УДК 342.951

ІНФОРМАЦІЙНА БЕЗПЕКА ОРГАНІВ ПРОКУРАТУРИ: ПИТАННЯ ОРГАНІЗАЦІЙНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ

Терещук Г.А., *кандидат юридичних наук, доцент Тернопільського національного економічного університету;* **Мазурик С.В.,** *прокурор Київської місцевої прокуратури № 6*

H. Tereshchuk, S. Mazuryk INFORMATION SECURITY OF THE PROSECUTOR'S OFFICE: QUESTION OF ORGANIZATIONAL AND LEGAL SUPPORT

Анотація. *У статті авторами проаналізовано поняття, сутність та зміст інформаційної безпеки в органах прокуратури України. Автори виокремили правові та технічні засоби забезпечення інформаційної безпеки в органах прокуратури та проаналізували інфраструктуру сучасної інформаційної безпеки прокуратури. За результатами дослідження стану нормативно-правового регулювання безпеки в органах прокуратури, автори запропонували виокремити інформаційну безпеку в самостійний напрямок прокурорської діяльності.*

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

Annotation*: In the article authors research the concept and content of information security in the Prosecutor's Office of Ukraine. The authors define the legal and technical means of information security of the prosecution and reviews the infrastructure of modern information security prosecutor. The authors propose to distinguish information security in a separate area of prosecution.*

The purpose of this article is the disclosure of the main provisions of the organizational and legal provision of information security of the prosecutor's offices of Ukraine, as well as the formation of proposals to improve legislation and practice in this area.

In formulating our own opinion about the threats to information security in the prosecutor's office, we note that we have identified the following categories of them, the factors: the rapid progress of information technologies, which can be used for unlawful influence on the information resources of the prosecutor's office. The relevant structural units that provide information support and support are not always able to have up-to-date information on innovations, as well as to develop countermeasures aimed at ensuring the functioning of the prosecutor's office; insolvency of prosecutors who, in some cases, abuse their authority to work with information, which leads to its distortion, incompleteness, unauthorized leakage, etc; lack of a clear information and organizational structure of special units of information work, crawled with the existence of independent information authority of individual units prosecutors, which leads to poor-quality information cooperation, information exchange; information sabotage related to the potential for interference with the operation of internal information systems, networks, which may lead to theft of information, as well as its use to counter prosecutors in carrying out their functions and their tasks.

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

Актуальність теми. 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 в процесі інформаційної діяльності. Інформаційна складова в роботі органів прокуратури, у першу чергу, 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 являється першим кроком на шляху до забезпечення безпеки в органах прокуратури.

У системі інформаційного права слід виокремити комплексні праці з питань інформаційної безпеки І.В. Арістової, Ю.П. Бурило, І. Р. Березовської, 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.

Метою цієї статті є розкриття основних положень організаційного та правового забезпечення інформаційної безпеки органів прокуратури України, а також формування пропозицій щодо удосконалення законодавства та практики в цій сфері.

Необхідність виокремлення та утвердження безпеки у відносинах, предметом яких є інформація, як самостійної ніші з'явилася у зв'язку з цілковитою інтеграцією суб'єктів в інформаційне середовище, набуттям власних інформаційних цінностей, потреб та інтересів. Сьогодні вони виступають вже не тільки як учасники культурних, політичних, правових, економічних, а й одночасно інформаційних відносин. На підтвердження цього, відзначимо позицію І. Р. Березовської, яка зазначає, що сучасний механізм забезпечення інформаційної безпеки держави реалізовується через застосування органами виконавчої влади таких адміністративно-правових засобів: 1) дозвільних засобів, які включають дозвіл на провадження діяльності, пов'язаної з державною таємницею, стандартизацію заходів забезпечення інформаційної безпеки, ліцензування та легалізацію. Крім того, нами виділені фізичні, апаратні, програмні, організаційні, законодавчі та морально-етичні засоби, які становлять основу механізмів застосування дозвільних засобів забезпечення інформаційної безпеки; 2) реєстраційних засобів, які найперше включають реєстрацію засобів масової інформації та державну реєстрацію персональних баз даних; 3) засобів адміністративно-правового примусу, до яких слід, насамперед, віднести засоби адміністративної відповідальності [1, с. 191]. Натомість, забезпечення інформаційної безпеки, може розглядатись як самостійне організаційно-правове явище, діяльність, що повзується не тільки з адміністративно-правовими засобами, але й іншими. Слід також вказати, що інформаційна безпека та засоби її забезпечення є самостійними комплексними категоріями, які врегульовані інформаційно-правовими нормами, з урахуванням специфіки функціонування органу публічної адміністрації, де такі заходи застосовуються.

