TOPICALITY OF FORENSIC MOLECULAR GENETIC EXAMINATION AND ISSUES REGARDING ITS PERFORMING

Topchiy V. V.

Modern progress in forensic molecular genetic examination allow to obtain information about a particular person using traces variety of biological origin especially while committing grave crimes against human life and health, that are usually found at the scene and belong to a human body. A significant advantage of this method under crime investigation is precisely the safe exclusion of suspected persons not involved in the commission of a crime, in identifying those who committed a crime with a high probability level. At the present stage of forensic molecular genetic examination development there are significant gaps in legislation that are solved by adopting relevant normative and legal acts and improving existing ones. Effective method for of DNA analysis development is the creation of appropriate bases of genetic features of a person. However, the legislative consolidation of this process should take place in the context of respecting and protecting personal rights. However, terms of performing molecular genetic examination significantly exceed the terms of pre-trial investigation. This problem can be solved by expanding network of laboratories that perform such examination. Despite presence of a small number of problems, it is possible to affirm that DNA analysis is the most effective and reliable of all known methods of person identification at the present stage. At present, expert molecular genetic analysis develops not only as a section of molecular genetic research but also as a complete element of criminalistic knowledge that is aimed at investigating and disclosing crimes. Therefore, implementation of molecular genetic research methods into the practice of law enforcement agencies in Ukraine will significantly increase investigation effectiveness of many serious crimes against person.

Keywords: DNA analysis, molecular genetic examination, identification, genotype profiling, criminal proceedings.

DOI: https://doi.org/10.32353/khrife.2018.29
УДК 343.98

А. А. Русецький, провідний науковий співробітник Харківського НДІСЕ, кандидат юридичних наук, доцент
E-mail: hniise@gov.ua

МІСЦЕ СУДОВИХ ЕКСПЕРТИЗ У СИСТЕМІ ПРОТИДІЇ КІБЕРЗАГРОЗАМ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Здійснено аналіз наукових думок щодо змісту протидії кіберзагрозам у сфері інформаційної безпеки України, визначено місце й функції судової експертизи в цій діяльності. Уточнено зміст експертної профілактики та з'ясовано функції-завдання, що вирішуються під час виявлення злочинів із втручання в роботу інформаційно-телекомунікаційних систем. Надано рекомендації щодо напрямів здійснення наукових досліджень для формування теоретичного підґрунтя використання судових експертиз у протидії кіберзагрозам.

Ключові слова: кіберзагрози, інформаційна безпека, шкідливе програмне забезпечення, протидія злочинам, комп'ютерно-технічна експертиза, несанкціоноване втручання в роботу інформаційно-телекомунікаційних систем.

XXI ст. ознаменувалося швидким розвитком нанотехнологій та Інтернету, що стало підґрунтям формування сучасного інформаційного суспільства. Як наслідок з'явилися новітні види злочинної діяльності, що формують низку загроз національній безпеці особливо в інформаційній сфері. Означене потребує впровадження новітніх методів виявлення та документування злочинів, побудови відповідної системи протидії злочинності з визначенням усіх її елементів.

Підґрунтям будь-якої системи протидії злочинності є виявлення правових і організаційних передумов загроз із зіставленням функцій-завдань, що вирішуються на кожному етапі протидії злочинам.

Вивчення праць науковців 90-х років минулого століття показало, що на етапі формування самостійної української держави активізувалися наукові дослідження з фундаментально-прикладних проблем судової експертизи та щодо її місця в протидії злочинній діяльності. Проблемами експертної профілактики займалися І. А. Алієв, Д. П. Гуріна, Ю. С. Сушко[1] та ін. Ними були започатковані концептуальні підходи до профілактичної діяльності під час здійснення судових експертиз різних видів.

