DOI: 10.33498/louu-2023-09-159

Діна Дрижакова

аспірантка кафедри кримінально-правової політики
та кримінального права
Навчально-наукового інституту права
Київського національного університету
імені Тараса Шевченка
(Київ, Україна)
d.dryzhakova@gmail.com

УДК 343.3/.7

ПРОБЛЕМИ ДОКАЗУВАННЯ ЗЛОЧИНІВ У СФЕРІ ВТРУЧАННЯ В ІНФОРМАЦІЙНІ СИСТЕМИ

Анотація. У статті досліджено питання щодо проблем доказування злочинів у сфері втручання в інформаційні системи.

Зазначено, що саме злочинний вплив на інформаційні системи або їх злочинне використання дає підстави визначити фактично комп'ютерну інформацію через місцезнаходження її на комп'ютерній техніці як джерела доказу.

Результати злочинного впливу на комп'ютерну інформацію (витік, втрата, підробка, блокування комп'ютерної інформації, порушення встановленого порядку її маршрутизації, зміна, знищення, блокування комп'ютерної інформації) чи комп'ютерну систему слід оцінювати через судову комп'ютерно-технічну експертизу.

Як висновок наголошено на тому, що потрібно врахувати досвід європейських країн і коригувати та розширити диспозиції статей з урахуванням порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, вдосконалити методику проведення експертиз з урахуванням технологічних можливостей сьогодення, внести зміни до Кримінального та Кримінально процесуального кодексів України щодо визначеності міжнародної юрисдикції за злочини у сфері втручання в комп'ютерні та інформаційні системи.

Ключові слова: комп'ютерний злочин; судова комп'ютерно-технічна експертиза; комп'ютерна інформація, комп'ютерна система.

Нині кіберпростір займає одну з найбільш критичних та актуальних галузей науки. Із цим дуже важко не погодитися. У кожній країні світу існують державні інститути, які займаються дослідженнями у профільних галузях науки та тісно і дуже плідно взаємодіють із державним апаратом. Інформаційні технології – це теж наука. На жаль, в Україні немає жодного інституту, який би займався опрацюванням цієї гілки та мав би певні винаходи або результати. Проте у законодавстві існує відповідальність за несанкціоноване втручання у роботу електронно-обчислювальних

машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (далі – АОЕМ), такі злочини, як шахрайство з банківськими платіжними картками, злочини у сфері телекомунікацій та інформаційно-телекомунікаційних мереж (шахрайство з оплатою міжнародних телефонних переговорів), незаконне використання банківської мережі електронних платежів, програмне (комп'ютерне) "піратство", шахрайство з використанням ігрових автоматів та багато інших.

Проблематикою правопорушень у сфері втручання у роботу АОЕМ є визначення доказової бази вчинення правопорушення. На нашу думку, у роботі АОЕМ можна виділити дві групи напряму: атака та захист. Для атакуючих найбільш важливо: програмування на низькорівневих мовах *(C, C++, ACM)*, бінарна експлуатація, фаззинг *(afl-plusplus)*, вебпентест *(burp-suite)* та злом і просунення у (локальних, приватних) мережах *(metasploit)*. Для захищаючих найбільш актуально: адміністрування *(Unix, Windows)*, програмування на скриптових мовах *(bash, PowerShell)*, вміння моделювати безпечні мережі тощо.

Яким же чином встановити момент вчинення правопорушення, доказову базу та країну, за законодавством якої особу-правопорушника буде притягнуто до відповідальності? Програмними засобами, про які йдеться у ст. 361 Кримінального кодексу України (далі – КК України)[1], є різні комп'ютерні програми, використання яких створює можливість для незаконного проникнення у комп'ютер, його систему чи комп'ютерну мережу, або ж полегшує таке незаконне проникнення. Під технічними засобами розуміються будь-які технічні пристрої, за допомогою яких без використання комп'ютерних програм здійснюється вплив на роботу АЕОМ.

