УДК 343.98:343.45

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ У НЕЗАКОННІЙ ІНСАЙДЕРСЬКІЙ ДІЯЛЬНОСТІ (КРИМІНАЛІСТИЧНИЙ АСПЕКТ)

Г. І. Резнікова, кандидат юридичних наук, науковий співробітник лабораторії «Використання сучасних досягнень науки і техніки у боротьбі зі злочинністю» Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України, м. Харків

Інформатизація світового співтовариства наприкінці XX–XXI ст., постійне оновлення інформаційних технологій (далі – ІТ) детермінували формування глобального інформаційного простору, поставивши перед правоохоронними органами України актуальне завдання – забезпечити інформаційну безпеку особи, суспільства та держави, зокрема, від кримінальних правопорушень, якими незаконно розголошується інформація з обмеженим доступом, яка становить предмет різних професійних таємниць. Утім, проблеми з’ясування ролі ІТ у процесі розголошення професійних таємниць в Україні не розглядались. Кримінальне процесуальне, кримінально-правове та криміналістичне забезпечення таємниць в Україні розглядались О. Є. Радутним, С. М. Логіновою, В. Г. Лісогором, А. О. Шаповаловою, Є. В. Кузьмічовою та ін.[1] Отже, криміналіс-

[1] Див.: Радутний О. Е. Кримінальна відповідальність за незаконне збирання, використання та розголошення відомостей, що становлять комерційну або банківську таємницю : монографія / О. Е. Радутний. – Х. : Ксілон, 2008. – 202 с.; Логінова С. М. Адвокатська таємниця: теорія та практика : автореф. дис. … канд. юрид. наук : 12.00.10 / С. М. Логінова ; Київ. нац. ун-т ім. Тараса Шевченка. – К., 2002. – 19 с.; Лісогор В. Г. Криміналістичне забезпечення збереження таємниці досудового слідства : наук.-практ. посіб. / В. Г. Лісогор. – Д. : Юрид. акад. МВС, 2005. – 156 с.; Кузьмічова Є. В. Охорона лікарської таємниці у кримінальному процесі України : автореф. дис. … канд. юрид. наук : 12.00.09 / Є. В. Кузьмічова ; Держ. подат. служба України, Нац. ун-т держ. подат. служби України. – Ірпінь, 2012. – 19 с.; Шаповалова А. О. Забезпечення охорони банківської таємниці у криміналь-

тичне вивчення ролі ІТ у незаконній інсайдерській діяльності становить актуальне завдання.

Розголошення професійних таємниць як прояв психологічної взаємодії осіб здійснюється у процесі спілкування між учасниками (у широкому сенсі). Спілкування – це процес передачі інформації, здійснення якого включає відправника інформації, канал передачі інформації та отримувача інформації [1, с. 46]. Механізм прийому та передачі інформації на фізіологічному рівні, пише В. В. Крилов, обмежений здібностями людини, які дозволили винайти та застосовувати технічні та енергетичні системи, що реалізують функції пристроїв передачі інформації [1, с. 45–46]. Отже, інформаційні канали поділяються на анатомо-фізіологічні та технічні. Відповідно розголошення таємниці може відбуватися як у безпосередньому спілкуванні за допомогою анатомо-фізіологічних засобів, так й опосередковано за допомогою технічних засобів і носіїв інформації.

Інформатизація суспільства вплинула на обрання інсайдерами способів реалізації злочинної мети, знарядь і засобів розголошення інформації з обмеженим доступом та детермінувала появу нових слідів злочину. Інформаційні технології (від англ. Information Technology, IT) – це процес, що використовує сукупність засобів і методів збору, накопичення, обробки та передачі даних (первинної інформації) для отримання інформації нової якості про стан об'єкта, процесу або явища. ІТ – це комп'ютерні технології, пов'язані з використанням комп'ютерів і програмного забезпечення для зберігання, перетворення, захисту, обробки, передачі та отримання інформації [2]. ІТ включають ресурси, які необхідні у процесі керування інформацією – комп'ютери, програмне забезпечення та мережі, що використовують для створення, зберігання, передачі та пошуку інформації [3, с. 182]. А. М. Ішин наголошує, що слушним є термін «нова» ІТ, оскільки він відображає в її структурі технології, які засновані на використанні як комп'ютерів, так й інших засобів, що забезпечують телекомунікацію [3, с. 182]. Засоби зв'язку та ЕОМ становлять технічну базу процесу збору, обробки, накопичення та розповсюдження інформації [1, с. 14–15], що активно залучається інсайдерами.