У наукових статтях початку XXI ст. проблеми протидії злочинності з використанням судової експертизи розглядалися в контексті профілактики злочинів під час здійснення конкретних судових експертиз. Аналіз робіт того часу дозволяє визначити, що змістом експертної профілактики є встановлення на підставі спеціальних знань фактів, що містять дані про обставини події, які сприяли вчиненню злочину (правопорушенню), і трансформації цих даних через вольові акти правочинних осіб із кінцевою метою ліквідації цих обставин у сьогоденні та майбутньому або доведення їх до мінімуму[2]. Аналогічної думки дотримується низка науковців. Вони вважають, що судова експертиза належить до діяльності, під час якої встановлюються причини й умови вчинення конкретних злочинів. Ураховуючи пануючі серед науковців і практиків думки щодо змісту боротьби та протидії злочинності, можна констатувати, що судова експертиза виконує загальні та спеціальні завдання, а не тільки з профілактики злочинів. Отже, експертна профілактична діяльність – це складова протидії злочинам, що полягає у використанні спеціальних знань, спрямованих на удосконалення теорети-

[1] *Алиев И. А.* Проблемы судебно-экспертной профилактики : дис. … д-ра юрид. наук. Киев, 1990; *Гуріна Д. П.* Експертна профілактика: становлення та перспективи розвитку : автореф. дис. ... канд. юрид. наук : 12.00.09. Київ, 2009. 16 с.; *Сушко Ю. С.* Актуальні проблеми профілактичної діяльності при проведенні судово-економічних експертиз : автореф. … канд. юрид. наук : 12.00.09. Київ, 1994. 25 с.

[2] *Бордюгов Л. Г.* Профілактична функція судової екологічної експертизи. URL: http://nauka.kushnir.mk.ua/?p=43758/ (дата звернення: 25.07.2018).

ко-правових, організаційно-тактичних основ проведення оперативно-розшукових, негласних слідчих (розшукових) дій та інших заходів із метою виявлення й усунення обставин учинення кримінальних та інших правопорушень.

Переважна більшість наукових досліджень на здобуття наукового ступеня доктора та кандидата юридичних наук зі спеціальності «судова експертиза» після прийняття Кримінального процесуального кодексу 2012 р. були спрямовані на створення системи експертного забезпечення в цілому в кримінальному процесі та під час досудового розслідування кримінального провадження. Так, на думку І. В. Пирога, до концептуальних основ судової експертології входить експертна профілактика[1]. О. Р. Россинська виокремлює профілактику як форму судово-експертної діяльності, що пов'язана з використанням результатів проведених експертиз у профілактиці злочинів, адміністративних і громадських правопорушень[2]. Однак вона не конкретизує організаційно-тактичний алгоритм використання результатів проведених експертиз у профілактиці злочинів.

Наступним напрямом застосування результатів експертної діяльності в профілактиці злочинів, на думку І. В. Пирога та В. Ю. Шепітька, є використання технічних і експертних засобів із попередження злочинів сьогодні[3]. Аналіз поглядів означених науковців свідчить, що є декілька таких напрямів, починаючи з розроблення запобіжних засобів до використання інтелектуальних експертних систем пошуку та аналізу аудіо-, відеоінформації.

Низка робіт М. Г. Щербаковського присвячена проблемам використання судової експертизи в кримінальному процесі, а також реалізації її профілактичної функції[4].

На наш погляд, судова експертиза в умовах сьогодення є методологічним підґрунтям не тільки досудового розслідування кримінального провадження, а й інших стадій протидії злочинності: отримання первинної інформації про кримінальну активність; загальна та спеціальна профілактика, виявлення й припинення злочинів. Особливо це стосується формування методичних рекомендацій щодо проведення негласних слідчих (розшукових) дій, а саме:

— отримання інформації з транспортних телекомунікаційних мереж (ст. 263 КПК України);

---

[1] *Пиріг І. В.* Теоретичні основи експертного забезпечення досудового розслідування : дис. … д-ра юрид. наук : 12.00.09. Харків : ХНУВС, 2015. С. 24.

[2] *Россинская Е. Р.* Общая теория судебной экспертизы и криминалистика как самостоятельные родственные науки. URL: http://rossinskaya.ru/articles/ (дата звернення: 25.07.2018).

[3] *Шепитько В. Ю.* О новеллах в использовании специальных знаний в уголовном процессе Украины. *Теория и практика судебной экспертизы в современных условиях* : материалы 4-й Междунар. науч.-практ. конф., Москва, 30–31 янв. 2013 г. Москва : Проспект, 2013. С. 340–342.