Під час збирання доказів при розслідуванні таких кримінальних правопорушень виникає проблема: поряд із "традиційними" слідами частиною відомостей є комп'ютерна інформація, яка не залишає змін у зовнішньому матеріальному середовищі, оскільки у більшості випадків має інформаційний характер[2], а серед науковців і практиків інтерпретується по-різному – як електронна, цифрова, комп'ютерна, віртуальна, бінарна інформація. Фактично комп'ютерна інформація через місцезнаходження її на комп'ютерній техніці отримує статус джерела доказу.

При цьому варто звернути увагу, що знищення комп'ютерної інформації на сьогодні не завжди може стати перепоною для отримання доказу вчинення злочину, адже існує велика кількість ефективних сучасних засобів пошуку (відновлення) знищеної електронної інформації, а тому

[1] Кримінальний кодекс України: Закон України від 5 квітня 2001 р. № 2341-III <https://zakon.rada.gov.ua/laws/show/2341-14/conv#n2527> (дата звернення: 17.09.2023).

[2] Д Пашнєв, 'Властивості комп'ютерної інформації як предмету злочину' (2012) 1 Вісник Кримінологічної асоціації України: збірник наукових праць 115–25.

сліди злочину, тобто інформація, яка може бути частиною доказової бази, має також свої особливості.

Сліди злочинів у сфері використання інформаційних технологій утворюються за результатами дії на комп'ютерну інформацію через зовнішній доступ до неї, що викликає певні зміни, пов'язані з подією злочину. Такими змінами можуть бути, зокрема: сліди знищення, модифікації, копіювання інформації, блокування інформаційної системи. Сліди змін залишаються на машинних носіях інформації і відображають зміни в інформації, що в них зберігається (порівняно з вихідним станом). Інформація може зберегти сліди її часткового знищення або модифікації (видалення з каталогів імен файлів, видалення або додавання окремих записів, фізичного руйнування або розмагнічування носіїв тощо). Інформаційними слідами є також результати роботи антивірусних і тестових програм. Ці сліди можуть бути виявлені при експертному дослідженні комп'ютерного обладнання, протоколів роботи операційних систем, додатків, антивірусних програм, програмного коду та ін. Сліди несанкціонованого доступу до інформації містяться у журналах операційних систем і окремих програмних продуктів, що створюють резервні копії файлів і файли-звіти, зберігають інформацію про останні проведені операції та виконані програми.

Цього питання торкалися у своїх дослідженнях багато вчених: Д. Азаров, М. Бікмурзін, М. Карчевський, В. Кузнецов, А. Музика, Є. Лащук, П. Орлов, С. Орлов, О. Радутний, М. Рудик, Н. Розенфельд, О. Смаглюк, І. Юрченко та ін.

Метою дослідження є виявлення особливостей кримінально-правової характеристики злочинів у сфері використання систем та комп'ютерних мереж і мереж електрозв'язку, доказової бази злочинів у цій сфері та розробка рекомендацій щодо кваліфікації діянь за статтями 361–363[1] КК України.

Переважна більшість складів злочинів у сфері використання АЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (далі – комп'ютерні злочини) є матеріальними, а тому виявляються за наслідками. Отже, під час кваліфікації цих злочинів та їх відмежування від суміжних складів злочинів, необхідно оцінювати розмір і характер заподіяної шкоди з точки зору характеристики її предмету.

Поряд зі шкодою – наслідком комп'ютерних злочинів, іде мета вчинення правопорушення. При визначенні мети комп'ютерних злочинів не слід обмежуватися лише фабулою статті – "несанкціоноване втручання". У більшості випадків як, наприклад, програмне (комп'ютерне) піратство, метою буде одержання грошової винагороди, збагачення. І здавалося б, все просто: зловмисники одержали доступ до комп'ютерних мереж компаній чи стратегічної установи і вимагають суму коштів

ПРАВО УКРАЇНИ • 2023 • № 9 • 159-167

за розблокування доступів до мережі компанії. І ось зловмисників можна брати на гарячому при одержанні грошей, але не зовсім так. Як правило, вимагають зловмисники віртуальні кошти (віртуальні активи) – криптовалюту.