ному процесі України : автореф. дис. … канд. юрид. наук : 12.00.09 / А. О. Шаповалова ; Київ. нац. ун-т внутр. справ. – К., 2009. – 20 с.; та ін.

Використання ІТ є необхідним атрибутом професійної придатності особи у суспільстві [3, с. 183]. А це впливає на видозміну обстановки розголошення професійних таємниць, розширення діапазону способів готування, вчинення та приховування, перелік доступних інсайдерам знарядь і засобів учинення злочинів. Водночас це обумовлює продуктивність та завуальованість злочинної діяльності для слідчих працівників правоохоронних органів [4, с. 125]. Є. П. Іщенко зауважує, що насиченість сучасного життя комп'ютерними системами, телекомунікаціями, віртуальною дійсністю не лише видозмінює злочинність, а й відкриває нові можливості у боротьбі з нею [5, с. 6–15]. Зауважимо, що вихід з обігу окремих програм, призначених для ЕОМ, машинних носіїв і засобів обробки інформації, та їх п'ятдесятивідсоткова заміна новою технікою відбувається один раз на один – два роки [6, с. 224]. Отже, виокремимо найбільш типові засоби і знаряддя розголошення таємниць, установлення яких має значення у процесі пошуку криміналістично значущої інформації про обставини кримінального правопорушення.

Здійснення професійної діяльності у різних сферах суспільного життя передбачає використання персонального комп'ютера (ЕОМ) як на етапі створення інформації, так і на етапі її обробки та використання. У результаті утворюється специфічний об'єкт «комп'ютерна інформація», що існує в електронному просторі та сприймається людиною за допомогою комп'ютера [1, с. 115–116] і периферійних пристроїв. Комп'ютер і програмне забезпечення можуть бути предметом та інструментом злочинної діяльності або сховищем чи інструментом обробки інформації щодо злочину [1, с. 225]. Поширеними способами розголошення таємниць є передача, розповсюдження та демонстрування сторонній особі документів (у широкому сенсі), які містять інформацію з обмеженим доступом, зокрема, письмові, фото-, відео- та електронні документи. Мають місце дії з підготовки до злочину, оскільки особа вдається до операцій з копіювання документа або ж його роздрукування, якщо таємниця відображена в електронний спосіб. У процесі підготовки, вчинення та приховування злочину інсайдер застосовує ЕОМ і периферійні пристрої, зокрема, пристрої вводу (сканер, цифрові фото- та відеокамери), виводу ін-

формації (монітори, проектори, принтери), зберігання інформації (диски CD-R/RW, DVD-R/RW, flash-накопичувачі тощо).

Розголошення професійних таємниць шляхом передачі документів або машинних носіїв інформації передбачає попередні підготовчі дії з копіювання та запису комп'ютерної інформації, що становить таємницю, на певний носій (паперовий, електронний). Нерідко інсайдер як засіб учинення злочину застосовує копіювально-розмножувальні апарати (наприклад, «Xerox», «Canon» тощо), які дозволяють швидко роздрукувати копію документа. Крім того, для незаконного копіювання інформації інсайдери використовують можливості ЕОМ і відповідного програмного забезпечення. Копіювання електронної інформації, що становить предмет таємниці, може здійснюватися з пам'яті ЕОМ на певний машинний носій інформації чи за допомогою знімка екрана (скріншоту), який утворюється завдяки можливостям операційних систем ЕОМ, програмних засобів або зовнішніх пристроїв. Стрімкого поширення набула практика копіювання інформації, що становить таємницю, за допомогою цифрових фотокамер і смартфонів. Цифрові зображення об'єктів можна одразу оглянути, роздрукувати, передати на значні відстані або швидко виготовити необмежену кількість копій [7, с. 88]. За допомогою цифрових фотоапаратів інформація відтворюються в електронному просторі – у пам'яті цифрового фотоапарату або картах пам'яті (зокрема, xD Picture Card) [7, с. 88] і може бути скопійована до пам'яті ЕОМ. Використання ПК, їх програм і периферійних пристроїв надає можливість проводити судові експертизи. Механізм утворення цифрових слідів має враховуватися, пише В. В. Білоус, під час проведення таких криміналістичних експертиз: технічної експертизи документів при встановленні, зокрема, чи виготовлений документ шляхом монтажу із застосуванням комп'ютерної та копіювально-розмножувальної техніки; ідентифікації особи, яка надрукувала текст з використанням програмного забезпечення, за особливостями навичок виконавця; встановлення типу й ідентифікації комп'ютерної техніки за виготовленим за її допомогою документом; експертизи відеозапису та фототехнічної експертизи при вирішенні завдань ідентифікації апаратури за файлами фото-, відеозаписів тощо [8, с. 427].

