УДК 343.9
DOI 10.33244/2617-4154.3(12).2023.236-242

Г. В. Дідківська,
д-р юрид. наук, професор
e-mail: galynadid@gmail.com
ORCID ID 0000-0002-3545-0429;
В. В. Топчій,
д-р юрид. наук, професор,
заслужений юрист України,
Державний податковий університет
e-mail: tv1959@ukr.net
ORCID ID 0000-0003-4596-6469

КРИМІНАЛІСТИЧНІ МЕХАНІЗМИ ОХОРОНИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У статті зазначається, що інформаційна безпека є одним із найважливіших чинників національної безпеки України. Інформаційна і національна безпеки повною мірою узгоджуються і співвідносяться між собою за схемою як частина і ціле. Сьогодні інформаційна складова не існує поза межами загальної національної безпеки, так само, як і національна безпека не буде всеохоплюючою без інформаційної безпеки. Тобто інформаційна безпека є невід'ємною складовою кожної зі сфер національної безпеки і потребує, зокрема, і криміналістичної охорони. Водночас інформаційна безпека є важливою самостійною сферою забезпечення національної безпеки. Саме тому розвиток України як суверенної, демократичної, правової та економічно стабільної держави можливий тільки за умови забезпечення належного рівня її інформаційної безпеки. Інформаційна безпека є складним, системним і багаторівневим феноменом, на стан і перспективи розвитку якого мають безпосередній вплив зовнішні і внутрішні чинники, найважливішими з яких є: політична обстановка у світі; наявність потенційних зовнішніх і внутрішніх загроз; стан і рівень інформаційно-комунікаційного розвитку країни; внутрішньополітична обстановка в державі.

Ключові слова: *криміналістика, інформаційна безпека, кримінальні провадження, кримінальне правопорушення, криміналістичні механізми, охорона, національна безпека.*

Кожною галуззю права, зокрема і криміналістикою, закріплюються у своїх інституціях і положеннях цілі, принципи, стратегія, напрями, основні засоби і методи політики держави у своїй сфері діяльності. Відповідно, і криміналістика закріплює у своїх положеннях основні концепції політики держави у сфері застосування криміналістичних механізмів охорони інформаційної безпеки.

Разом з тим криміналістика не є пасивним реєстратором державної політики такої діяльності. Вона має свої власні непорушні основні положення, на які не може і не

повинна впливати політика держави. Така позиція закріплена у ст. 8 Конституції України як принцип верховенства права.

Визначним у проблематиці теорії організації інформаційної безпеки є з'ясування її напрямів на засадах комплексного підходу щодо методів підтримки режиму, охорони та захисту інформаційної безпеки. Умовно можна визначити такі напрями організації підтримки, охорони та захисту: правові, управлінські, інженерно-технологічні. У складі останніх щодо комп'ютерних систем як автономні визначаються програмно-математичні (комп'ютерні програмні продукти захисту) та апаратні. В окремих джерелах вони об'єднуються в категорії «апаратно-програмні». На основі зазначених положень можна зробити висновок про існування потреби формування проблематики окремих аспектів (інститутів) у складі комплексної наукової дисципліни – загальної теорії і практики інформаційної безпеки щодо підтримки, охорони та захисту інформації. У зв'язку з цим існує можливість виділення двох частин теорії: загальної частини (фундаментальних, загальних положень) та особливої частини (відносин щодо окремих напрямів функцій на основі загальних положень). На загальнотеоретичному рівні визначимося в наступних ключових, таких проблемах інформаційної безпеки щодо організаційного аспекту підтримки, охорони та захисту інформації в автоматизованих (комп'ютерних) інформаційних системах.