Інформаційною безпекою Д.О. Красіков називає стан захищеності прав та інтересів держави, суспільства, окремих фізичних та юридичних осіб (їх об'єднань), які стосуються порядку збирання, обробки, зберігання розповсюдження та доступу до інформації. При цьому інформаційна безпека є однією із складових частин національної безпеки України і співвідноситься з нею як частина і ціле [2, с.173]. Остання теза зумовлює звернення до Закону України «Про основи національної безпеки України, який передбачає такі основні напрями державної політики з питань національної безпеки в інформаційній сфері:забезпечення інформаційного суверенітету України; вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну; активне залучення засобів масової інформації до запобігання і протидії корупції, зловживанням службовим становищем, іншим явищам, які загрожують національній безпеці України; забезпечення неухильного дотримання конституційних прав на свободу слова, доступ до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації та журналістів, заборони цензури, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції, за виконання професійних обов'язків, за критику; вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України [3].

Серед інших нормативних джерел, які визначають поняття інформаційної безпеки, необхідно згадати положення Закон України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» у якому, остання визначається

як стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Вирішення проблеми інформаційної безпеки має здійснюватися шляхом: створення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її критичних елементів; підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їх наслідків, здійснення міжнародного співробітництва з цих питань; вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії комп'ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері; розгортання та розвитку Національної системи конфіденційного зв'язку як сучасної захищеної транспортної основи, здатної інтегрувати територіально розподілені інформаційні системи, в яких обробляється конфіденційна інформація [4].

Отже, виходячи із того, що забезпечення інформаційної безпеки є однією з внутрішньоорганізаціних (управлінських) 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 в 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 08.01.2014 №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 року №77, Наказом Генерального прокурора України № 69 від 17.08.2012 «Про порядок ведення Єдиного реєстру досудових розслідувань», Наказом Генерального прокурора України від 23.06.2016 № 216 «Про порядок надсилання документів електронною поштою та факсимільним зв’язком», Наказом Генерального прокурора України від 24.02.2016 «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» 22.09.2014 року № 17 гн.

Зокрема, одним із елементів концепції внутрішньої безпеки зазначено інформаційну безпеку, правові заходи забезпечення якої включають:

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

2) з метою проведення перевірок забезпечувати посадовим особам управління внутрішньої безпеки органів прокуратури безперешкодний доступ 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 своєчасно реагувати на публікації такого змісту [5]. На додачу до цього, в Генеральній прокуратурі України утворено Генеральну інспекцію, головним призначенням якої є формування повноцінного режиму дотримання законності в діяльності самої системи органів прокуратури, шляхом проведення комплексу заходів щодо запобігання та припинення кримінальних правопорушень, вчинених прокурорам, а також здійснення нагляду за додержанням законів під час проведення оперативно-розшукової діяльності, досудового розслідування стосовно прокурорів та працівників органів прокуратури (крім випадків, віднесених до компетенції Спеціалізованої антикорупційної прокуратури, та випадків, передбачених законом) тощо. Одним із завдань цієї Інспекції є забезпечення дотримання інформаційної безпеки в Генеральній прокуратурі України [6], яке реалізується через виконання таких функцій відділом забезпечення дотримання інформаційної безпеки в Генеральній прокуратурі України: здійснення статистичної та аналітичної обробки інформації, яка стосується діяльності Генеральної інспекції; проведення навчання для працівників прокуратури, органів прокуратури та закладів, установ, що входять до сфери управління органів прокуратури, щодо питань захисту викривачів; контроль за рівнем захисту інформації, яка обробляється Генеральною інспекцією; контроль за дотриманням ІТ безпеки Генеральною інспекцією; розробка і впровадження заходів щодо вдосконалення сфери захисту інформації, в тому числі ІТ безпеки; технічна підтримка, обслуговування захищеної комп'ютерної мережі та серверів Генеральної інспекції [6].