Великий обсяг комп'ютерної інформації, що складає предмет таємниці, спонукає інсайдерів до її копіювання на машинні носії. Особа на технічному рівні, використовуючи комп'ютер, копіює інформацію на певний пристрій її зберігання – лазерні накопичувачі (CD-R, RW, DVD-R, RW) або на флеш-пам'ять, які у подальшому передаються сторонній особі й використовуються злочинцем як засіб учинення злочину. Флеш-пам'ять (або USB Flash Drive) є найбільш вживаною у процесі незаконного зберігання інформації з обмеженим доступом через її ємність, швидкість передачі даних і компактність носія. Носії електронної інформації є ключовим елементом комп'ютерних об'єктів, оскільки є місцем знаходження предмета посягання – інформації під час учинення злочинів [5, с. 6–15].

ПК може бути засобом і знаряддям учинення інсайдером злочину. ЕОМ є знаряддям злочину, коли розголошення таємниці здійснюється шляхом демонстрування особі за допомогою ПК документів (електронних, цифрових фото- та відеодокументів). Знаряддями виступають також стільникові (мобільні) телефони, смартфони (комунікатори), портативні ЕОМ (лептопи, ноутбуки тощо). Портативні комп'ютери – це малогабаритні переносні комп'ютери, які обирають інсайдери через їх портативність і компактність, що забезпечує можливість роботи з ними в будь-якому місці за рахунок компактних джерел живлення.

Програмне забезпечення та комп'ютерні мережі теж стають знаряддями та засобами розголошення таємниць. Значущим є питання щодо типів інформаційних повідомлень, що передаються через системи і мережі ЕОМ, оскільки розголошення таємниць відбувається шляхом надсилання електронних документів або повідомлень стороннім особам. Розголошення таємниць шляхом надсилання електронних повідомлень (електронної пошти), що містять інформацію з обмеженим доступом, передбачає використання комп'ютерів, комп'ютерних мереж (локальних, глобальних) і програмних засобів (наприклад, «Fox-mail», «Microsoft Outlook» тощо). Електронна пошта використовується не лише у процесі інформаційного обміну між злочинцями, а й як засіб учинення злочину. Сліди передачі інформації можуть бути виявлені у вигляді текстових

файлів на ЕОМ абонентів, а також можуть перебувати певний час у копіях на поштовому сервері адміністратора, звідки їх слід вилучати [5, с. 124]. Інформація щодо комп'ютерної мережі, яка стала знаряддям учинення злочину й несе на собі електронні сліди, може бути використана для виявлення злочину та обставин події. Так, слідчий зможе встановити провайдера послуг Інтернет, місце знаходження робочої станції та особу абонента – користувача, з якою укладено договір при виокремленні абонентського номера чи коду ідентифікації для надання послуг [5, с. 6–15].

Наразі існують різні мережі передачі даних, під якими розуміють сукупність кінцевих пристроїв (терміналів) зв'язку, що об'єднані каналами передачі даних, і комутуючі пристрої (вузли мережі), що забезпечують обмін повідомленнями між усіма кінцевими пристроями. Поширеними видами сучасного зв'язку є телефонний зв'язок, комп'ютерна телефонія, радіотелефонний зв'язок, мережі стільникового радіозв'язку та системи стандарту Wi-Fi. Комп'ютерна телефонія та стільниковий зв'язок активно використовуються інсайдерами. Мобільний телефон – це мініатюрна приймально-передавальна станція, що оснащена процесором із необхідним обсягом пам'яті, в якій зберігаються службові дані та інформація його власника. У випадках розголошення професійних таємниць за допомогою мереж зв'язку залишається криміналістично значуща інформація, зокрема, щодо факту спілкування між злочинцем, посередниками та сторонньою особою, якій була розголошена таємниця, місця перебування осіб у цей момент, часу вчинення злочину. Власник мобільного телефону при підключенні до стільникових ліній зв'язку отримує сім-карту, що містить відомості, необхідні для автентифікації: мобільний ідентифікаційний номер та алгоритм, за допомогою яких підтверджується справжність абонента. Криміналістичне значення має персональна білінгова та комунікаційна інформація. Перша містить відомості щодо кількості та тривалості дзвінків, що здійснюються у місцевій мережі та у роумінгу й дозволяє зробити висновки щодо інтенсивності та кола спілкування власника мобільного телефону. Друга містить дані про вхідні та вихідні дзвінки з апарату, включаючи номер абонента, дату та час початку з'єднання, його тривалість та ін. [5, с. 6–15]. Ця інформація має криміналіс-