На зазначені напрями підтримки інформаційної безпеки відповідного об'єкта захисту впливають такі визначні фактори: а) фактор рівня досягнень науково-технічного прогресу (переважно в галузі розвитку, вдосконалення технічних засобів); б) технологічний фактор (в окремих джерелах його ще називають алгоритмічний фактор, коли техніка може бути одна, а технології її застосування різні, цей фактор ще є визначним для формування методик як отримання інформації, так і захисту її); в) соціальний (людський) фактор. Важливим елементом організації інформаційної безпеки є поділ заходів на групи щодо протидії. У теорії і практиці майже однозначно виділяють три такі групи: активні засоби захисту (наприклад, розвідка, дезінформація, зашумлення тощо); пасивні засоби захисту (наприклад, створення перешкод несанкціонованому витоку інформації тощо); комплекс засобів захисту (органічне поєднання попередньо вказаних груп). З огляду на зазначені поняття в умовах інформатизації України можна визначити наступну класифікацію загроз інформаційній безпеці людини, суспільству, державі. За сутністю походження, з точки зору системно-інтегративного підходу їх можна умовно поділити на три види: природні загрози (стихійні лиха): землетруси, повені, смерчі, стихійні пожежі, зливи тощо; техногенні загрози: аварії, катастрофи тощо, породжені технічними (штучними) та технологічними системами [1].

Поширення комп'ютерної техніки суттєво посилило проблему захисту інформації взагалі і зокрема – безперешкодної передачі персональних даних у цифровому вигляді. Основна мета будь-якої системи інформаційної безпеки полягає в забезпеченні сталого функціонування об'єкта, що захищається: в запобіганні загроз його безпеки, в захисті законних інтересів власника інформації від протиправних посягань. За цілями загрози інформаційної безпеки можуть бути класифіковані так: 1) несанкціоноване читання

інформації; 2) несанкціоновані зміни інформації; 3) несанкціоноване знищення інформації. Можуть бути й інші варіанти, зокрема класифікації загроз за типом використовуваної слабкості захисту, за способом дій порушника тощо. Основою захисту від збоїв пристроїв зберігання інформації є організація системи резервного копіювання та дублювання даних [2, с. 41].

То що ж таке інформаційна безпека? Інформаційною безпекою вважають суспільні відносини щодо створення і перебування в належному стані дієвого режиму функціонування цілісної інформаційної системи; комплекс організаційних, правових та інженерно-технологічних заходів щодо правової охорони, запобігання і подолання природних, техногенних і соціогенних та злочинних загроз, реалізація яких може пошкодити чи припинити функціонування такої системи.

У сучасних інформаційних системах рекомендується зберігати і передавати інформацію з обмеженим доступом у зашифрованому вигляді. Квантові методи передачі інформації гарантують неможливість розшифровки повідомлення. Здатність криптографічного алгоритму протистояти розшифровці позначається як криптографічна стійкість повідомлення з обмеженим доступом. Ідентифікація та аутентифікація можуть бути використані у системах виявлення вторгнень і системах управління ідентифікацією та доступом. Ідентифікація користувача може бути використана для збору інформації про зловмисників в імітаційних системах Honeypot і подальшого налаштування рівня політики безпеки реальної системи залежно від отриманої службової інформації від користувачів. За наявності права постійного, тимчасового або разового доступу до контрольованої зони порушники інформаційної безпеки поділяються на зовнішніх та внутрішніх. Програмування забезпечення інформаційної безпеки служби криміналістики у процесі розробки програм ефективного управління та захисту інформаційних ресурсів передбачає систематизацію алгоритмів і відповідної інформації.

Потрібно враховувати, що під час забезпечення інформаційної безпеки процес управління ризиками та загрозами інформаційній безпеці є одним з ключових аспектів. Вибір управлінських рішень не може бути ефективним без чіткої системи застосування нормативно-методичних документів на основі досвіду роботи у сфері, пов’язаної із захистом конфіденційної інформації [2, с. 6]. У процесі розслідування комп’ютерних кримінальних правопорушень виключно важливим є тактика і технологія призначення слідчим криміналістом судових експертиз під час розслідування комп’ютерних кримінальних правопорушень, де основне місце відводиться опису сучасних можливостей експертного дослідження, яке дається через переліки типових завдань основних судових експертиз, що призначаються під час вивчення вищевказаних об’єктів. Насамперед це, безумовно, стосується судової комп’ютерно-технічної експертизи, яка сьогодні являє собою клас судових експертиз, до якої входять: апаратно-комп’ютерна, програмно-комп’ютерна, інформаційно-комп’ютерна, комп’ютерно-мережева експертизи. Також формуються нові судові комп’ютерно-технічні експертизи пристроїв стільникового зв’язку. Впроваджуються такі нові засоби, як мобільний криміналіст, UFED, XRY, Encase та інші апаратно-програмні комплекси, призначені для збирання і

