РОЗДІЛ 5
КРИМІНАЛЬНИЙ ПРОЦЕС ТА КРИМІНАЛІСТИКА; СУДОВА ЕКСПЕРТИЗА; ОПЕРАТИВНО-РОЗШУКОВА ДІЯЛЬНІСТЬ

УДК 343
DOI https://doi.org/10.32782/2524-0374/2020-3-2/20

СТРАТЕГІЇ РОЗВИТКУ БЕЗПЕКИ ЦИФРОВИХ КОМУНІКАЦІЙ СЛУЖБИ КРИМІНАЛІСТИКИ

FORENSIC SECURITY DIGITAL COMMUNICATIONS DEVELOPMENT STRATEGIES

Коваль С.М., здобувач кафедри адміністративного та митного права
Університет митної справи та фінансів

У статті досліджуються стратегії розвитку безпеки цифрових комунікацій служби криміналістики. Охарактеризовано напрями розвитку цифрових комунікацій служби криміналістики у сучасній системі правоохоронних органів та визначено стандарти побудови системи інформаційної безпеки слідчого-криміналіста. Увага акцентувана на тому, що сучасна дійсність характеризується колосальним зростанням обсягів інформації, обумовлюючи необхідність створення модернізованої інформаційної інфраструктури служби криміналістики з масштабним дата-центром, що забезпечить довгострокове мережеве зберігання даних, зокрема з обмеженим доступом.

Наголошується про актуальність формування мобільного цифрового інформаційного середовища служби криімналістики, що вимагає підтримки з боку держави в рамках єдиної політики реформування правоохоронної системи.

Методологічним базисом дослідження є сукупність загальнонаукових та спеціальних методів і прийомів наукового пізнання. Методом правового регулювання інформаційних відносин є комплексне використання методів адміністративного та цивільного права. Однією з методологічних засад є інтеграційний метод дослідження інформаційно-технологічного потенціалу служби криміналістики. Доцільність використання інтеграційного методу може свідчити упорядкування масивів і компонентів автоматизованих інформаційно-технологічних систем у службі криміналістики, зумовлюючих забезпечення процесів розслідування із застосуванням передових технологій форензики, комп'ютерної техніки і засобів зв'язку.

У висновках сформульовано розуміння системи інформаційної безпеки слідчого-криміналіста у широкому та вузькому сенсі, а також запропоновано організаційно-правову модель інформаційної трансформації окремих служб криміналістики відповідних правоохоронних органів. Платформа планується ресурсом з обмеженим доступом, якому мають притаманні функції технологій штучного інтелекту для пошуку, систематизації та верифікації інформації.

Ключові слова: інформаційна безпека, інформаційні ресурси, правоохоронні органи, слідчий-криміналіст, служба криміналістики, цифрові комунікації.

The article examines the strategies for the development of digital communications security of the forensic service. The directions of development of digital communications of the forensic service in the modern system of law enforcement agencies are characterized and the standards of building the information security system of the forensic investigator are determined. Emphasis was placed on the fact that the current reality is characterized by a huge increase in information, necessitating the creation of a modernized information infrastructure of the forensic service with a large data center that will provide long-term network storage, including limited access.

It is emphasized that the formation of a mobile digital information environment of the criminalistics service is urgent, which requires support from the state within the framework of a unified policy of reforming the law enforcement system.

The methodological basis of the study is a set of general and special methods and techniques of scientific knowledge. The method of legal regulation of information relations is the integrated use of methods of administrative and civil law. One of the methodological principles is the integration method of studying the information technology potential of the forensic service. The expediency of using the integration method can be evidenced by the ordering of arrays and components of automated information technology systems in the forensic service, leading to the provision of investigative processes using advanced technologies of forensics, computer technology and communications.

The conclusions formulate the understanding of the information security system of the forensic investigator in a broad and narrow sense, as well as propose an organizational and legal model of information transformation of individual forensic services of the relevant law enforcement agencies. This platform is planned by a resource with limited access, which has the inherent functions of artificial intelligence technologies for search, systematization and verification of information.

Key words: information security, information resources, law enforcement agencies, investigator-criminologist, forensics service, digital communications.