тичне значення у процесі встановлення обставин учиненого злочину, а також кола причетних до нього осіб. Реєстрація та довготривале зберігання параметрів телефонних з'єднань, наявність взаємозв'язку абонента та базової станції, а також технічні можливості комп'ютерних мереж і систем керування базами даних дозволяють опрацювати великі обсяги інформації та отримати відомості, значущі для розслідування [5, с. 6–15].

Використовується інсайдерами й IP-телефонія – набір комунікаційних протоколів, технологій та методів, що забезпечують традиційні для телефонії набір номеру, дзвінок і двостороннє голосове спілкування, а також відеоспілкування у мережі Інтернет або будь-яких інших IP-мережах, у процесі якого звуки людського голосу перетворюються в цифрові пакети та прямують мережами IP-телефонії. Коли дані досягають адресата, вони декодуються в голосові сигнали. Існують два базові типи телефонних запитів Інтернет-телефонії: з ПК на ПК або з ПК на телефон, для чого залучаються окремі ЕОМ, програмне забезпечення («Skype») та мобільні телефони. У разі запиту стислі пакети даних прямують Інтернетом за адресою призначення, утворюючи «доріжки електронних слідів».

Таким чином, урахування закономірностей утворення, передачі та відображення інформації об'єктивній дійсності дає певні знання під час розслідування злочинів щодо можливих каналів розголошення таємниць, можливих напрямів пошуку слідів злочину. Протиправний напрям використання ІТ призвів до виник-нення кіберзлочинності та міграції у віртуальне середовище способів готування, вчинення й приховування широкого кола традиційних злочинів [8, с. 425–426]. Діяльність із розголошення таємниць завдяки різним формам відображення інформації в об'єктивній дійсності та появі ІТ специфічно відображається в електронному просторі у вигляді електронних слідів. В. В. Білоус зауважує, що в епоху ІТ традиційна класифікація слідів утрачає здатність повною мірою задовольняти потреби криміналістики [8, с. 426]. Відмінності у відображенні матеріальних слідів, що досліджуються трасологією, та електронних слідів дозволили виокремити поряд із матеріальними та ідеальними, ще й електронні сліди [9, с. 7]. Принципова відмінність електронного простору полягає у тому, що взаємодіючі в ньому

об'єкти (файли даних, програм), які беруть участь у процесі відображення (слідоутворення), позбавлені зовнішньої будови, через це досвід, накопичений трасологією, є незатребуваним [10, с. 104].

Дискусійним є питання щодо того, який термін доцільно використовувати для позначення електронних слідів злочину. У літературі зустрічаються такі терміни: «віртуальні сліди» [11, с. 350–355], «електронні (цифрові) сліди» [8, с. 426] та «інформаційні сліди» [12, с. 265]. В. Ю. Агібалов пише, що є виправданим використання терміна «віртуальні сліди», оскільки в результаті електронно-цифрового відображення на матеріальному носії фіксується образ, що містить цифрові значення параметрів формальної математичної моделі реального фізичного явища, що спостерігається [9, с. 7]. Здебільшого терміни «віртуальні сліди» та «електронні (цифрові)» сліди використовуються як синоніми. Доцільніше використовувати термін «електронні сліди», оскільки будь-який електронний документ у структурі є електронно-цифровим, а тому не варто кожний раз підкреслювати його внутрішню будову.