перевірки цифрових слідів злочинів. Кінцевим етапом зазначеної оптимізації організації роботи служби криміналістики має стати досягнення двох взаємопов'язаних цілей. Першою з них є створення і введення в експлуатацію швидкого, надійного програмного забезпечення, що володіє широкими функціональними можливостями. Другою – професійне виховання працівників служби криміналістики і досягнення ними такого рівня усвідомлення своєї відповідальності перед суспільством і законом, у ході якого не виникало б бажання скористатися довіреним програмним забезпеченням у незаконних цілях. Мінімальні вимоги інформаційної безпеки зобов'язують керівника відділу криміналістики належно організувати контроль за тим, щоб з інформаційними системами працювали особи, які пройшли відповідну підготовку та ознайомлені з призначеною для користувача документацією на програмне забезпечення; в разі переведення на іншу посаду, звільнення або зміну функціоналу працівника служби криміналістики, який мав доступ до ключових елементів програмного забезпечення, особою, відповідальною за інформаційну безпеку, була проведена необхідна робота; посадові інструкції щодо роботи з інформаційними системами були складені з чітким розподілом обов'язків між працівниками, що виключає дублювання або двояке тлумачення; структурний підрозділ, що відповідає за забезпечення інформаційної безпеки, був оснащений необхідним не тільки загальносистемних, але і спеціальним програмним забезпеченням. Інформаційна безпека повинна забезпечуватися єдиною комплексною програмою, технічна реалізація якої можлива в актуальних умовах матеріально-технічного забезпечення служби криміналістики і основними принципами якої виступають: простота, пріоритетність заходів попереджувального характеру, персональна відповідальність працівника служби криміналістики. В інформаційній системі реєстрації необхідне створення криміналістичних обліків за способами комп'ютерних злочинів (modus operandi), які повинні забезпечувати здійснення обміну інформацією на міждержавному рівні. Зв'язки цифровізації криміналістичної та судово-експертної діяльності здійснюються через відомчі довідково-інформаційні фонди, де зосереджені, зокрема, зразки для порівняльних досліджень [2, с. 194].

Для забезпечення ефективного захисту інформації повинні виконуватися такі кроки з впровадження, контролю і підтримки системи управління інформаційною безпекою: 1) проведення класифікації об'єктів захисту і визначення їх критичності; 2) оцінка ризиків інформаційної безпеки; 3) вибір та реалізація відповідних вимог забезпечення інформаційною безпекою, зниження рівня ризиків; 4) здійснення контролю, підтримки і підвищення ефективності засобів управління безпекою, пов'язаних з активами організації [3, с. 162].

Сучасне розуміння інформаційної безпеки в умовах інтенсивної інформатизації України як соціального явища відбувається поступово і так. Інформаційна безпека в умовах інформатизації України під час формування інформаційного суспільства здебільшого розуміється як суспільні відносини щодо створення і підтримки у належному стані порядку ефективного функціонування відповідної автоматизованої інформаційної системи, систем телекомунікації, інших подібних мереж; комплекс організаційних, правових та інженерно-технологічних можливостей щодо охорони,

захисту, запобігання і подолання природних, техногенних і соціогенних загроз, реалізація яких може порушити чи припинити життєдіяльність конкретної соціотехнічної інформаційної системи.