Актуальність проблеми. Стрімке зростання обсягів інформації, формування колосальних інформаційних масивів і баз даних, цифрове опосередкування все більшої кількості областей і видів соціальної взаємодії, діяльності державних і громадських інститутів є значущим фактором розвитку сучасного суспільства, формує нову цифрову реальність. Активна цифровізація призводять до необхідності розробок приватних теорій і навчань, спрямованих на забезпечення використання електронної техніки в ході розслідування злочинів, а також на виявлення, фіксацію, дослідження і використання електронної інформації та інформаційно-технологічних пристроїв. Інформаційні технології та можливості інформаційно-телекомунікаційних мереж не тільки впливають на всі види діяльності людини, а й кардинально трансформують багато з них. Цей технологічний прорив, поза всяким сумнівом, є значимим чинником розвитку сучасного суспільства [9, с. 85-86].

Цифрове середовище створює юридизм нового типу, де рівень протидії встановленню істини суттєво зростає. Науково-технічний прогрес, концептуально будучи безсумнівним суспільним благом, одночасно ускладнює і вдосконалює форми протиправної діяльності, зобов'язуючи слідчих-криміналістів йти в ногу з часом – мати знання і навички, необхідні для протидії протиправним проявам. Формування мобільного інформаційного середовища суб'єктів, що ведуть боротьбу зі злочинністю, вимагає підтримки з боку держави в рамках єдиної політики.

Отже, настав час активізації формування нового інформаційного напряму у діяльності усіх правоохоронних органів України. Окремі проблемні питання у цьому

напрямку досліджували фахівці з інформаційного права (О. Архипов, Є. Балекно, В. Василюк, А. Венгеров, Ю. Волков, В. Ворожко, В. Гриценко, О. Дженакова, С. Демський, С. Ємельянов, Р. Калюжний, Л. Капінус, І. Касперський, Л. Коваленко, В. Копилов, О. Кохановська, П. Кузнецов, В. Ліпкан, П. Мельник, В. Наумов, Д. Перов, О. Климентьев, С. Павлюк, Н. Попова, П. Скок, І. Сопілко, О. Тихомиров, С. Хрипко, О. Червякова, М. Швець, К. Янішевська та ін.), теорії прокурорської діяльності (А. Альбеєва, О. Баганець, С. Банах, Є. Безкровний, О. Іванченко, А. Карпусь, М. Кістанова, І. Кожем'яка, І. Козьяков, С. Костенко, В. Кулаков, І. Курбатова, В. Лакизюк, А. Лапкін, О. Михайленко, С. Неворотіна, Ю. Пасічна, М. Руденко, М. Стефанчук, В. Сухонос, А. Ткач, А. Ярмиш та ін.), теорії правоохоронної діяльності та поліцеїстики (Л. Аркуша, П. Каркач, О. Комісаров, В. Мацюк, Т. Михальчук, В. Некрасов, А. Овчинський, І. Озерський, Л. Родинюк, Т. Соколан, Н. Філіпченко, О. Чудновський, А. Шарнін, А. Шкляренко та ін.), безпеки інформаційно-комунікаційних технологій (А. Войтик, Н. Ворзобова, Н. Гатченко, Ю. Гатчін, Г. Жигулін, В. Захаров, А. Ісаєв, Н. Кармановський, Ю. Каторін, О. Клімова, С. Князєв, О. Козенко, М. Кравчук, В. Кучинський, О. Матяш, В. Мацюк, О. Михайліченко, В. Некрасов, А. Ожиганов, С. Платунова, В. Прожерін, Н. Прохожев, О. Радкевич, А. Разумовський, В. Сапальов, А. Співак, І. Хараберюш, О. Хараберюш, А. Яковлєв та ін.) та інші. Вплив науково-технічного прогресу на право, а, отже, на діяльність правоохоронних структур широко вивчається в роботах багатьох вчених і практичних працівників (А. Ахвердян, А. Власов, М. Гаджиєва, О. Іванченко, О. Капінус, М. Кистанова, Н. Козаєва, В. Оганян, О. Петрашова, О. Пікур та ін.). За останні роки помітними стали дослідження близького спрямування О. Амеліна, О. Баганца, Б. Васильчука, С. Гайдая, В. Кашки, С. Мазурика, І. Піляя, Ю. Севрука, П. Шаганенка, де автори, торкаючись проблем включеності прокурора до системи інформаційного права, розглядали питання адміністративно-правового регулювання інформаційного забезпечення діяльності правоохоронних органів.

Предмет публікації – стратегії розвитку безпеки цифрових комунікацій служби криміналістики. **Мета статті –** охарактеризувати напрями розвитку цифрових комунікацій служби криміналістики з урахуванням її місця у сучасній системі правоохоронних органів та визначити стандарти побудови системи інформаційної безпеки слідчого-криміналіста.