Серед іншого, захист інформації в системі прокуратури покладається на спеціально утворений Департамент інформаційних технологій, документального та матеріально-технічного забезпечення Генеральної прокуратури України. У структурі цього департаменту існує відділ адміністрування мереж та технічного захисту інформації, одним із завдань якого є антивірусний захист комп’ютерної техніки, а також технічний захист інформації в інформаційно-телекомунікаційних системах та в автоматизованих системах на об’єктах інформаційної діяльності Генеральної прокуратури України [7]. Однак існування у кожному департаменті або управлінні власного відділу інформаційно-технологічного супроводження, скоріше формує певні проблеми у взаємодії різних підрозділів прокуратури, які намагаються створити та забезпечити безпеку саме окремо взятого структурного підрозділу, що в результаті призводить до проблем інформаційного обміну, незнання реальної картини подій в інших структурних підрозділах, створення інформаційних бар’єрів тощо. Звичайно, володіння та користування специфічною інформацією передбачає необхідність її убезпечення, але ця діяльність повинна злиднюватись на загальноприйнятих засадах, встановлених правилах. Отже, на нашу думку, циркуляція інформації та питання інформаційної безпеки повинна бути закріплена на рівні окремого Регламенту інформаційної діяльності в органах прокуратури, який повинен узагальнити усі аспекти інформаційної роботи: отримання, збереження, аналітики, безпеки тощо. Тим самим, можна буде уникнути інформаційної ангажованості окремих підрозділів та необґрунтованого приховування інформації.

Виходячи із того, що у своїй службовій діяльності органи прокуратури оперують службовою та іншою інформацією з обмеженим доступом, що була отримана в ході досудового розслідування, наглядовою діяльністю, судового процесу, можна говорити, що вони на ряду 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 (в тому числі 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 [8, с. 98].

До інших загроз інформаційної безпеки в органах прокуратури слід віднести: незаконне проникнення в інформаційне середовище системи органів прокуратури (хакерство); діяльність громадян, установ, організацій у вигляді цілеспрямованих акцій спрямованих на підрив ділової репутації, авторитету органів прокуратури в суспільстві, поширення неправдивих відомостей про діяльність прокурорів; несанкціонований витік інформації про хід або результати прокурорської діяльності, в тому числі, у потоках міжвідомчих інформаційно-аналітичних систем; дезорганізація або пошкодження зведених інформаційних масивів, автоматизованих робочих місць, збої в їх роботі; ризик інформаційного терору (можливості організованих злочинних угрупувань, використовуючи власні технічні можливості або ресурси інших установ, здобувати конфіденційну або таємну інформацією, змінювати, підроблювати, чи використовувати її у власних інтересах) [9, с. 16]; низькій рівень зворотного зв'язку, неналагодженість комунікації із органами державної влади, підприємствами, установами, організаціями, тощо.

З цього приводу також існує думка А.С. Хомича про те, що на сучасному етапі основними реальними та потенційними загрозами інформаційній безпеці прокуратури є: 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[10].

Формуючи власну думку з приводу загроз інформаційний безпеці в органах прокуратури, зазначимо, що ми визначили наступні їх категорії, фактори:

1. Стрімкий прогрес інформаційних технологій, які можуть використовуватись для протиправного впливу на інформаційні ресурси прокуратури. Відповідні структурні підрозділи, які здійснюють інформаційну підтримку та забезпечення не завжди здатні володіти актуальною інформацію про новації, а також формувати контрзаходи, спрямовані на убезпечення діяльності системи прокуратури.
2. Недоброчесність працівників прокуратури, які в деяких випадках зловживають наданими їм повноваженнями щодо роботи з інформацією, що призводить до її викривлення, неповноти, несанкціонованого витоку тощо.
3. Відсутність чіткої інформаційно-організаційної структури спеціальних підрозділів інформаційної роботи, що пов'язано із існуванням самостійних інформаційних повноважень окремих підрозділів прокуратори, що призводить до неякісної інформаційної співпраці, обміну інформацією.
4. Інформаційні диверсії, що пов'язані з потенційною можливістю втручання у роботу внутрішніх інформаційних систем, мереж, що може призводити до викрадення інформації, а також використання її для протидії прокурорам при виконання ними функцій та покладних на них завдань.