І ось тут починається найцікавіше із доказовою базою. Відповідно до Конституції України[3] єдиною державною валютою в Україні є гривня. Частиною 2 ст. 19 Конституції України встановлено, що органи державної влади та органи місцевого самоврядування, їх посадові особи зобов'язані діяти лише на підставі, у межах повноважень та у спосіб, що передбачені Конституцією та законами України.

Згідно зі ст. 2 Закону України "Про Національний банк України" (далі – Закон про НБУ)[4] НБУ є центральним банком України, особливим центральним органом державного управління, юридичний статус, завдання, функції, повноваження і принципи організації якого визначаються Конституцією України, цим Законом та іншими законами України. При цьому зазначаємо, що НБУ відповідно до повноважень, наданих законодавством України, встановлює правила використання лише тих інструментів фінансового ринку, регулювання яких згідно із законодавством покладено на НБУ.

Правовий статус віртуальних активів, питання комплексного врегулювання правовідносин, що виникають у зв'язку з оборотом віртуальних активів в Україні, права та обов'язки учасників ринку віртуальних активів, засади державної політики у сфері обороту віртуальних активів визначені Законом України "Про віртуальні активи"[5]. Відповідно до цього Закону регуляторами ринку віртуальних активів є Національна комісія з цінних паперів та фондового ринку (далі – НКЦПФР) та НБУ. Зокрема, НБУ здійснюватиме державне регулювання обороту на території України такого різновиду фінансових віртуальних активів, як віртуальні активи, забезпечені валютними цінностями. При цьому у п. 1 розділу VI Закону України "Про віртуальні активи" встановлено, що Закон набирає чинності лише з дня набрання чинності законом України про внесення змін до Податкового кодексу України[6] щодо особливостей оподаткування операцій з віртуальними активами, але не раніше дня опублікування цього Закону.

14 червня НКЦПФР нарешті презентувала представникам профільних державних органів та ринковій спільноті текст законопроєкту про

[3] Конституція України: Закон України від 28 червня 1996 р. № 254к/96-ВР <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text> (дата звернення: 17.09.2023).
[4] Про Національний банк України: Закон України від 20 травня 1999 р. № 679-XIV <https://zakon.rada.gov.ua/laws/show/679-14#Text> (дата звернення: 17.09.2023).
[5] Про віртуальні активи: Закон України від 17 лютого 2022 р. № 2074-IX <https://zakon.rada.gov.ua/laws/show/2074-20#Text> (дата звернення: 17.09.2023).
[6] Податковий кодекс України: Закон України від 2 грудня 2010 р. № 2755-VI <https://zakon.rada.gov.ua/laws/show/2755-17#Text> (дата звернення: 17.09.2023).

оподаткування криптоактивів, який базується на положеннях європейського "Закону про крипторинки"[7]. Нагадаємо, що 31 травня 2023 р. Європейський парламент схвалив нові загальні правила нагляду та захисту прав споживачів щодо криптовалют – *Markets in Crypto assets (MiCA)*. Регламент набрав чинності в ЄС 29 червня 2023 р. і почне повністю діяти з 30 грудня 2024 р. *MiCA* – це документ, який передбачає регулювання віртуальних активів у Європейському Союзі (далі – ЄС), захищаючи користувачів та інвесторів у цій галузі.

Натепер криптовалюти в Україні як грошова одиниця так і не визнані. А в законодавстві йдеться про купівлю-продаж криптовалют через біржу, що має стати ідентифікатором особи, але є й інші додатки на кшалт *TrustWallet,* які не передбачають ідентифікацію особи як власника. Отже, як бачимо, один із доказів наявності умислу одержання винагороди доволі складно одержати.

Ще одним цікавим доказовим моментом цієї категорії правопорушень є місце вчинення злочину, безпосередньо країна. Оскільки, як відомо, категорія правопорушень у сфері втручання у роботу інформаційних систем передбачає підміну *IP*-адреси, тобто реального місця вчинення правопорушення, а отже, і законодавства відповідної держави у цій сфері злочинів.

