УДК 343.98
DOI https://doi.org/10.32782/2524-0374/2019-5/74

ПРОБЛЕМНІ ПИТАННЯ ОБСТАНОВКИ ВЧИНЕННЯ НЕСАНКЦІОНОВАНИХ ДІЙ З ІНФОРМАЦІЄЮ, ЯКА ОБРОБЛЯЄТЬСЯ В ЕЛЕКТРОННОМУ ВИГЛЯДІ

PROBLEM ISSUES OF THE SITUATION OF UNAUTHORIZED ACTIONS WITH INFORMATION PROCESSED IN ELECTRONIC VIEW

Курман О.В., к.ю.н., доцент,
доцент кафедри криміналістики
Національний юридичний університет імені Ярослава Мудрого

У статті розглядаються питання обстановки вчинення уповноваженою особою несанкціонованих дій з інформацією, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях інформації. Зазначене злочинне діяння передбачене ст. 362 КК України. Як відомо, обстановка злочину є елементом криміналістичної характеристики, яка становить частину окремої криміналістичної методики. Реалії сьогодення вказують на наявні проблеми, пов'язані з практичною реалізацією притягнення до відповідальності винних осіб за ст. 362 КК України через неоднозначність тлумачення норм закону та відставання методичного забезпечення процесу розслідування. Правові відносини у сфері обробки інформації в електронних засобах регулюються Законом України «Про захист інформації в інформаційно-телекомунікаційних системах». У Законі визначено обов'язок власника системи забезпечити комплексний захист інформації тільки стосовно державних інформаційних ресурсів, однак відсутнє однозначне роз'яснення того, хто і коли забезпечує захист інформації в інших випадках. Також у статті говориться про відсутність законодавчого закріплення деяких термінів, що використовуються у законі, а саме: «перехоплення» та «копіювання» інформації.

Вчиненню дій, передбачених ст. 362 КК України, сприяє і те, що на підприємствах, установах, де використовуються відомості в електронній формі, у багатьох випадках відсутні внутрішні документи, інструкції, що регламентують доступ співробітників до документів із інформацією. У науковій роботі зазначається, що несанкціонованим діям з інформацією також сприяють системні порушення співробітниками чинних правил організації технічного захисту територій і приміщень, ведення службової інформації стосовно генерації електронних ключів та паролів доступу, реєстрації та аналізу дій користувачів, порядку обліку, зберігання та видачі користувачам носіїв конфіденційної інформації, допуску до приміщень, де здійснюється автоматична обробка даних.

Ключові слова: захист інформації, порядок доступу до інформації, комп'ютерні мережі, обстановка злочину, методика розслідування, несанкціоновані дії.

The article deals with the situation of commissioning by an authorized person of unauthorized actions with information that is processed in electronic computers (computers), automated systems, computer networks or stored on the media of such information. The said criminal act is provided for in Art. 362 of the Criminal Code of Ukraine. As you know, the situation of the crime is an element of forensic characteristics, which in turn forms part of a separate forensic methodology. The realities of today point to the existing problems associated with the practical implementation of the prosecution of perpetrators under Art. 362 of the Criminal Code of Ukraine due to ambiguity in the interpretation of the law and the lack of methodological support for the investigation process. Legal relations in the field of information processing in electronic media are regulated by the Law of Ukraine "On Information Protection in Information and Telecommunication Systems". The Act defines the obligation of the system owner to provide comprehensive information protection only with respect to state information resources, but there is no clear explanation as to who and when provides information protection in other cases. The article also notes the absence of legislative fixing of some of the terms used in the law, in particular: "interception" and "copying" of information. To commit the actions provided for in Art. 361 of the Criminal Code of Ukraine also contributes to the fact that in enterprises, institutions where information is used in electronic form, in many cases there are no internal documents, instructions regulating the access of employees to documents with information. Systematic violations by employees of the existing rules for organizing technical protection of premises, maintaining official information, rules for generating electronic keys and passwords, registering and analyzing user actions, rules for recording, storing and issuing storage media to users and rules for accessing premises where automatic data processing is carried out, contributes to unauthorized actions with information.

Key words: information security, order of access to information, computer networks, situation of the crime, investigation technique, unauthorized actions.