Електронні сліди – це зафіксовані комп'ютерною системою на матеріальному носії результати відображення реального процесу чи дії іншої комп'ютерної системи, пов'язані зі злочином, у вигляді цифрового образу формальної моделі цього процесу [9, с. 13–14]. Ці сліди мають специфічні властивості: 1) «віртуальні сліди» існують на матеріальному носії, але недоступні безпосередньому сприйняттю; 2) ці сліди внутрішньо не є надійними, оскільки їх можливо неправильно зчитати [10, с. 102]. У процесі розголошення таємниці інсайдер надсилає інформацію через локальні або глобальні мережі у вигляді електронних повідомлень (e-mail) з метою доведення її до відома сторонньої особи. У такому випадку утворюється «доріжка електронних слідів», яка становить систему утворених слідів у комп'ютерній мережі, що складається з кількох послідовно розташованих у часі та логічно взаємопов'язаних записів щодо проходження комп'ютерної інформації лініями зв'язку через комутаційне устаткування операторів зв'язку від комп'ютера злочинця до комп'ютера іншої особи. Вилучення даних, пише В. В. Крилов, що містяться в електронній пошті, може здійснюватися за правилами накладення арешту на

поштово-телеграфну кореспонденцію із пред'явленням вимог до власника поштового вузла, де зареєстрована «скринька» [1, с. 120].

Носіями електронних слідів незаконного розголошення таємниці та осередками їх локалізації є: жорсткий диск («вінчестер»), оптичні диски (CD, DVD), інші носії інформації (носії флеш-пам'яті тощо). Досліджуючи сліди в оперативних запам'ятовуючих пристроях ЕОМ, необхідно звертати увагу на лог-файли (журнали роботи програм), де може зберегтися криміналістично значуща інформація щодо кримінального правопорушення [13, с. 84–85]. Більшість організацій та установ ведуть спеціальні електронні протоколи (журнали, лог-файли), в яких протоколюються дані щодо запитів до відповідних інформаційних ресурсів, інформаційного обміну, який відбувається [14]. Доцільно зберегти та зафіксувати лог-файли, вміст кешів, а також зняти з комп'ютерів короткочасні дані (щодо поточних мережевих з'єднань, динамічних адрес, списків процесів, сесій тощо), зробити копію (за секторами) жорсткого диску та зберегти інші потенційні електронні сліди [15]. Варто відшукувати й «приховані» файли та архіви, в яких можуть зберігатися криміналістично значущі дані. При виявленні файлів із зашифрованою інформацією або таких, що вимагають для їх перегляду стандартними програмами введення паролів, їх слід спрямовувати на розшифровування спеціалістам [1, с. 253].

Певні можливості з установлення обставин розголошення таємниці надають електронні сліди, що залишені на оперативно-запам'ятовуючих пристроях периферійного устаткування (зокрема, лазерного принтера). Периферійні пристрої вводу-виводу можуть певний час зберігати фрагменти програмного забезпечення та інформації, для отримання якої необхідні спеціальні знання [1, с. 253]. Отже, використання ІТ зумовило появу нових слідів розголошення таємниць, перелік предметів і документів – речових доказів учинення злочину. З'явилися такі речові докази, як носії комп'ютерної інформації із певною електронною специфікою [5, с. 6–15]; вони відображають сліди модифікації інформації.

Таким чином, нові ІТ, які охоплюють усі ресурси, що необхідні для керування інформацією, – комп'ютери, програмне забезпечення та мережі, що використовуються для створення, зберігання та пере-

дачі інформації, дали нові можливості інсайдерам. Це спричиняє видозміну обстановки розголошення професійних таємниць та спонукає інсайдерів до активного залучення як знарядь та засобів протиправного діяння – ЕОМ, машинних носіїв інформації, програмного забезпечення, комп'ютерних мереж, що детермінують появу електронних слідів злочину поруч з ідеальними і матеріальними.

Перелік літератури

1. Крылов В. В. Расследование преступлений в сфере информации / В. В. Крылов. – М. : Изд-во «Городец», 1998. – 264 с.

2. Философия науки и техники: тематический словарь / С. И. Некрасов, Н. А. Некрасова. 2010. [Електронний ресурс]. – Режим доступу: http://science_philosophy.academic.ru.

3. Ишин А. М. Теоретические аспекты информационного обеспечения органов предварительного следствия в ходе расследования преступлений : монография / А. М. Ишин. – Калининград : Изд-во Калинингр. ЮИ МВД России, 2003. – 224 с.

4. Кустов А. М. Криминалистическая характеристика преступлений и механизм преступлений / А. М. Кустов // Воронежские криминалистические чтения : сб. науч. тр. / под ред. О. Я. Баева. – Воронеж : Изд-во Воронеж. гос. ун-та, 2005. – Вып. 6. – С. 135–145.

5. Ищенко Е. П. Криминалистика и новые информационные технологии / Е. П. Ищенко // Вестник криминалистики. – 2009. – Вып. 3 (31). – С. 6–15.