Місцем виявлення електронних слідів можуть бути як матеріальні, так і нематеріальні об'єкти: ресурси мережі Інтернет, профіль користувача у соціальних мережах, електронні платіжні системи *(PayPal, LiqPay, iPay.ua, Qiwi, WebMoney, Perfect Money* та ін.), бази даних (абонентів операторів зв'язку, криміналістичних обліків Міністерства внутрішніх справ України та ін.), локальні мережі різних структур, "жорсткі диски" персональних комп'ютерів (ноутбуків, планшетів та ін.), карти пам'яті, засоби стільникового зв'язку і багато іншого[8].

Нині одним із технічних засобів, які найчастіше використовуються у протиправних цілях, є засоби стільникового зв'язку. Вони можуть слугувати не лише носіями криміналістично значущої інформації, а й предметами, знаряддями злочинів. Наприклад, при вчиненні вимагання вже типовими є дії злочинних груп, коли по мобільному телефону висуваються вимоги про зарахування на абонентський рахунок злочинця грошових коштів за повернення викраденого транспортного засобу.

Типовими для кримінальних правопорушень, учинених із використанням засобів стільникового зв'язку, будуть такі сліди: інформаційні

[7] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 <https://eur-lex.europa.eu/eli/reg/2023/1114/oj> (accessed: 17.09.2023).

[8] М Климчук, Ю Комиссарчук, С Марко, Б Стецик, *Судова комп'ютерно-технічна експертиза у кримінальному провадженні: навчальний посібник* (Львівський державний університет внутрішніх справ 2022) 11.

сліди на машинних носіях оператора зв'язку (наприклад, дані первинного номера телефону, який використовується для зв'язку та зберігається у *log*-файлах; дати сеансу зв'язку; інформація про час зв'язку; статичні або динамічні *IP*-адресні журнали реєстрації провайдера в Інтернеті і відповідні телефонні номери; швидкості передачі повідомлення; вихідні журналів сеансів зв'язку, що включають тип використаних протоколів, самі протоколи та ін.)[9]; сліди на самому мобільному телефоні (приміром, *IMEI*-код, *SMS*-повідомлення), відомості про надіслані повідомлення, телефонні з'єднання, абонентська книга телефону, телефонні номери, що використовуються, сліди мікрочастинок, пальців рук. Сліди, присутні на *SIM*-карті і наявні на мобільному телефоні, зазвичай ідентичні[10].

3 квітня 2022 р. набрав чинності Закон України "Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану"[11], після чого були внесені відповідні до законодавчих нормативних актів[12]. Згідно з ч. 6 ст. 361 КК України:

> Дії, передбачені частинами першою – четвертою цієї статті, не вважаються несанкціонованим втручанням в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, якщо вони були вчинені відповідно до порядку пошуку та виявлення потенційних вразливостей таких систем чи мереж[13].

Відповідно до Постанови Кабінету Міністрів України "Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж" (далі – Постанова № 497)[14] визначається механізм здійснення пошуку та виявлення потенційної вразливості інформаційних (автоматизованих),

---

[9] С Потапов, И Потапова, 'Использование экспертиз при расследовании и раскрытии преступлений, совершенных с применением сотовых телефонов' [2016] 11 (11) Социально-экономические процессы и явления 157.

[10] М Климчук, 'Сліди кримінальних правопорушень, учинених із використанням засобів стільникового зв'язку, й особливості їх виявлення' в *Актуальні питання виявлення та розкриття злочинів Національною поліцією: вітчизняний та зарубіжний досвід: матеріали Міжнар. наук.-практ. круглого столу* (НАВС 2020) 86.

[11] Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану: Закон України від 24 березня 2022 р. № 2149-IX <https://zakon.rada.gov.ua/laws/show/2149-20#Text> (дата звернення: 17.09.2023).

[12] Микола Хавронюк, 'Втручання в роботу інформаційно-комунікаційних систем: кримінальна відповідальність' (29.04.2022) <https://pravo.org.ua/blogs/vtruchannya-v-robotu-informatsijno-komunikatsijnyh-system-kryminalna-vidpovidalnist> (дата звернення: 17.09.2023).