[4] *Щербаковський М. Г.* Теоретико-методологічні та праксеологічні засади судових експертиз у кримінальному процесі : автореф. дис. … д-ра юрид. наук : 12.00.09. Харків, 2016. 34 с.

— отримання інформації з електронних інформаційних систем (ст. 264 КПК України);

— обстеження публічно недоступних місць, житла чи іншого володіння особи (ст. 267 КПК України);

— негласне отримання зразків, необхідних для порівняльного дослідження (ст. 274 КПК України).

Як убачається з аналізу наукових розробок у галузі судової експертизи, в переважній більшості робіт розглядаються проблемні питання використання висновків і результатів судових експертиз у профілактиці злочинів. На наш погляд, такий підхід є однобічним. Логіка побудови новітньої моделі протидії злочинності передбачає використання результатів експертної діяльності на всіх стадіях протидії злочинам, що забезпечить формування її проактивного характеру.

Ураховуючи завдання протидії злочинності взагалі та профілактики злочинів зокрема, можемо запропонувати форми використання результатів і засобів судової експертизи в протидії злочинам у сфері інформаційної безпеки відповідно до вимог законодавства й змісту інформаційної безпеки та існуючих загроз із боку злочинного середовища.

Виходячи зі змісту ст. 1 Закону України «Про судову експертизу», судова експертиза полягає в дослідженні експертом на основі спеціальних знань у галузі науки, техніки, мистецтва, ремесла тощо об'єктів, явищ і процесів із метою надання висновку з питань, що є або будуть предметом судового розгляду[1]. Отже, щоб провести дослідження, експерт повинен володіти низкою спеціальних знань, що визначаються конкретними видами злочинів, на встановлення фактів учинення яких спрямована експертиза. Стосовно використання судової експертизи щодо протидії кіберзагрозам у сфері інформаційної безпеки необхідно з'ясувати її зміст.

Відповідно до теоретичної парадигми інформаційної безпеки вона є предметом регулювання нормативних актів різного рівня. Так, у ст. 17 Конституції України наголошується, що захист суверенітету й територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу. Отже, однією з основних функцій-завдань держави є створення ефективного механізму виявлення та нейтралізації загроз інформаційній безпеці України.

У ст. 1 Закону України «Про національну безпеку України» визначається необхідність прийняття Державної стратегії кібербезпеки України, у якій потрібно передбачити загрози кібербезпеці України, пріоритети та напрями її забезпечення з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства й держави[2].

---

[1] Про судову експертизу : Закон України від 25.02.1994 № 4038-XII. *Відом. Верхов. Ради України.* 1994. № 28. Ст. 232.

[2] Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. URL: http://zakon0.rada.gov.ua/laws/show/2469-19 (дата звернення: 25.07.2018).

Означені нормативні акти були прийняті відповідно до підписаної 23 листопада 2001 р. в Будапешті Конвенції Ради Європи про кіберзлочинність (далі – Конвенція)[1]. Ця Конвенція сприяла формуванню системи координації діяльності правоохоронних органів країн Європи в протидії комп'ютерним злочинам і криміналізації дій расистського та ксенофобного характеру, учинених через комп'ютерні системи. Визначити правові та організаційні чинники кожного структурного елемента протидії злочинності взагалі та кіберзлочинності зокрема можна завдяки з'ясуванню її теоретико-прикладного змісту. Крім того, вимогою Конвенції було вдосконалення національного законодавства у сфері забезпечення інформаційної безпеки відповідно до вимог світових стандартів забезпечення суспільних інтересів, прав і свобод людини.

Ураховуючи норми Конвенції, у чинній Доктрині інформаційної безпеки України основні національні інтереси України в інформаційній сфері поділено на життєво важливі інтереси особи та життєво важливі інтереси суспільства й держави. Першу групу складають: забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації; забезпечення конституційних прав людини на захист приватного життя; захищеність від руйнівних інформаційно-психологічних впливів[2].