Бурхливий розвиток сучасних технологій водночас із перевагами наділяє суспільство й проблемами, пов'язаними з появою нових злочинів та вдосконаленням механізмів вчинення вже існуючих. До таких належать і злочини у сфері інформаційних технологій. Одним із ефективних механізмів боротьби із злочинністю є своєчасне розкриття та розслідування конкретного злочину. Однак це вимагає наявності сучасних методик розслідування. Щоб ці методики були дійсно дієвими, вони повинні базуватися на вивченні двох взаємопов'язаних, але протилежних елементів, якими є механізм вчинення злочину конкретного виду та діяльність правоохоронних органів із розслідування цього злочинного делікту.

Результати дослідження злочинних механізмів відображені у криміналістичній характеристиці та її елементах як інформаційній моделі злочину. Саме криміналістична характеристика сприяє таким процесам: 1) розробленню окремих методик розслідування; 2) побудові типових програм і моделей розслідування злочинів; 3) визначенню напряму розслідування конкретного злочину [1, с. 11].

Проблемами розроблення ефективних криміналістичних механізмів протидії злочинності в різні часи займалися такі вчені, як В.А. Журавель [2], В.О. Коновалова [3], В.Е. Корноухов [4], Ю.М. Чорноус [5], Б.В. Щур [6], В.М. Шевчук [7] та інші. Питанням боротьби зі злочинами у сфері інформаційних технологій присвятили свої наукові дослідження О.І. Мотлях [8], Л.П. Паламарчук [9], Д.В. Пашнєв [10], І.Р. Шинкаренко [11] та інші.

Однак слід зазначити, що, враховуючи розвиток науково-технічного прогресу, високих технологій, зростання рівня електронних комунікацій між людьми, злочинний світ також не стоїть на місці. З'являються нові способи злочинних зазіхань, механізми вчинення правопорушень, знаряддя і засоби. Все це висуває вимогу постійного доопрацювання наявних методик розслідування злочинів та розроблення нових. Хоча Розділ 16 «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» у Кримінальному кодексі України з'явився давно і, здавалося б, сьогодні повинні бути відпрацьовані методики розслідування зазначених у ньому злочинів, однак реалії сьогодення вказують на наявні проблеми, пов'язані з практичною реалізацією притягнення до відповідальності винних осіб через неоднозначність тлумачення норм закону та відставання методичного забезпечення процесу розслідування.

Метою статті є дослідження обстановки вчинення несанкціонованих дій з інформацією, яка обробляється в електронному вигляді особами, які мають право доступу до неї.

Зокрема, у 16 розділі КК України зазначена ст. 362, яка передбачає відповідальність за несанкціоновані дії з інформацією, що обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях інформації, вчинені особою, яка має право доступу до неї.

Обов'язковою умовою злочинного механізму зазначеного кримінального правопорушення є несанкціонована дія з інформацією. У Законі України «Про захист інформації в інформаційно-телекомунікаційних системах» наводиться дефініція поняття «несанкціоновані дії щодо інформації в системі», до яких належать такі, що проводяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства. Згідно зі ст. 1 даного Закону доступ до інформації в системі – це отримання користувачем можливості обробляти інформацію в системі. Порядок доступу до інформації в системі – це умови отримання користувачем можливості обробляти інформацію в системі та правила її обробки. Обробка інформації в системі – це виконання однієї або кількох операцій, зокрема збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрація, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів.

Виникає питання відносно того, хто ж все таки встановлює правила та умови обробки інформації, адже згідно зі ст. 4 Закону порядок доступу до інформації визначає її володілець. Відповідно до ст. 1 порядок доступу до інформації в системі – це умови отримання користувачем можливості обробляти інформацію в системі та правила обробки цієї інформації. А згідно зі ст. 8 умови обробки інформації в системі визначаються власником системи відповідно до договору з володільцем інформації, якщо інше не передбачене законодавством.

Привертає увагу те, що в Законі встановлено обов'язок власника системи забезпечити захист інформації. Однак у ст. 1 Закону наводиться визначення тільки технічного захисту інформації та комплексної системи захисту інформації.

Технічний захист інформації – це вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до неї. Комплексна система захисту інформації – це взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації [12]. У ч. 2 ст. 8. визначено, що державні інформаційні ресурси та інформація з обмеженим доступом, вимогу щодо захисту якої встановлено законом, повинні оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством.