6. Вехов В. Б. К вопросу о понятии криминалистического компьютероведения / В. Б. Вехов // Информационная безопасность и компьютерные технологии в деятельности правоохранительных органов : межвуз. сб. науч. тр. – Вып. 2. – Саратов : СЮИ МВД России, 2003. – С. 215–226.

7. Хахановський В. Г. Використання досягнень сучасних інформаційних технологій в діяльності правоохоронних органів / В. Г. Хахановський, І. В. Мартиненко // Сучасні проблеми інформатизації органів внутрішніх справ України : матеріали міжвуз. наук.-практ. конф. (Україна, Київ, 15 берез. 2001 р.) / відп. ред. А. В. Іщенко. – К. : Нац. акад. внутр. справ України, 2002. – С. 86–88.

8. Білоус В. В. Електронні сліди як актуальний напрямок криміналістичних досліджень / В. В. Білоус // Правове життя сучасної України : матеріали міжнар. наук. конф. проф.-виклад. складу, присвяч. 15-річчю Нац. ун-ту «Одес. юрид. акад.» та 165-річчю Одес. школи права, 20–21 квіт. 2012. – О. : Фенікс, 2012. – Т. 2. – С. 425–427.

9. Агибалов В. Ю. Виртуальные следы в криминалистике и уголовном процессе : автореф. дис. … канд. юрид. наук : 12.00.09 / В. Ю. Агибалов ; Воронеж. гос. ун-т. – Воронеж, 2010. – 23 с.

10. Мещеряков В. А. Преступления в сфере компьютерной информации: основы теории и практики расследования / В. А. Мещеряков. – Воронеж : Изд-во ВГУ, 2002. – 408 с.

11. Агибалов В. Ю. Криминалистическая сущность виртуальных следов / В. Ю. Агибалов // Вестник ВГУ. Серия: Право. Воронеж. гос. ун-т. – 2009. – № 2. – С. 350–355.

12. Бірюкова Т. П. Сліди, як елемент криміналістичної характеристики злочинів у сфері використання комп'ютерних технологій / Т. П. Бірюкова, Д. В. Бірюков // Актуальні проблеми кримінального права, процесу та криміналістики : матеріали IV міжнар. наук.-практ. конф., присвяч. 95-річчю з дня народж. проф. М. В. Салтевського (1917–2009) / Нац. акад. прав. наук України, Міжнар. гуманітар. ун-т, Нац. ун-т «Одес. юрид. акад», ОНУ ім. Мечнікова, ЛНУ ім. І. Франка, Прикарпат. нац. ун-т ім. В. Стефаника. – О. : Фенікс, 2012. – С. 263–266.

13. Лісовий В. В. Виявлення, фіксація та вилучення доказів при розслідуванні порушень роботи автоматизованих систем / В. В. Лісовий // Сучасні проблеми інформатизації органів внутрішніх справ України : матеріали міжвуз. наук.-практ. конф. (Україна, Київ, 15 берез. 2001 р.) / відп. ред. А. В. Іщенко. – К. : Нац. акад. внутр. справ України, 2002. – С. 79–86.

14. Собецкий И. В. О доказательственном значении лог-файлов [Електронний ресурс] / И. В. Собецкий. – Режим доступу: http://www.securitylab.ru/39167.html.

15. Федотов Н. Н. Расследование инцидентов ИБ: Как расследовать разглашение конфиденциальной информации в блогах и форумах? [Електронний ресурс] / Н. Н. Федотов. – Режим доступу: http://forensics.ru/investigation_blogs.html.

16. Большой энциклопедический политехнический словарь [Електронний ресурс]. – Режим доступу: http://dic.academic.ru/dic.nsf/polytechnic/6482.

Транслітерація переліку літератури

1. Kryilov V. V. Rassledovanie prestupleniy v sfere informatsii. [The investigation of crimes in the area of information]. Moskva: Izdatelstvo Gorodets, 1998, 264 p. [in Russian].

2. Filosofiya nauki i tehniki: tematicheskiy slovar [The philosophy of of science and technology: thesaurus] Retrieved from: http://science_philosophy.academic.ru [in Russian].

3. Ishin A. M. Teoreticheskie aspektyi informatsionnogo obespecheniya organov predvaritelnogo sledstviya v hode rassledovaniya prestupleniy [Theoretical aspects of information support of the preliminary investigation in the investigation of crimes]. Kaliningrad : Izd-vo Kaliningr. YuI MVD Rossii, 2003, 224 p. [in Russian].