Другу групу складають: усебічне задоволення потреб громадян, підприємств, установ і організацій усіх форм власності в доступі до достовірної та об'єктивної інформації; розвиток і захист національної інформаційної інфраструктури; формування ефективної правової системи захисту особи, суспільства та держави від деструктивних пропагандистських впливів; безпечне функціонування й розвиток національного інформаційного простору та його інтеграція у європейський і світовий інформаційний простір; забезпечення розвитку інформаційно-комунікаційних технологій, інформаційних ресурсів України та ін.

Ураховуючи означені правові акти та спираючись на аналіз думок науковців у сфері інформаційного безпеки, можна виокремити основні види загроз національній безпеці в інформаційній сфері:

— комп'ютерна злочинність;

— інформаційний тероризм;

— розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб і національних інтересів суспільства й держави;

---

[1] Про ратифікацію Конвенції про кіберзлочинність : Закон України від 07.09.2005 № 2824-IV. *Відом. Верхов. Ради України*. 2006. № 5. Ст. 71.

[2] Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України : Указ Президента України від 25.02.2017 № 47/2017. URL: https://www.president.gov.ua/documents/472017-21374 (дата звернення: 25.07.2018).

— намагання маніпулювати громадською думкою, зокрема шляхом поширення недостовірної, неповної або упередженої інформації;

— прояви обмеження свободи слова й доступу громадян до інформації та інших їх прав і свобод;

— поширення в засобах масової інформації культу насильства, жорстокості, порнографії та інших проявів аморальності;

— поширення ідеологій і впливу деструктивних неокультів;

— небезпечне для економічної незалежності України зростання частки іноземного капіталу в стратегічних галузях економіки, пов'язаних з інформаційною сферою;

— інспірування інших деструктивних процесів в інформаційній сфері нашої держави[1].

Означені загрози трансформуються в конкретні злочини, що визначають організаційно-тактичні особливості здійснення всіх складових протидії, у тому числі проведення відповідних експертиз. Аналіз криміногенної ситуації у сфері кіберпростору свідчить, що тільки за шість місяців 2018 р. органами кіберполіції виявлено 2,3 тис. правопорушень у цій сфері. Найбільш розповсюдженими протиправними діями є несанкціоновані втручання в роботу інформаційно-телекомунікаційних систем (ІТС). У ході проведення оперативно-розшукових заходів (ОРЗ) і негласних слідчих (розшукових) дій (НС(Р)Д) під час кримінального провадження оперативні працівники та слідчі повинні володіти прийомами виявлення означених протиправних дій і об'єктів, що можуть бути предметом досліджень. Теоретичним підґрунтям таких прийомів повинні бути експертні висновки та рекомендації відповідних методик на ґрунті праць таких науковців, як Ю. В. Гаврилін, В. А. Голубєв, С. М. Гусаров, В. О. Вітюк, О. П. Войтович, В. А. Каплун, В. В. Крилов, Л. М. Соловйов, Т. Л. Тропіна, В. С. Цимбалюк та ін. Однак питання визначення понятійного апарату в цій сфері досліджено неповною мірою[2].

Аналіз наукових розробок останніх років свідчить, що складність узагальнення емпіричного матеріалу полягає в тому, що методики виявлення таких втручань із використанням шкідливих програмних засобів (ШПЗ) мають закритий характер і переважно розробляються відповідними підрозділами СБУ[3]. Однак значна кількість комп'ютерно-технічних експертиз

[1] Загрози національній безпеці держави в інформаційній сфері. URL: https://pidruchniki.com/1834071936975/politologiya/ (дата звернення: 25.07.2018).

[2] *Парфиро О. А., Нізовцев Ю. Ю.* Актуальні питання судово-експертного дослідження шкідливих програмних засобів у межах протидії кібертероризму. *Криміналістичний вісник*. 2016. № 1 (25). С. 78–84. URL: elar.naiau.kiev.ua/bitstream/ (дата звернення: 25.07.2018).

[3] *Нізовцев Ю. Ю.* Щодо проблем притягнення до кримінальної відповідальності осіб за незаконні дії зі спеціальними програмними засобами негласного отримання інформації. *Правове забезпечення оперативно-службової діяльності: актуальні проблеми та шляхи їх вирішення* : матеріали постійно діючого наук.-практ. семінару, Харків, 27 трав. 2016 р. Харків : Право, 2016. Вип. 7. С. 301–304.

