підготовки органами прокуратури організаційно-розпорядчих документів з питань, пов'язаних із трудовими відносинами, отримання статистичної, адміністративної та іншої інформації щодо персоналу, а також ведення кадрового діловодства [7].

Інформацію з обмеженим доступом можна умовно класифікувати на конфіденційну, таємну, службову та професійну таємницю. Така інформація є основним об'єктом прокурорської діяльності та може виражатися у різних нормативних актах-документах, рішеннях, приписах, вказівках.

Зовнішню сторону інфраструктури інформаційного середовища, що є елементом системи захисту, утворюють, наприклад, відомості зі ЗМІ про публічну діяльність органів прокуратури або інформація на офіційному сайті Генеральної прокуратури України (http://www.gp.gov.ua/).

Вплив інформаційної загрози у деяких випадках може мати катастрофічні наслідки на функціонування органів прокуратури у цілому.

В інформаційній діяльності органів прокуратури загрозу стабільності, цілісності інформаційних ресурсів можуть становити інформаційні небезпеки технічного походження: по-перше, блокування доступу до кількох або одного ресурсів інформаційної системи спричиняє короткострокові або довгострокові збої в роботі з інформацією; по-друге, технічні (навмисні або ненавмисні) помилки користувачів, операторів, системних адміністраторів; по-третє, фальсифікації у формі пошкодження обладнання, введення неправильних даних, модифікація даних, несанкціоноване надання доступу до даних із обмеженим доступом [14, с. 149–150].

Необхідність подолання інформаційних загроз потребує, окрім правових засобів, використання сучасних технічних засобів захисту інформації. Їх поява супроводжується розвитком масової персональної комп'ютеризації та переходом на електронну форму інформаційної роботи за допомогою електронно-обчислювального забезпечення.

У навчальному посібнику О.В. Рибальського, В.Г. Хахановського та В.А. Кудінова наводиться перелік видів технічного захисту інформації, які зазвичай використовують в органах внутрішніх справ: захист акустичної інформації від зняття радіозакладними пристроями; захист інформації від витоку по технічних каналах, утворених допоміжними технічними засобами; захист інформації від несанкціонованого запису звукозаписувальними пристроями; захист електронної інформації; захист письмової інформації від оптичного зняття [13]. Органи прокуратури не є винятком із цього. Разом із цим, слід виокремити такі засоби технічного захисту інформації в системі інформатизації та електронізації в органах прокуратури, як:

– блокування пристроїв та інтерфейсів вводу-виводу інформації [7];
– електронний цифровий підпис;
– корпоративізація інформаційно-обчислювальної мережі;
– ідентифікація та аутентифікація доступу в персональний акаунт;
– антивірусне програмне забезпечення тощо.

Висновки. Отже, з огляду на підвищений рівень загроз та небезпек у щоденній діяльності працівників прокуратури парадигма інформаційної захищеності повинна трансформуватися у самостійний напрям та функцію органів прокуратури із гармонійним поєднанням

правового та технічного сегменту. Для цього необхідно розробити концепцію інформаційної безпеки. З урахуванням ієрархічної структури рекомендується визначити повноваження кожного прокурора із здійснення заходів щодо забезпечення інформаційної безпеки. Високий рівень захищеності у роботі із масовими інформаційними потоками вимагає мінімізації технічних збоїв, що можливо досягти потужним та сучасним програмним забезпеченням. Не менш важливим залишається усвідомлення прокурорами своєї значущості в якості суб'єктів інформаційного права – елементів національної безпеки.

Список використаних джерел:

1. Камышев Э.Н. Информационная безопасность и защита информации: Учебное пособие. – Томск: ТПУ, 2009. – 95 с.

2. Князев А.А. Информационная война // Энциклопедический словарь СМИ. – Бишкек: Издательство КРСУ, 2002.

3. Кормич Б.А. Організаційно-правові основи політики інформаційної безпеки України : автореф дис. … докт. юрид. наук за спеціальністю 12.00.07. – Національний університет внутрішніх справ МВС України. – Харків, 2004. – 41 с.

4. Логінов О.В. Адміністративно-правове забезпечення інформаційної безпеки органів виконавчої влади: дис. … канд. юрид. наук за спеціальністю 12.00.07. – Національна академія внутрішніх справ України. – Київ, 2005. – 236 с.

5. Максименко Ю.Є. Теоретико-правові засади забезпечення інформаційної безпеки України: автореф. дис. … канд.. юрид. наук за спеціальністю 12.00.01. – Київський національний університет внутрішніх справ. – Київ, 2007. – 22 с.

6. Малий Я. Інформаційна безпека України: стан та перспективи розвитку / Я. Малий // Збірник наукових праць. – 2015. – Вип. № 44 Ефективність державного управління. – С. 13–20.

7. Надання послуг в області технічного захисту інформації [текст]. – [Електронний ресурс]. – Режим доступу : http://www.ulyssys.com/i/lng.ua/page.security.

8. Порядок обробки персональних даних працівників органів прокуратури у базі персональних даних «Кадри органів прокуратури України» : затв. Наказом Генерального прокурора України від 26 липня 2014 р. №77.

9. Про затвердження Порядків обробки персональних даних в органах прокуратури України : Наказ Генерального прокуратура України від 26 липня 2014 р. № 77. – Електронний ресурс. – режим доступу : http://www.gp.gov.ua/ua/personal_data_protection.

10. Про організацію роботи з питань внутрішньої безпеки в органах прокуратури України : Наказ Генерального прокурора України від 22 вересня 2014 р. № 17 гн.

11. Про основи національної безпеки України : Закон України від 19 червня 2003 р. № 964-IV // Відомості Верховної Ради України (ВВР). – 2003. – № 39. – ст. 351.

12. Про порядок ведення Єдиного реєстру досудових розслідувань : Наказ Генерального прокурора України № 69 від 17 серпня 2012 р. – Електронний ресурс. – [режим доступу] : http://lug.gp.gov.ua/ua/lugpes.html?_m=publications&_t=cat&id=114099.

13. Рибальський О.В., Хахановський В.Г., Кудінов В.А. Основи інформаційної безпеки та технічного захисту інформації. Посібник для курсантів ВНЗ МВС України. – К.: Вид. Національної академії внутріш. справ, 2012. – 104 с.

14. Хомич А.С. Інформаційні технології як загроза інформаційній безпеці прокуратури // Право і безпека. – 2012. – № 3. – 147–150.