Отже, в Законі визначено обов'язок власника системи забезпечити комплексний захист інформації тільки стосовно державних інформаційних ресурсів. Чи означає це, що у всіх інших випадках власник системи забезпечує тільки технічний захист інформації відповідно до умов договору між ним і володільцем інформації? Відповіді на це питання Закон не дає.

Таким чином, несанкціоновані дії з інформацією – це дії, пов'язані з порушенням встановлених правил володільцем інформації, який згідно зі ст. 4 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» визначає порядок доступу до інформації, перелік користувачів та їх повноваження стосовно цієї інформації. Отже, особа, якій належать права на інформацію, повинна визначити певні правила, за якими законні користувачі (особи, які мають право доступу до такої інформації) можуть здійснювати дії, пов'язані з її обробкою. Якщо така інформація перебуває в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах, необхідно враховувати, що володілець інформації і власник системи (мережі) – не завжди та сама особа. Встановлені володільцем правила обробки інформації повинні бути погоджені в контексті практичної реалізації з власником системи через укладення договору, а власник системи забезпечує захист інформації в системі в порядку та на умовах, визначених у договорі, якщо інше не передбачено законом.

Отже, вести мову про несанкціоновані дії з інформацією, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях інформації, вчинені особою, яка має право доступу до неї, можна за сукупності таких умов: 1) володільцем інформації були визначені умови та правила отримання й обробки інформації; 2) власник електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж розробив та впровадив заходи захисту інформації в системі; 3) власник системи розробив правила її роботи; 4) між володільцем інформації та власником системи укладений договір щодо порядку доступу до інформації та її захисту; 5) злочинець має доступ до інформації на законних підставах; 6) злочинець виконав хоча б одну із дій, а саме: несанкціоновану зміну, знищення, блокування, перехоплення або копіювання інформації; 7) несанкціоноване перехоплення або копіювання інформації призвело до її витоку.

Аналіз змісту зазначеної статті дозволяє виділити декілька таких способів несанкціонованих дій з інформацією: по-перше, несанкціоновані дії зі зміни, знищення або блокування інформації, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях інформації; по-друге, несанкціоноване перехоплення або копіювання інформації.

Пояснення суті деяких способів наведене у ст. 1 Закону або логічно витікає із визначення термінів. Знищення інформації – це дії, внаслідок яких інформація в системі зникає. Блокування інформації – це дії, внаслідок яких унеможливлюється доступ до інформації в системі. Зміна інформації – це дії щодо інформації в системі, внаслідок яких змінюється її зміст [12].

Визначення несанкціонованого перехоплення в Законі не наводиться, однак в п. 3.1.13 спільного наказу СБУ та Адміністрації державної служби спеціального зв'язку та захисту інформації України № 1519/533 від 4 вересня 2018 року «Технічні засоби для здійснення уповноваженими органами оперативно-розшукових заходів та негласних слідчих (розшукових) дій у телекомунікаційних мережах загального користування України. Загальні технічні вимоги» роз'яснюється, як розуміти перехоплення телекомунікацій. З огляду на аналіз наведеної норми можна визначити, що несанкціоноване перехоплення – це незаконні дії, пов'язані зі спостереженням, відбором за визначеними ознаками та фіксацією сеансів зв'язку із застосуванням спеціальних технічних засобів.

Тлумачення категорії «копіювання інформації» також не наводиться в Законі, однак з урахуванням загальноприйнятого розуміння можна визначити, що несанкціоноване копіювання інформації, яка обробляється в ЕОМ (комп'ютерах), автоматизованих системах чи комп'ютерних мережах – це здійснення без дозволу власника переносу інформації або її частини з одного фізичного носія на інший. Під час переносу відбувається зчитування інформації з одного носія

та її записування на інший без зміни цілісності, властивостей та функцій інформації [13].