здійснюється співробітниками відповідних лабораторій науково-дослідних установ судових експертиз Міністерства юстиції України.

На сьогодні нормативно-правові акти, що стосуються забезпечення кібербезпеки в Україні, мають низку неузгодженостей щодо понятійно-термінологічного апарату особливо стосовно конкретних видів об'єктів судової експертизи, ознак несанкціонованих утручань у роботу ІТС; рекомендацій щодо пошуку, виявлення, фіксації та вилучення цих об'єктів.

Вивчення наукових здобутків у сфері використання судових експертиз за фактами несанкціонованих утручань у роботу ІТС дозволяє визначити, що для забезпечення формування ефективних організаційно-тактичних моделей ОРЗ – НС(Р)Д щодо виявлення таких протиправних дій шляхом віддалених атак за допомогою ШПЗ необхідно закріпити в експертних методиках класифікацію таких несанкціонованих утручань і класифікацію ШПЗ із визначенням характерних ознак кожного способу віддаленої атаки на відмову в обслуговуванні та ознак ШПЗ.

Аналіз наукових праць експертів СБУ свідчить, що на сьогодні відсутня єдина думка щодо визначення терміна «шкідливий програмний засіб» і як наслідок відсутність єдиного підходу до проведення судових експертиз для виявлення ознак їх застосування. З означеного можемо констатувати, що в різних випадках судові експерти роблять висновки, спираючись на власний розсуд, знання та практичний досвід, і як наслідок різні експерти можуть зробити різні висновки.

Вивчення досвіду кіберполіції НП України та СБУ дозволяє визначити, що одним із розповсюджених злочинів із використання ШПЗ є викрадення конфіденційних даних[1].

На сьогодні відсутні сучасні методики визначення конкретних програмних засобів ШПЗ. Як наслідок, відсутні уніфікація методик і розробки на їх підґрунті рекомендацій для слідчих та оперативних працівників щодо проведення ОРЗ – НС(Р)Д із метою виявлення об'єктів, що мають ШПЗ, і визначення питань, які необхідно вирішити під час проведення судових експертиз.

З наведеного можемо констатувати, що:

— протидія злочинам у сфері інформаційної безпеки структурно складається з таких стадій: пошук первинної інформації про злочинну активність в інформаційній сфері; профілактика кіберзлочинів; виявлення протиправних дій у сфері інформаційної безпеки під час оперативно-розшукового провадження та здійснення ОРЗ; досудове розслідування кримінального провадження та здійснення НС(Р)Д у його межах;

— судова експертиза є важливою складовою системи протидії злочинам у сфері інформаційної безпеки та методологічним підґрунтям формування організаційно-тактичної моделі оперативно-розшукового та кримінального провадження;

[1] Кіберполіція викрила працівника вишу, який розповсюджував ШПЗ та займався майнінгом криптовалюти за рахунок державного університету. URL: https://cyberpolice.gov.ua/news/ (дата звернення: 09.02.2018).

— протидія кіберзагрозам у сфері інформаційної безпеки в Україні повинна ґрунтуватися на системно-комплексному підході до використання всіх структурних елементів правоохоронної системи, координації всіх суб'єктів, у тому числі й судових експертів, з відповідною розробкою науково-обґрунтованих ефективних методів попередження, виявлення та розслідування злочинів;

— теоретичним підґрунтям формування системного підходу до протидії злочинам у цій сфері є здійснення наукових досліджень у теоретико-прикладних галузях юридичної науки: криміналістиці, теорії судової експертизи, теорії оперативно-розшукової діяльності, теорії розвідки та контррозвідки.

МЕСТО СУДЕБНЫХ ЭКСПЕРТИЗ В СИСТЕМЕ ПРОТИВОДЕЙСТВИЯ КИБЕРУГРОЗАМ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УКРАИНЫ

Русецкий А. А.