4. Kustov A. M. Kriminalisticheskaya harakteristika prestupleniy i mehanizm prestupleniy [Criminalistic characteristic of crimes and offenses mechanism]. Voronezhskie kriminalisticheskie chteniya : sb. nauch. trudov. [Voronezh criminalistical reading: Collected papers]. Voronezh : Izd-vo Voronezh. gos. un-ta, 2005, Vol. 6, pp. 135–145[in Russian].

5. Ischenko E. P. Kriminalistika i novyie informatsionnyie tehnologii [Criminalistics and the new information technologies] Vestnik kriminalistiki. Vol. 3 (31) , 2009, pp. 6–15 [in Russian].

6. Vehov V. B. K voprosu o ponyatii kriminalisticheskogo kompyuterovedeniya [On the concept of conducting criminalistical computer]. Informatsionnaya bezopasnost i kompyuternyie tehnologii v deyatelnosti pravoohranitelnyih organov: mezhvuz. sb. nauch. tr., vol. 2, Saratov : SYui MVD Rossii, 2003, pp. 215–226 [in Russian].

7. Hahanovskiy V. G. Vikoristannya dosyagnen suchasnih informatsiynih tehnologiy v diyalnosti pravoohoronnih organiv [Application of achievements of modern information technology in law enforcement activities] Suchasni problemi informatizatsiyi organiv vnutrishnih sprav Ukrayini [Modern problems of informatization of the Interior of Ukraine]. Kiyiv : Nats. akad. vnutr. sprav Ukrayini / vIdp. red. A. V. Ischenko, 2002. – pp. 86–88 [in Ukrainian].

8. Bilous V. V. Elektronni slidi yak aktualniy napryamok kriminalistichnih doslidzhen [Electronic traces as topical direction criminalistics researches]. Pravove zhittya suchasnoyi Ukrayini [The legal life of modern Ukraine: Collected papers]. Odesa : Feniks, 2012, pp. 425–427 [in Ukrainian].

9. Agibalov V. Yu. Virtualnyie sledyi v kriminalistike i ugolovnom protsesse [Virtual traces in criminalistics and criminal trial]. Voronezh, 2010, 23 p. [in Russian].

10. Mescheryakov V. A. Prestupleniya v sfere kompyuternoy informatsii: osnovyi teorii i praktiki rassledovaniya [Crimes in the sphere of computer information: basics of the theory and practice of investigation]. Voronezh : Izd-vo VGU, 2002, 408 p. [in Russian].

11. Agibalov V. Yu. Kriminalisticheskaya suschnost virtualnyih sledov [The criminalistic essence of virtual tracks]. Vestnik VGU. Seriya: Pravo [Herald

VGU]. Voronezhskiy gosudarstvennyiy universitet, 2009, no. 2, pp. 350–355 [in Russian].

12. Biryukova T. P. Slidi, yak element kriminalistichnoyi harakteristiki zlochiniv u sferi vikoristannya komp’yuternih tehnologiy [Traces as element of kriminalistical characteristics of crimes in sphere of computer technologies]. Aktualni problemi kriminalnogo prava, protsesu ta kriminalistiki [The actual problems of criminal law, process and criminalistics: Collected papers]. Odesa : Feniks, 2012, pp. 263–266 [in Ukrainian].

13. Lisoviy V. V. Viyavlennya, fiksatsiya ta viluchennya dokaziv pri rozsliduvanni porushen roboti avtomatizovanih sistem [Detection, fixation and removal of evidence in the investigation of disorders of the automated systems]. Suchasni problemi informatizatsiyi organsv vnutrishnih sprav Ukrayini [Modern problems of informatization of the Interior of Ukraine]. Kiyiv: pp. 79–86 [in Ukrainian].

14. Sobetskiy I. V. O dokazatelstvennom znachenii log-faylov [Of the evidential meaning of log files] [Elektronniy resurs]. Retrieved from: http://’www.securitylab.ru/39167.html [in Russian].

15. Fedotov N. N. Rassledovanie intsidentov IB : Kak rassledovat razglashenie konfidentsialnoy informatsii v blogah i forumah? [The investigation incident of IS: How to investigate the disclosure of confidential information in blogs and forums?] Retrieved from: http://forensics.ru/investigation_blogs.html [in Russian].

16. Bolshoy entsiklopedicheskiy politehnicheskiy slovar [The Great Encyclopedic Dictionary Polytechnic]. Retrieved from : http://dic.academic.ru/dic.nsf/ polytechnic/6482 [in Russian].