[13] Кримінальний кодекс України (н 1).

[14] Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж: Постанова Кабінету Міністрів України від 16 травня 2023 р. № 497 <https://zakon.rada.gov.ua/laws/show/497-2023-%D0%BF#Text> (дата звернення: 17.09.2023).

електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (далі – пошук потенційної вразливості системи). Дія цього Порядку не поширюється на інформаційні (автоматизовані), електронні комунікаційні, інформаційно-комунікаційні системи, електронні комунікаційні мережі, в яких обробляється службова інформація та/або інформація, що становить державну таємницю, розвідувальну таємницю, банківську таємницю.

З урахуванням того, що предметом більшості комп'ютерних злочинів є комп'ютерна інформація або комп'ютерна система (під якою слід розуміти будь-яку із систем: *ЕОМ* (комп'ютер), автоматизовану систему, комп'ютерну мережу чи мережу електрозв'язку), диспозиція ст. 361 КК України відповідно до Постанови № 497, має обмежену сферу дії. Саме злочинний вплив на інформаційні системи або їх злочинне використання дає підстави визначити фактично, комп'ютерну інформацію через місцезнаходження її на комп'ютерній техніці отримує статус джерела доказу. Результати злочинного впливу на комп'ютерну інформацію (витік, втрата, підробка, блокування комп'ютерної інформації, порушення встановленого порядку її маршрутизації (ст. 361), зміна, знищення, блокування комп'ютерної інформації (ст. 362)) чи комп'ютерну систему слід оцінювати через судову комп'ютерно-технічну експертизу.

Судова комп'ютерно-технічна експертиза (далі – СКТЕ) – це окрема, суворо регламентована процесуальна дія, що здійснюється під час розслідування кримінальних правопорушень. Вона є основною процесуальною формою використання спеціальних знань у галузі комп'ютерних технологій, а її результати можуть являти собою найважливішу частину доказової бази у конкретному кримінальному провадженні.

Однак, щоб висновок експерта було визнано допустимим, законодавством передбачені вимоги до призначення судової експертизи, а слідчою та експертною практикою вироблено рекомендації щодо ефективного її проведення. Крім того, будь-яка експертиза повинна проводитись на підставі методики, що відповідає сучасному рівню розвитку науки і техніки. І, оскільки такий вид судової експертизи, як СКТЕ, відносно новий, при її призначенні часто виникає низка типових помилок. Акцентування на них уваги є необхідним[15].

Розслідування кримінальних правопорушень, учинених із використанням комп'ютерної техніки та комп'ютерних технологій, ускладнюється тим, що з постійним розвитком інформаційних технологій з'являються об'єкти дослідження, яких раніше просто не було, змінюються, модифікуються механізми і методи вчинення раніше відомих видів

[15] Климчук, Комісарчук, Марко, Стецик (н 8) 4.

ПРАВО УКРАЇНИ • 2023 • № 9 • 159-167

злочинів, з'являються абсолютно нові їх види[16]. Експерти через швидке старіння методик, велику кількість об'єктів дослідження і широке коло таких питань експертизи значну частину часу витрачають на адаптацію і доопрацювання загальних методик під окремі завдання експертизи, пошук необхідних методів – розробку окремих методик проведення СКТЕ. Складність і тривалість розробки окремих методик СКТЕ збільшуються при накладенні експертною організацією обмежень на вибір методів проведення експертизи за ресурсами (термінами, вартістю експертного програмного забезпечення та ін.).

Наслідки різних упущень уповноважених осіб, які здійснюють збирання такої специфічно збереженої інформації, а також непрофесійні дії фахівців у зазначеній сфері, можуть мати негативні наслідки, адже у такому разі завдання кримінального провадження реалізуються неповністю або частково, що може спричинити прийняття необґрунтованого і незаконного підсумкового рішення у конкретному кримінальному провадженні.