В існуючій сфері забезпечення інформаційної безпеки одним з найбільш пріоритетних напрямків є захист персональних даних. З урахуванням впливу діючих загальносвітових тенденцій з питань щодо захисту інформації в цілому, і персональних даних зокрема, виникає питання про необхідність застосування все більш і більш досконалих засобів і механізмів захисту інформації.

У загальному розумінні будь-яка інформація, що відноситься до фізичної особи (суб'єкта персональних даних), має бути віднесена до персональних даних. Правове регулювання обігу персональних даних особи залишається однією з актуальних проблем сучасної правової науки і практики.

Специфіка полягає в необхідності створення оптимального правового механізму обороту і захисту персональних даних, що враховує в рівній мірі публічно-правовий інтерес держави і приватний інтерес індивіда.

Вирішення цієї проблеми неможливе також без моніторингу стану ринку інформаційних технологій, продуктів і послуг та відстеження загальних тенденцій розвитку інформаційного суспільства. Інститут персональних даних, що є одним з інститутів інформаційного права, в зв'язку зі складним характером всієї галузі теж є комплексним.

Поширення комп'ютерної техніки суттєво посилило проблему захисту інформації взагалі, і зокрема – безперешкодної передачі персональних даних у цифровому вигляді. Головна мета будь-якої системи інформаційної безпеки полягає в забезпеченні сталого функціонування об'єкта, що захищається: в запобігання загроз його безпеки, в захисті законних інтересів володільця інформації від протиправних посягань. За цілями загрози інформаційної безпеки можуь бути класифіковані наступним чином: 1) несанкціоноване читання інформації; 2) несанкціоновані зміни інформації; 3) несанкціоноване знищення інформації.

Можуть бути й інші варіанти, у тому числі 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 [5, с. 41].

В сучасних інформаційних системах рекомендується зберігати і передавати інформацію з обмеженим доступом в 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 та відповідної інформації.

На сьогодні єдиної автоматизованої системи збору, зберігання, переробки й видачі такої інформації поки що не створено. Звітні дані надходять до Міжвідомчого НДЦ на операційних системах Unix, MSDOS, Windows NT, OS/2, Linux та ін. В них використовуються різні формати даних, статистичні форми представляються на різних носіях. Це значно ускладнює опрацювання цієї інформації. Виходом є уніфікація законодавства в галузі інформаційних технологій, їхньої безпеки, прийняття єдиних стандартів криптографії. Це істотно знижує обсяги апаратно-програмних засобів і електронного документообігу служби криміналістики, а в загальній інфраструктурі усіх правоохоронних органів держави, забезпечує створення єдиних центрів, що сприятиме зростанню продуктивності антикримінальних заходів. У цьому напрямку одним з основних завдань є захист інформації служби криміналістики від спеціального впливу та несанкціонованих дій під час її обробки, використання й зберігання [7, с. 9].

Комп'ютерна форензика є основним і найбільш об'ємним розділом цифрової криміналістики. Безумовно, елементи форензики (електронної цифрової криміналістики), яка досягла глибини розробки – її положення базуються на інших природничих, гуманітарних і технічних науках та тісно пов'язані з ними, – дуже важливі й для діяльності з приводу захисту інформації з обмеженим доступом у цифрових умовах як одного з напрямів розвитку інформаційного права [10, с. 110-121]. Методи комп'ютерної криміналістики можуть забезпечити повноцінне розслідування інцидентів інформаційної безпеки. Тож правильний підхід і використання необхідних методів цифрової криміналістики відповідно до вимог до кожного інциденту забезпечить збір необхідних цифрових доказів.

Також дозволить визначити слабкі місця у мережі, провести повноцінні превентивні заходи [6, с. 36-41].

Забезпечення особистої професійної безпеки співробітників служби криміналістики залишається одним з актуальних завдань. О. Тамодлін пропнує розглядати інформаційну безпеку особистості в широкому і вузькому сенсі. У широкому сенсі інформаційна безпека особистості – це стан, при якому відсутня можливість заподіяння людині якогось шкоди відомостями з зовнішнього світу. Таке трактування охоплює багато сторін розглянутої проблеми – від соціальної до технічної. У вузькому сенсі захист конституційних прав людини і громадянина на пошук, отримання, виробництво, поширення інформації, на недоторканність інформації про приватне життя, а також його психіки від деструктивного впливу інформації інформаційна безпека особистості забезпечується державою, громадськими та іншими організаціями або окремими громадянами.