Вчиненню дій, передбачених ст. 362 КК України, сприяє й те, що на підприємствах, установах, де використовуються відомості в електронній формі, у багатьох випадках відсутні внутрішні документи, інструкції, що регламентують доступ співробітників до документів з інформацією. У таких інструкціях обов'язково повинно бути відображено таке: 1) функції керівництва у сфері захисту інформації; 2) механізм обліку інформації; 3) механізм забезпечення збереження інформації; 4) механізм доступу до відомостей представників правоохоронних та контролюючих органів; 5) порядок розповсюдження інформації; 6) види відповідальності за розголошення інформації; 7) термін, протягом якого діють спеціальні правила обробки інформації в системі за допомогою технічних і програмних засобів стосовно збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання інформації.

Несанкціонованим діям з інформацією також сприяють системні порушення співробітниками таких норм: 1) правил організації технічного захисту територій і приміщень, що охороняються, мереж та систем, що забезпечують функціонування систем життєдіяльності; 2) порядку експлуатації систем обробки та передачі інформації; 3) порядку ведення службової інформації стосовно генерації електронних ключів та паролів доступу; 4) порядку оперативного контролю за функціонуванням системи захисту інформації; 5) порядку реєстрації та аналізу дій користувачів; 6) порядку обліку, зберігання та видачі користувачам носіїв конфіденційної інформації; 7) порядку допуску до приміщень, де здійснюється автоматична обробка даних [14, с. 105].

Отже, говорячи про обстановку вчинення несанкціонованих дій особою, яка має право доступу до інформації, що обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях інформації, необхідно виокремлювати чинники об'єктивного і суб'єктивного характеру, тобто законодавчу неврегульованість деяких дефініцій диспозиції ст. 362 КК України та недоліки в організації роботи підприємств, установ та організацій стосовно інформації, яка обробляється в електронному вигляді.

ЛІТЕРАТУРА

1. Криміналістика : підручник : у 2 т. Т. 2 / В.Ю. Шепітько, В.А. Журавель, В.О. Коновалова та ін. ; за ред. В.Ю. Шепітька. Харків : Право, 2019. 328 с.
2. Журавель В.А. Криміналістичні методики: сучасні наукові концепції : монографія. Харків : Апостіль, 2012. 304 с.
3. Колесниченко А.Н. Криминалистическая характеристика преступлений : учебное пособие. Харьков : Юрид. ин-т, 1985. 93 с.
4. Корноухов В.Е. Методика расследования преступлений: теоретические основы : монография. Москва : Норма, 2018. 224 с.
5. Чорноус Ю.М. Криміналістичне забезпечення розслідування злочинів : монографія. Вінниця : «Нілан-ЛТД», 2017. 492 с.
6. Щур Б.В. Теоретичні основи формування та застосування криміналістичних методик : монографія. Харьков : Харків юрид., 2010. 320 с.
7. Шевчук В.М. Тактичні операції у криміналістиці: теоретичні засади формування та практика реалізації : монографія. Харків : «Апостіль», 2013. 440 с.
8. Мотлях О.І. Питання методики розслідування злочинів у сфері інформаційних комп'ютерних технологій : автореф. дис. ... канд. юрид. наук : 12.00.09 «Кримінальний процес та криміналістика. Судова експертиза». Київ : Б. в., 2005. 20 с.
9. Паламарчук Л.П. Криміналістичне забезпечення розслідування незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж : автореф. дис. ... канд. юрид. наук : 12.00.09 «Кримінальний процес та криміналістика. Судова експертиза». Київ : Б. в., 2005. 18 с.
10. Пашнєв Д.В. Використання спеціальних знань при розслідуванні злочинів, вчинених із застосуванням комп'ютерних технологій : автореф. дис. ... канд. юрид. наук : 12.00.09 «Кримінальний процес та криміналістика. Судова експертиза». Харків, 2007. 20 с.
11. Преступления в сфере использования компьютерной техники: квалификация, расследование и противодействие : моногр. / И.Р. Шинкаренко, В.О. Голубев, Н.В. Карчевський, И.Ф. Хараберюш. Донецк : РВВ ЛДУВС, 2007. 267 с.
12. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 року № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80 (дата звернення: 10.09.2019).
13. Розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» : новий коментар. URL: http://www.crime-research.ru/criminal_code/ (дата звернення: 09.09.2019).
14. Сербин И.С. Криминалистическое обеспечение защиты коммерческой тайны : монография. Москва : «Юрлитинформ», 2008. 152 с.