Проанализированы теоретические разработки и практический опыт противодействия киберугрозам в сфере информационной безопасности Украины. Определено, что противодействие преступлениям в сфере информационной безопасности структурно состоит из нескольких стадий. К ним относятся: поиск первичной информации о преступной активности в информационной сфере; профилактика киберпреступлений; выявление противоправных действий в сфере информационной безопасности в ходе оперативно-розыскных мероприятий и досудебного расследования уголовного производства. Наиболее распространенными противоправными действиями в сферы информационной безопасности являются несанкционированные вмешательства в работу информационно-телекоммуникационных систем. Для выявления этих преступлений во время проведения оперативно-розыскных мероприятий в рамках уголовного производства оперативные работники и следователи должны владеть приемами обнаружения указанных противоправных действий и объектов, которые могут быть предметом исследований. Теоретическими основами рекомендаций по поиску, обнаружению, фиксации и изъятию этих объектов должны быть соответствующие криминалистические методики. Правовым основанием формирования таких методик должны быть законодательные и ведомственные нормативные акты. Однако в ряде нормативно-правовых актов, имеющих отношение к обеспечению кибербезопасности в Украине, есть несогласованности понятийного аппарата, особенно в отношении конкретных видов объектов судебной экспертизы, признаков несанкционированных вмешательств в работу информационно-телекоммуникационных систем. Выяснено, что противодействие киберугрозам в сфере информационной безопасности в Украине должно основываться на системно-комплексном подходе к использованию всех структурных элементов, координации деятельности его субъектов, в том числе и судебных экспертов. Теоретическим основанием формирования системно-комплексного подхода противодействия преступлениям в этой сфере является осуществление науковедческих исследований теоретико-прикладных отраслей юридической науки: криминалистики, теории судебной экспертизы, теории оперативно-розыскной деятельности.

Ключевые слова: киберугрозы, информационная безопасность, вредоносное программное обеспечение, противодействие преступлениям, компьютерно-техни-

ческая экспертиза, несанкционированное вмешательство в работу информационно-телекоммуникационных систем.

PLACE OF FORENSIC SCIENCE IN THE CYBERTHREATS PREVENTION SYSTEM IN FIELD OF A UKRAINIAN INFORMATION SECURITY

Rusetskyi A. A.

Theoretical developments and practical experience of countering cyberthreats in the field of information security of Ukraine are analyzed. It is determined that the crime prevention in the field of information security is structurally composed of several stages. They include: search for primary information on criminal activity in the information field ; prevention of cybercrime; detection of illegal actions in the field of information security while operative investigative activities and pre-trial investigation of criminal proceedings. The most common illegal actions in the field of information security is unauthorized tampering in the work of information and telecommunications systems. In order to identify these crimes during operative investigative activities within the criminal procedure operational officers and investigators must possess methods of detecting specified illegal actions and objects that can be subject to research. Theoretical bases of recommendations for search, detection, fixation and seizure of these facilities should be appropriate criminalistic methods. Legal basis for the formation of these methods should be legislative and departmental regulatory acts. However, in a number of normative legal acts related to ensuring cybersecurity in Ukraine, there are inconsistencies in the conceptual apparatus, especially with regard to specific object types of forensic science, signs of unauthorized tampering in the work of information and telecommunications systems. It was found out that counteraction to cyberthreats in the field of information security in Ukraine should be based on a system integrated approach to use of all structural elements, coordination of its subject activities including forensic experts. The theoretical basis for the formation of a system integrated approach to crime prevention in this field is the implementation of research on research of theoretical applied branches of jurisprudence: criminalistics, theory of forensic science, theory of operative investigative activities.

Keywords: cyberthreats, information security, harmful software, crime prevention, computer forensic examination, unauthorized tampering in the work of information and telecommunication systems.

DOI: https://doi.org/10.32353/khrife.2018.30
УДК 343.98

Н. Є. Філіпенко, провідний науковий співробітник Харківського НДІСЕ, кандидат юридичних наук, доцент
E-mail: filipenko_natalia@ukr.net

ІНФОРМАЦІЙНІ СИСТЕМИ В СУДОВО-ЕКСПЕРТНІЙ ДІЯЛЬНОСТІ

(оглядова стаття)

Розглянуто теоретичні проблеми використання інформаційних систем у судово-експертних дослідженнях. Проаналізовано позиції та підходи вчених до визначення поняття й сутності теоретичної категорії «інфор-