Зупинимося на забезпеченні інформаційної безпеки слідчих-криміналістів.

Об'єктами забезпечення інформаційної безпеки інформаційного вузла служби криміналістики є інформаційні ресурси відповідного рівня, що мають обмежений доступ, і які становлять таємницю, а також відкрита (загальнодоступна) інформація, яка необхідна для функціонування установи, незалежно від форми та виду її представлення. Крім того, об'єктом забезпечення інформаційної безпеки постає інформаційна інфраструктура, що включає системи обробки і аналізу інформації, технічні та програмні засоби її обробки, передачі і відображення, в тому числі канали інформаційного обміну і телекомунікації, системи та засоби захисту інформації, об'єкти, приміщення і будівля, де розміщено чутливі елементи служби криміналістики.

Потрібно враховувати, що при забезпеченні інформаційної безпеки процес управління ризиками та загрозами інформаційній безпеці є одним з ключових аспектів. Вибір управлінських рішень не може бути ефективним без суворої системи застосування нормативно-методичних документів на основі досвіду роботи в області, пов'язаної із захистом конфіденційної інформації [2, с. 6].

При розслідуванні комп'ютерних злочинів винятково важливим є тактика і технологія призначення слідчим-криміналістом судових експертиз при розслідуванні комп'ютерних злочинів, де основне місце відводиться опису сучасних можливостей експертного дослідження, яке дається через переліки типових задач основних родів судових експертиз, що призначаються при вивченні вищевказаних об'єктів. В першу чергу, це, безумовно, стосується судової комп'ютерно-технічної експертизи, яка в даний час являє собою клас судових експертиз, до якої входять: апаратно-комп'ютерна, програмно-комп'ютерна, інформаційно-комп'ютерна, комп'ютерно-мережева експертизи.

Також формується новий рід судових комп'ютерно-технічних експертиз 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. Другий – професійне виховання працівників служби криміналістики і досягнення ними такого рівня усвідомлення своєї відповідальності перед суспільством і законом, при якому не виникало б бажання скористатися довіреним програмним забезпеченням у незаконних цілях.

Розвиток цифрових технологій може суттєво змінити систему взаємодії органів розслідування. Служба криміналістики має бути не тільки оператором інформаційної системи кримінальної статистики, а й процесуальним керівником діяльності з виявлення, розслідування і розкриття злочинів і пред'явленню звинувачення. Слідчий-криміналіст повинен володіти можливостями доступу до матеріалів електронного кримінальної справи в режимі онлайн. Це дасть можливість на якісно новому рівні реалізовувати слідчим-криміналістом покладені на нього повноваження, пов'язані з як з кримінальним переслідуванням і контролем за діяльністю слідчих, так і більш ефективно реалізовувати інформаційну функцію, у випадках роботи зі скаргами і зверненнями громадян, ЗМІ тощо [1, с. 15-25].

Забезпечення інформаційної безпеки слідчого-криміналіста на базі цифрових технологій включене до загального прагнення створення у службі криміналістики та на необхідному рівні підтримування ефективної системи захисту інформації, здатної в кожному конкретному випадку з урахуванням специфіки діяльності визначити необхідну сукупність сил і засобів, а також заходів, які використовуються при вирішенні завдань щодо захисту інформації.

Однією з ключових складових реального процесу в рамках запропонованого методу управління інформаційною безпекою є персоналізація відповідальності користувачів, які отримали доступ до захищених інформаційних активів. Дана складова має здійснюватися в прив'язці до процесу управління інформаційною безпекою, а при роботі з персоналом увагу слід звернути на встановлення парольного захисту. Система інформаційної безпеки особистості слідчого-криміналіста у широкому та вузькому сенсі, що скадається з інформаційно-правової безпеки та інформаційно-психологічної безпеки. Забезпечення інформаційної безпеки слідчого-криміналіста є основою стійкості органів досудового розслідування, а службова інформація, що накопичується у службі криміналістики, стає важливим ресурсом, який необхідно захищати.

Мінімальні вимоги інформаційної безпеки зобов'язують керівника відділу криміналістики належним чином організувати контроль за тим, щоб з інформаційними системами працювали особи, які пройшли відповідну підготовку та ознайомлені з призначеної для користувача документації 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 по роботі 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, було оснащено необхідним не тільки загальносистемних, але і спеціальним програмним забезпеченням.

Інформаційна безпека повинна забезпечуватися єдиної комплексної програми, 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, в тому числі зразки для порівняльних досліджень [8, с. 194].