Тому огляд сучасних практик під час формування безпечних паролів і доведення результатів огляду до відома співробітників є ключовим елементом у процесі формування парольної політики організації. Так, потрібно встановити правила видачі інформації для співробітників організації тільки після перевірки ідентичності користувачів з використанням безпечних способів. Облікові записи засобів захисту інформації, що створені за замовчуванням, повинні бути видалені або заблоковані. Рекомендується встановлення регламенту дії у разі компрометації паролів. На жаль, як бачимо, нині на концептуальному рівні відсутня розроблена система теоретико-методологічних засад забезпечення інформаційної безпеки служби криміналістики. Отже, враховуючи світовий досвід, вважаємо перспективним проєкт створення цифрової інформаційної мережі кабінетів криміналістики із застосуванням комп'ютерних технологій. У разі забезпечення захисту окремо має бути визначено підстави та порядок пронесення на територію, що охороняється, без відповідного дозволу особистої кіно-, фото-, звуко- і відеозаписуючої апаратури, розмножувальної, копіювальної техніки, персональних комп'ютерів і блоків до них, а в деяких випадках навіть і мобільних телефонів. Приміщення, в яких ведуться секретні роботи, повинні бути постійно закриті на замок. Включення сигналізації проводиться начальником охорони або його заступником у присутності працівника служби криміналістики, який здає приміщення. Про час включення сигналізації робиться відмітка у відповідному журналі [3, с. 133–134].

Цифрова трансформація служби криміналістики – це процес корінного перетворення концепції і формату функціонування систем усіх рівнів за допомогою оцифровки: переведення всіх ресурсів на цифровий формат, впровадження та формування пулу цифрових технологій, а також створення мережевих платформ інтеграції та взаємодії користувачів цифрових технологій у цілях досягнення сталого і довгострокового існування в динамічних умовах цифрового простору. Під час розробки цільових програм інформаційного захисту потрібно застосовувати технологію, що передбачає облік (поряд з набором показників ефективності) принципів інформатизації й інтересів усіх категорій користувачів (прокурорів, слідчих, експертів, оперативних працівників), а також використовувати спеціалізований інтернет-портал й управлінську модель. Інформаційно-правова безпека слідчого криміналіста – це стан захищеності права шукати, одержувати, зберігати, використовувати і поширювати інформацію, а також права на недоторканність інформації про приватне життя. Висувається пропозиція щодо модернізації системи налагодженого зв'язку обміну інформацією, організаційно-правовою формою втілення чого має стати створення Національної цифрової онлайн-платформи об'єднаної служби криміналістики України. Платформа планується ресурсом з обмеженим доступом, якому притаманні функції технологій штучного інтелекту для пошуку, систематизації та верифікації інформації. Така організаційно-правова модель інформаційної трансформації окремих служб

криміналістики МВС, СБУ і ДБР із залученням детективів-криміналістів кримінальної лабораторії НАБУ має забезпечити автоматичне співвіднесення інформаційних даних за різними напрямами слідчої роботи. Для підвищення гарантій професійної діяльності слідчих-криміналістів необхідно впровадити нові тактики і методики забезпечення інформаційної безпеки служби криміналістики. Одним з інструментів забезпечення професійної надійності та безпеки слідчих-криміналістів є закріплення у проєкті Закону України «Про систему досудового слідства України та статус слідчих» нормативних положень, присвячених організаційно-правовому визначенню статусу, завдань, функцій та обсягу повноважень слідчого криміналіста і кваліфікаційних вимог до осіб, які мають намір зайняти цю посаду [4].

Інформаційна безпека є одним із найважливіших чинників національної безпеки України. Інформаційна і національна безпека повною мірою узгоджуються та співвідносяться між собою за схемами «частина» і «ціле». Сьогодні інформаційна складова не існує поза межами загальної національної безпеки, так само, як і національна безпека не буде всеосяжною без інформаційної безпеки [5]. Загальним підґрунтям цих понять є, безумовно, поняття «безпека», що обумовлює стан захищеності життєвих інтересів людини як особистості, суспільства, держави. Сьогодні їх варто розглядати у геополітичному вимірі як невід'ємну частину державної політики із системою заходів економічного, політичного, організаційного та іншого спрямування, які адекватні загрозам життєво важливим інтересам громадян, суспільства і держави саме в такому контексті [5]. Тобто інформаційна безпека є невід'ємною складовою кожної зі сфер національної безпеки. Водночас інформаційна безпека є важливою самостійною сферою забезпечення національної безпеки. Саме тому розвиток України як суверенної, демократичної, правової та економічно стабільної держави можливий тільки за умови забезпечення належного рівня її інформаційної безпеки [6]. Інформаційна безпека є складним, системним і багаторівневим феноменом, на стан і перспективи розвитку якого мають безпосередній вплив зовнішні і внутрішні чинники, найважливішими з яких є: політична обстановка у світі; наявність потенційних зовнішніх і внутрішніх загроз; стан і рівень інформаційно-комунікаційного розвитку країни; внутрішньополітична обстановка в державі та ін. [6].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Цимбалюк В. Окремі питання щодо визначення категорії «інформаційна безпека» у нормативно-правовому аспекті. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2004. Вип. 8. С. 30–33.