Резнікова Г. І. Роль інформаційних технологій у процесі незаконного розголошення професійних таємниць

Досліджено вплив інформаційних технологій на процес підготовки, вчинення та приховування незаконного розголошення інформації з обмеженим доступом. Визначено, що поява та інтенсивна зміна новітніх інформаційних технологій вплинула на видозміну обстановки вчинення злочину, форми відображення предмета злочинного посягання – інформації з обмеженим доступом у об’єктивній дійсності (матеріальна, ідеальна, електронна), а також на знаряддя та засоби, які використовують інсайдери. З’ясовано, що порушення інформаційної безпеки певної професійної діяльності внаслідок незаконного розголошення професійних таємниць здійснюється із залученням інсайдерами окремих знарядь та засобів учинення злочинів, які детермінують утворення та локалізацію трьох груп слідів злочинів. Доведено, що розголошення професійних таємниць є проявом психологічної взаємодії осіб і здійснюється у процесі спілкування між його учасниками. Підкреслено, що інформаційні канали, за допомогою яких доводиться до відома

особи інформація з обмеженим доступом, поділяються на два види: анатомо-фізіологічні та технічні. З'ясовано, що незаконне розголошення таємниці може відбуватись під час безпосереднього спілкування за допомогою анатомо-фізіологічних засобів, або ж опосередковано за допомогою технічних засобів і носіїв інформації. Встановлено, що інсайдер застосовує персональний комп'ютер і периферійні пристрої вводу та виводу інформації, пристрої зберігання інформації, а також сучасні засоби та мережі зв'язку.

Ключові слова: *інформаційні технології, обстановка вчинення злочинів, знаряддя та засоби вчинення злочинів, типові сліди злочину.*

Резникова А. И. Роль информационных технологий в процессе незаконного разглашения профессиональных тайн

Исследовано влияние информационных технологий на процесс подготовки, совершения и сокрытия незаконного разглашения информации с ограниченным доступом. Определено, что появление и интенсивное изменение новейших информационных технологий повлияли на видоизменение обстановки совершения преступления, формы отражения предмета преступного посягательства – информации с ограниченным доступом в объективной действительности (материальная, идеальная, электронная), а также на орудия и средства, которые используют инсайдеры. Установлено, что нарушения информационной безопасности профессиональной деятельности вследствие незаконного разглашения профессиональных тайн осуществляется с привлечением инсайдерами отдельных орудий и средств совершения преступлений, детерминирующих образования и локализацию трех групп следов преступлений. Доказано, что разглашение профессиональных тайн является проявлением психологического взаимодействия лиц и осуществляется в процессе общения. При этом информационные каналы, с помощью которых доводится до сведения лица информация с ограниченным доступом, делятся на два вида: анатомо-физиологические и технические. Установлено, что незаконное разглашение тайны может происходить во время непосредственного общения с помощью анатомо-физиологических средств, или опосредованно через технические средства и носители информации. Установлено, что инсайдер применяет персональный компьютер и периферийные устройства ввода и вывода информации, устройства хранения информации, а также современные средства и сети связи.

Ключевые слова: *информационные технологии, обстановка совершения преступлений, орудия и средства совершения преступлений, типовые следы преступлений.*

Reznikova H. I. The role of information technology in the illegal disclosure of professional secrets

The influence of information technology on the process of preparing, committing and concealing illegal disclosure of information with limited access has been investigated. It was determined that the appearance of intense change and new information technologies affected the modification of the crime situation, reflect forms the subject of

*a criminal assault – of classified information in objective reality, and the means and instruments which using insiders. The violation of information security of a professional activity as a result of illegal disclosure of professiona**l** secrets is carried out with the involvement of insiders specific tools and means to commit a crime which determine the formation and localization of three groups of traces of crimes have been found out. The disclosure of professional secrets is a manifestation of psychological interaction between people and carried out in the process of communication between the parties has been proved. Emphasized that information channels through which communicated to persons classified information, are divided into two types: anatomical and physiological and technical. That the illegal disclosure of secrets can take place during direct communication with the anatomical and physiological means or indirectly, through technical means and media have been found out. The insider uses a personal computer and peripherals input and output information storage device, as well as modern equipment and communication networks has been established.*

Key words: *information with the limited access, secret, disclosure, professional secret, criminalistic classification of the crimes, criminalistic characteristic of the crimes, typical versions.*