Механізм вчинення злочинів з використанням комп'ютерних технологій свідчить про те, що органам розслідування доводиться мати справу з новими видами цифрових слідів, їх локалізацією, знаходженням їх під різ-

ною юрисдикцією. Вивчення практики роботи слідчо-оперативних груп на місці злочину, при розслідуванні матеріалів конкретних кримінальних справ наочно демонструє, що трасологические, біологічні та інші традиційні сліди злочинів все більше і більше витісняються цифровими у вигляді даних стільникового зв'язку, відеоспостереження, IP, MAC, IMEI-адресами. Комп'ютерна інформація на електронних носіях все частіше і частіше використовується в якості речових доказів. Несвоєчасне правове врегулювання відносин у сфері боротьби з комп'ютерною злочинністю, суперечливість національного законодавства та відповідного термінологічного апарату в різних державах посилюють криміногенну обстановку і перешкоджають ефективну боротьбу з цим злом.

Паралельно необхідно розробляти і формувати нові інформаційно-технологічні криміналістичні рекомендації по тактиці підготовки та виробництва окремих слідчих дій, пов'язаних з виявленням, фіксацією, вилученням і дослідженням електронних слідів і їх матеріальних носіїв.

Методика розслідування злочинів у сфері комп'ютерної інформації та злочинів з використанням комп'ютерних технологій вимагає вдосконалення взаємодії слідчих-криміналістів з фахівцями з області інформаційних технологій та суміжних галузей знань, провайдерами зв'язку, інтернет-провайдерами тощо. Організаційні методи забезпечення інформаційної безпеки знаходять своє практичне застосування в діяльності керівництва правоохоронних органів взагалі і служби криміналістики зокрема, плануються і проводяться заходи забезпечення інформаційної безпеки об'єктів інформаційної інфраструктури, що містять інформацію, яка безпосередньо підлягає захисту [2, с. 19].

На перше місце в забезпеченні інформаційної безпеки виходить належне проведення організаційно-технічних заходів з питань захисту вже наявної інформації. Керівництво повинно взяти на себе обов'язок систематично контролювати кваліфікаційне відповідність кадрового складу, безпосередньо забезпечує інформаційну безпеку органу; адекватне технічне оснащення будівель і приміщень служби криміналістики, при необхідності звертаючись до допомоги фахівців з інших правоохоронних органів для проведення аудиту системи безпеки; загальну обстановку в колективі і діяльність кожного працівника зокрема з питань дотримання норм безпеки. Виходячи із специфіки діяльності обсяг відомостей, що становлять інформацію з обмеженим доступом, визначається керівниками. Керівник підрозділу служби криміналістики має право самостійно встановлювати правила роботи з такою інформацією, в тому числі призначати співробітників, які відповідальні за облік і зберігання документів, передачу документів в інші підрозділи.

Таким чином, ризик інформаційної безпеки стає інструментом для визначення наслідків реалізації загрози і має яскраво виражений кримінальний характер. Подібний підхід є прийнятним для організацій, що займаються комерційною діяльністю, основна мета яких це отримання прибутку. Однак в сформованих сучасних тенденціях розвитку інформаційних технологій, інформація, що відноситься до комерційної таємниці, є лише одним із видів конфіденційної інформації. У зв'язку з даними обставинами ризик-орієнтований підхід отримує протиріччя. Справа у тому, що в разі неможливості визначення вартості активу, оцінити втрати даного активу в кількісному еквіваленті неможливо. Прикладом такої інформації можуть бути: державна таємниця, персональні дані (інформація), професійна (службова, корпоративна) інформація, таємниця слідства, адвокатська таємниця, нотаріальна таємниця, таємниця судочинства. Дані види для кожної організації, а також носії їх містять, будуть захищеними інформаційними активами, при цьому захист такої інформації буде диктуватися не тільки побажаннями самої організації, але і відповідними законодавчими вимогами [3, с. 61]. Відповідно до загальноприйнятих підходів до інцидентів інформаційної безпеки, в рамках даного процесу виділяють ряд складових елементів, управління якими дозволяє найбільш ефективно забезпечувати управління інцидентами інформаційної безпеки в організації [3, с. 184]. В рамках проведення службового розслідування інциденту інформаційної безпеки повинні бути сформовані робочі групи для проведення розслідування, в складі яких повинні бути визначені права та обов'язки членів та керівників груп, порядок розслідування, критерії та правила взаємодії.