Основними заходами захисту інформації деякі вчені пропонують вважати: документальне оформлення переліку відомостей конфіденціального характеру, в тому числі з урахуванням відомчої специфіки цих відомостей; реалізація дозвільної системи допуску виконавців (користувачів, обслуговуючого персоналу) до інформації; обмеження доступу персоналу та сторонніх осіб до приміщень, де розміщені засоби інформатизаційно-комунікаційного обладнання, а також зберігаються носії інформації;

розмежування доступу користувачів і обслуговуючого персоналу до інформаційних ресурсів, програмним засобам обробки (передачі) і захисту інформації; реєстрація дій користувачів і обслуговуючого персоналу, контроль несанкціонованого доступу та дій користувачів, обслуговуючого персоналу і сторонніх осіб; облік і надійне зберігання паперових та цифрових носіїв конфіденційної інформації та звернення, що виключає розкрадання, підміну і знищення; використання сертифікованих за вимогами безпеки інформації спеціальних захисних знаків, які створюються на основі фізико-хімічних технологій для контролю доступу до об'єктів захисту і для захисту документів від підробки; резервування технічних засобів, дублювання масивів і носіїв інформації; використання технічних засобів, які відповідають вимогам стандартів з електромагнітної сумісності; використання сертифікованих засобів захисту інформації; розміщення дисплеїв і інших засобів відображення інформації, що виключає її несанкціонований перегляд; організація фізичного захисту приміщень та власне технічних засобів охорони, що запобігають або суттєво ускладнюють проникнення в будівлі, приміщення сторонніх осіб, розкрадання документів і носіїв інформації, самих засобів інформації; запобігання проникнення програм-вірусів, програмних закладок тощо [11, с.115-117].

Наступним питанням, яке потребує з'ясування, являється зміст інформації, що потребує захисту в органах прокуратури України. В даному 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.

Одним із напрямів інформаційної діяльності органів прокуратури є персональні дані, які згідно із Законом України «Про захист персональних даних» від 01.06.2010 р. № 2297-VI можуть бути віднесені до конфіденційної інформації, незаконне розголошення якої карається законом. Механізм захисту персональних даних в органах прокуратури містить дві складових.

По-перше, захист відомостей про осіб, що фігурують в процесуальних актах-документах, управлінських рішеннях, зведених інтегрованих інформаційних масивах. До прикладу, такі відомостей можуть зберігатися в інформаційній (автоматизованій) системі «Єдиний реєстр досудових розслідувань» (далі - ЄРДР), адміністратором якого є, власне, Генеральна прокуратура України. Згідно із Наказом Генерального прокуратура України «Про затвердження Порядків обробки персональних даних в органах прокуратури України» від 26 липня 2014 року № 77 кожен працівник прокуратури дає підписку про зобов'язання не допускати розголошення у будь-який спосіб персональних даних, в тому числі відомостей із ЄРДР, які йому довірені або стали відомі у зв'язку з виконанням службових обов'язків [12]. 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 [13].

По-друге, безпека персональної інформації про співробітників прокуратури. Загалом обробка персональних даних про працівників прокуратури 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 з трудовими відносинами, отримання статистичної, адміністративної та іншої інформації щодо персоналу, а також ведення кадрового діловодства [12].

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

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

Вплив інформаційної загрози в 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 сучасні 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 виділити засоби технічного захисту інформації в системі інформатизації та електронізації в органах прокуратури: блокування пристроїв і інтерфейсів вводу-виводу інформації [15]; електронний цифровий підпис; корпоративізація інформаційно-обчислювальної мережі; ідентифікація та аутентифікація доступу в персональний аккаунт; антивірусне програмне забезпечення тощо.