Невирішеною залишається низка практичних проблем, пов'язаних із поводженням з електронною слідовою інформацією, призначенням і проведенням СКТЕ, використанням її результатів у кримінальному процесуальному доказуванні.

Висновки. Підсумовуючи викладене, слід зазначити, що потрібно врахувати досвід європейських країн і коригувати та розширити диспозиції статей з урахуванням порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, вдосконалити методику проведення експертиз з урахуванням технологічних можливостей сьогодення, внести зміни до Кримінального та Кримінально процесуального кодексів України щодо визначеності міжнародної юрисдикції за злочини у сфері втручання у комп'ютерні та інформаційні системи.

REFERENCES

Bibliography

Authored books

1. Klymchuk M, Komissarchuk Yu, Marko S, Stetsyk B, *Sudova komp'iuterno-tekhnichna ekspertyza u kryminalnomu provadzhenni: navchalnyi posibnyk* (Lvivskyi derzhavnyi universytet vnutrishnikh sprav 2022) (in Ukrainian).

[16] А Шелупанов, А Смолина, 'Методика проведения подготовительной стадии исследования при производстве компьютерно-технической экспертизы' [2016] 19 (1) Доклады ТУСУРа 31–34.

Journal articles

2. Pashniev D, 'Vlastyvosti komp'iuternoi informatsii yak predmetu zlochynu' (2012) 1 Visnyk Kryminolohichnoi asotsiatsii Ukrainy: zbirnyk naukovykh prats 115–25 (in Ukrainian).
3. Potapov S, Potapova I, 'Ispol'zovanie jekspertiz pri rassledovanii i raskrytii prestuplenij, sovershennyh s primeneniem sotovyh telefonov' [2016] 11 (11) Social'no-jekonomicheskie processy i javlenija 157 (in Russian).
4. Shelupanov A, Smolina A, 'Metodika provedenija podgotovitel'noj stadii issledovanija pri proizvodstve komp'juterno-tehnicheskoj jekspertizy' [2016] 19 (1) Doklady TUSURa 31–4 (in Russian).

Conference papers

5. Klymchuk M, 'Slidy kryminalnykh pravoporushen, uchynenykh iz vykorystanniam zasobiv stilnykovoho zv'iazku, y osoblyvosti yikh vyiavlennia' v *Aktualni pytannia vyiavlennia ta rozkryttia zlochyniv Natsionalnoiu politsiieiu: vitchyznianyi ta zarubizhnyi dosvid: materialy Mizhnar. nauk.-prakt. kruhloho stolu* (NAVS 2020) 86 (in Ukrainian).

Websites

6. Khavroniuk M, 'Vtruchannia v robotu informatsiino-komunikatsiinykh system: kryminalna vidpovidalnist' (29.04.2022) <https://pravo.org.ua/blogs/vtruchannya-v-robotu-informatsijno-komunikatsijnyh-system-kryminalna-vidpovidalnist> (accessed: 17.09.2023) (in Ukrainian).

Dina Dryzhakova

ISSUES OF PROVING CRIMINAL OFFENSES RELATED TO THE INTERFERENCE WITH INFORMATION SYSTEMS

Abstract. This article examines the problems of proving crimes in the field of interference in information systems.

It is noted that it is criminal influence on information systems or their criminal use that gives grounds for determining that computer information, due to its location on computer equipment, receives the status of a source of evidence.

The results of criminal influence on computer information (leakage, loss, forgery, blocking of computer information, violation of the established order of its routing, change, destruction, blocking of computer information or computer the system should be evaluated through computer forensics.

As a conclusion, it is emphasized that it is necessary to take into account the experience of European countries and to adjust and expand the disposition of articles taking into account the order of searching and identifying potential vulnerabilities of information (automated), electronic communication, information and communication systems, electronic communication networks, to improve the methodology of conducting examinations taking into account technological of today's possibilities, to make changes to the criminal and criminal procedural code regarding the determination of international jurisdiction for crimes in the field of interference in computer and information systems.

Keywords: computer crime; computer forensic expertise; computer information; information.