Для забезпечення ефективного захисту інформації повинні виконуватися наступні 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, знижують рівень ризиків; 4) здійснення контролю, підтримки і підвищення ефективності засобів управління безпекою, пов'язаних з активами організації [4, с. 162].

Огляд сучасних практик при формуванні безпечних паролів і доведення результатів огляду до відома співробітників є ключовим елементом при формуванні 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 в разі компрометації паролів. Нажаль, як ми бачимо, нині на концептуальному рівні відсутня розроблена система теоретико-методологічних засад забезпечення інформаційної безпеки служби криміналістики. Таким чином, враховуючи світовий досвід, вважаємо перспективним проект створення цифрової інформаційної мережі кабінетів криміналістики із застосуванням комп'ютерних технологій. При забезпеченні 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 [4, с. 133-134].

Криптографічна підсистема контролю можливостей для захисту документів у діяльності служби криміналістики класифікована на чотири рівні: 1 рівень) найвищий рівень контролю, достатній для захисту інформації з грифом «ОВ» («особливо важливо»); 2 рівень) достатній для забезпечення, яке використовується при захисті інформації з грифом «ЦТ» («цілком таємно»); 3 рівень) достатній для забезпечення, яке використовується при захисті інформації з грифом «С» («секретно»); 4 рівень) найнижчий рівень контролю, достатній для захисту конфіденційної інформації.

Одним з перспективних напрямків комп'ютерної інформації має стати інформаційно-технологічне забезпечення і розвиток електронної криміналістики, вивчення електронних документів як електронних доказів, які в майбутньому складуть електронну кримінальну справу. Отже, процес цифровізації служби криміналістики не зводиться лише до оцифрування відомостей: фактично мова йде про спроби створення штучного інтелекту, що передбачає розробку експертних систем і баз даних, вивчення методів і засобів отримання, уявлення, структурування і використання знань.

Висновки. Цифрова трансформація служби криміналістики – це процес корінного перетворення концепції і формату функціонування систем всіх 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, в цілях досягнення сталого і довгострокового існування в динамічних умовах цифрового простору. При розробці цільових програм інформаційного захисту потрібно застосовувати технологію, що передбачає облік (поряд з набором показників ефективності) принципів інформатизації й інтересів всіх категорій користувачів (прокурорів, слідчих, експертів, оперативних працівників), а також використовувати спеціалізований інтернет-портал і 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 напрямками слідчої роботи.

Для підвищення гарантій професійної діяльності слідчих-криміналістов необхідно впровадити нові тактики і методики забезпечення інформаційної безпеки служби криміналістики. Одним з інструментів забезпечення професійної надійності та безпеки слідчих-криміналістів є закріплення у проекті Законі «Про систему досудового слідства України та статус слідчих» нормативних положень, присвячених організаційно-правовому визначенню статусу, завдань, функцій та обсягу повноважень слідчого-криміналіста та кваліфікаційних вимог до осіб, які мають намір зайняти цю посаду.

ЛІТЕРАТУРА

1. Головко Л. В. Цифровизация в уголовном процессе: локальная оптимизация или глобальная революция? *Вестник экономической безопасности.* 2019. № 1. С. 15-25.

2. Жигулин Г. П. Организационное и правовое обеспечение информационной безопасности. СПб. : НИУ ИТМО, 2014. 173 с.

3. Исаев А. С. Метод и модель управления информационной безопасностью на основе динамических экспертных систем поддержки принятия решений : дис. … канд. техн. наук : 05.13.19 – Методы и системы защиты информации, инф. безопасность. СПб, 2015. 187 с.

4. Кармановский Н. С., Михайличенко О. В., Прохожев Н. Н. Организационно-правовое и методическое обеспечение информационной безопасности. СПб. : ИТМО, 2016. 148 с.

5. Кучинский В. Ф. Сетевые технологии обработки информации. СПб. : ИТМО, 2015. 115 с.

6. Майорова Е. В., Черток А. В. Использование методов форензики при расследовании инцидентов компьютерной безопасности. *Технико-технологические проблемы сервиса (СПбГЭУ).* 2019. № 4 (50). С. 36-41.

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

8. Россинская Е. Р. Теория информационно-компьютерного обеспечения криминалистической деятельности : концепция, система, основные закономерности. *Вестник Вост.-Сиб. ин-та МВД РФ.* 2019. № 2. С.193-202.

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

10. Смушкин А. Б. О природе электронной цифровой криминалистики. *Lex russica.* 2020. Т. 73. № 6. С. 110-121.