2. Остапов С. Е., Євсеєв С. П., Король О. Г. Технології захисту інформації : навчальний посібник. Харків : Вид. ХНЕУ, 2013. 476 с.

3. Синеокий О. В. Основы информационного права и законодательства в области высоких технологий и ИТ-инноваций. Харків : Право, 2011. 592 с.

4. Про систему досудового слідства України та статус слідчих : проєкт Закону. URL : http://lsej.org.ua/3-2_2020/22.pdf

5. Соснін О. В. Проблеми державного управління системою національних інформаційних ресурсів з наукового потенціалу України : монографія. К. : Інститут держави і права ім. В. М. Корецького НАН України, 2003. 572 с.

6. Доктрина інформаційної безпеки України, затверджена Указом Президента України від 8 липня 2009 року № 514/2009.

REFERENCES

1. Tsymbaliuk V. Okremi pytannia shchodo vyznachennia katehorii «informatsiina bezpeka» u normatyvno-pravovomu aspekti. *Pravove, normatyvne ta metrolohichne zabezpechennia systemy zakhystu informatsii v Ukraini.* 2004. Vyp. 8. S. 30–33.

2. Ostapov S. E., Yevseiev S. P., Korol O. H. Tekhnolohii zakhystu informatsii : navchalnyi posibnyk. Kharkiv : Vyd. KhNEU, 2013. 476 s.

3. Syneokyi O. V. Osnovы ynformatsyonnoho prava y zakonodatelstva v oblasty vыsokykh tekhnolohyi y YT-ynnovatsyi. Kharkiv : Pravo, 2011. 592 s.

4. Pro systemu dosudovoho slidstva Ukrainy ta status slidchykh : Proiekt Zakonu. URL : http://lsej.org.ua/3-2_2020/22.pdf

5. Sosnin O. V. Problemy derzhavnoho upravlinnia systemoiu natsionalnykh informatsiinykh resursiv z naukovoho potentsialu Ukrainy : monohrafiia. K. : Instytut derzhavy i prava im. V. M. Koretskoho NAN Ukrainy, 2003. 572 s.

6. Doktryna informatsiinoi bezpeky Ukrainy. Zatverdzhena Ukazom Prezydenta Ukrainy vid 8 lypnia 2009 roku № 514/2009.

G. Didkivska, V. Topchii. Forensic mechanisms of information security protection

This article notes that information security is one of the most important factors of Ukraine's national security. Information and national security are fully coordinated and interrelated according to the scheme as a part and a whole. Today, the information component does not exist outside of overall national security, just as national security will not be comprehensive without information security. That is, information security is an integral component of each of the spheres of national security and requires forensic protection as well. At the same time, information security is an important independent area of national security. That is why the development of Ukraine as a sovereign, democratic, legal and economically stable state is possible only under the condition of ensuring the appropriate level of its information security. Information security is a complex, systemic and multi-level phenomenon, the state and prospects of whose development are directly influenced by external and internal factors, the most important of which are: the political situation in the world; presence of potential external and internal threats; the state and level of information and communication development of the country; internal political situation in the state.

Keywords*. Forensics, information security, criminal proceedings, criminal offense, forensic mechanisms, security, national security.*

Стаття надійшла до редколегії 2 травня 2023 року