Отже, з огляду на підвищений рівень загроз та небезпек в щоденній діяльності працівників прокуратури, парадигма інформаційної захищеності повинна трансформуватися в самостійний напрямок та функцію органів прокуратури із гармонійним поєднанням правового та технічного сегменту. Для цього цілком необхідно розробити концепцію інформаційної безпеки органів прокуратури. 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.

Отже підсумуємо.

1. Виходячи із того, що забезпечення інформаційної безпеки є однією з внутрішньоорганізаціних (управлінських) 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 в процесі здійснення прокурорської діяльності.

2. Інституалізація питань забезпечення інформаційної безпеки забезпечується через діяльність фактично у кожному департаменті або управлінні власного відділу інформаційно-технологічного супроводження, що, скоріше формує певні проблеми у взаємодії різних підрозділів прокуратури, що в результаті призводить до проблем інформаційного обміну, незнання реальної картини подій в інших структурних підрозділах, створення інформаційних бар'єрів тощо. Звичайно, володіння та користування специфічною інформацією передбачає необхідність її убезпечення, але ця діяльність повинна здійснюватися на загальноприйнятих засадах, встановлених правилах. Отже, на нашу думку, циркуляція інформації та питання інформаційної безпеки повинна бути закріплена на рівні окремого Регламенту інформаційної діяльності в органах прокуратури, який повинен узагальнити усі аспекти інформаційної роботи: отримання, збереження, аналітики, безпеки тощо. Тим самим, можна буде уникнути інформаційної ангажованості окремих підрозділів та необґрунтованого приховування інформації.

3. Формуючи власну думку з приводу загроз інформаційний безпеці в органах прокуратури, зазначимо, що ми визначили наступні їх категорії, фактори:

– Стрімкий прогрес інформаційних технологій, які можуть використовуватись для протиправного впливу на інформаційні ресурси прокуратури. Відповідні структурні підрозділи, які здійснюють інформаційну підтримку та забезпечення не завжди здатні володіти актуальною інформацію про новації, а також формувати контрзаходи, спрямовані на убезпечення діяльності системи прокуратури.

– Недоброчесність працівників прокуратури, які в деяких випадках зловживають наданими їм повноваженнями щодо роботи з інформацією, що призводить до її викривлення, неповноти, несанкціонованого витоку тощо.

– Відсутність чіткої інформаційно-організаційної структури спеціальних підрозділів інформаційної роботи, що пов'язано із існуванням самостійних інформаційних повноважень окремих підрозділів прокуратори, що призводить до неякісної інформаційної співпраці, обміну інформацією.

– Інформаційні диверсії, що пов'язані з потенційною можливістю втручання у роботу внутрішніх інформаційних систем, мереж, що може призводити до викрадення інформації, а також використання її для протидії прокурорам при виконання ними функцій та покладних на них завдань.

4. Удосконалення способів забезпечення інформаційної безпеки в органах прокуратури ми вбачаємо у їх закріпленні на рівні концептуальних та нормативних документів. Зокрема, ми пропонуємо:

Передбачити у Концепції інформаційної безпеки України положення про специфікацію внутрішньо організаційної діяльності органів публічної адміністрації та правоохоронних органів у сфері інформаційної безпеки. Забезпечити визначення місця органів прокуратури в якості одного із активних суб'єктів забезпечення законності у сфері діяльності пов'язаною із забезпеченням інформації безпеки тощо.

Розробити Концепцію інформаційної безпеки органів прокуратури, у якій передбачити питання інституалізації структурних підрозділів, способи забезпечення, заходи перспективного розвитку засад забезпечення інформаційної безпеки, а також визначити шляхи правового регулювання зазначеної сфери.

Утворити в структурі Генеральної прокуратури України спеціальний структурний підрозділ забезпечення інформаційної безпеки, розробити положення про нього.

Список використаних джерел

1. Березовська І. Р. Адміністративно-правові засоби забезпечення інформаційної безпеки в Україні. – Дисертація на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право. – Національна академія внутрішніх справ, Київ, 2012. – 239с.
2. Красіков Д.О. Правове забезпечення інформаційної безпеки в діяльності органів внутрішніх справ України. – Дисертація на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право. – Національна академія внутрішніх справ, Київ, 2012. – 220с.
3. Про основи національної безпеки України: Закон від 19.06.2003 № 964-IV // Відомості Верховної Ради України (ВВР), 2003, № 39, ст.351
4. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон від 09.01.2007 № 537-V // Відомості Верховної Ради України (ВВР), 2007, № 12, ст.102
5. Про організацію роботи з питань внутрішньої безпеки в органах прокуратури України : Наказ Генерального прокурора України від 22.09.2014 року № 17 гн
6. Положення про Генеральну інспекцію Генеральної прокуратури України : Наказ Генерального прокурора України від 16 червня 2016 року № 204
7. Положення про Департамент інформаційних технологій, документального та матеріально-технічного забезпечення Генеральної прокуратури України : Наказ Генеральної прокуратури України від 30 серпня 2016 року № 310
8. 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.
9. Камышев Э.Н. Информационная безопасность и защита информации: Учебное пособие. - Томск: ТПУ, 2009. - 95 с.
10. Хомич А.С. Інформаційні технології як загроза інформаційній безпеці прокуратури : Право і безпека. 2012. № 3 (45) / Електронний ресурс : http://www.nbuv.gov.ua/old_jrn/soc_gum/Pib/2012_3/PB-3/PB-3_33.pdf
11. Зимин Виктор Матвеевич Административно-правовая организация информационного обеспечения деятельности судов общей юрисдикции [Электронный ресурс]: Дис. ... канд. юрид. наук : 12.00.14 .-М.: РГБ, 2005 – 183 с.
12. Про затвердження Порядків обробки персональних даних в органах прокуратури України : Наказ Генерального прокуратура України від 26 липня 2014 року № 77. – Електронний ресурс. – режим доступу : http://www.gp.gov.ua/ua/personal_data_protection
13. Про порядок ведення Єдиного реєстру досудових розслідувань : Наказ Генерального прокурора України № 69 від 17.08.2012. – Електронний ресурс. – [режим доступу] : http://lug.gp.gov.ua/ua/lugpes.html?_m=publications&_t=cat&id=114099
14. 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
15. Надання послуг в області технічного захисту інформації [текст]. – [Електронний ресуср]. – режим доступу : http://www.ulyssys.com/i/lng.ua/page.security

ПРИВАТНИЙ НАВЧАЛЬНИЙ ЗАКЛАД ЯК СУБ'ЄКТ ПІДПРИЄМНИЦЬКОЇ ДІЯЛЬНОСТІ

Тимошенко М.О., *кандидат юридичних наук, проректор Європейського університету*

Анотація: *Обґрунтовано сутність функціонування вищого навчального закладу як суб'єкта підприємницької діяльності, що є товаровиробником освітніх послуг. Проведено аналіз динаміки змін кількості вищих навчальних закладів України в розрізі форм власності за 2010-2016 н/р. Досліджено можливості приватних вищих навчальних закладів в сучасному суспільстві. Обґрунтовано переваги приватних вищих навчальних закладів для суспільства, студентів та викладачів. Виявлено, що ефективне функціонування приватних вишів на ринку освітніх послуг прямопропорційно пов'язане із використанням новітніх технологій, інновацій та наявності ефективної стратегії розвитку.*

Ключові слова: *приватний вищий навчальний заклад, суб'єкт підприємницької діяльності, освітні послуги, освітня діяльність, освітній рівень.*

Summary: *The article argues essence of performance of a higher educational establishment as a business entity, producing educational services. The research analyses dynamics of changes in the number of higher educational establishments of Ukraine in terms of the forms of ownership for the period of 2010-2016. The author investigates opportunities of private higher educational establishments in the modern society and argues their advantages for the society, students and teachers. It is proved that efficient performance of private higher educational establishments at the market of educational services is directly influenced by application of innovative technologies and an efficient strategy of development.*

Key words: *private higher educational establishment, business entity, educational services, educational activity, educational level.*