МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет «Одеська юридична академія»

ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ В УМОВАХ ВІЙНИ ТА ГЛОБАЛЬНИХ ВИКЛИКІВ XXI СТОЛІТТЯ: СИНЕРГІЯ НАУКОВИХ, ОСВІТНІХ ТА ТЕХНОЛОГІЧНИХ РІШЕНЬ

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

19 травня 2023 року

У двох томах

Том 2

Видавництво
«Юридика»
2023

УДК 005.332.2(4):316.42(477)"364""20"(062.552)
Є24

Рекомендовано до друку Вченою радою
Національного університету «Одеська юридична академія»
(протокол № 3 від 16.06.2023 р.)

За загальною редакцією **С. В. Ківалова.**

Відповідальний за випуск **М. Р. Аракелян.**
Матеріали видано в авторській редакції.

Європейські орієнтири розвитку України в умовах війни та
Є24 глобальних викликів XXI століття: синергія наукових, освітніх та технологічних рішень : у 2 т. : матеріали Міжнар. наук.-практ. конф. (м. Одеса, 19 травня 2023 р.) / за загальною редакцією С. В. Ківалова. – Одеса : Видавництво «Юридика», 2023. – Т. 2. – 828 с.

ISBN 978-617-8263-40-9

Матеріали Міжнародної науково-практичної конференції «Європейські орієнтири розвитку України в умовах війни та глобальних викликів XXI століття: синергія наукових, освітніх та технологічних рішень». У другому томі збірника відображено наукові напрацювання вчених, практиків, військовослужбовців у теоретичній та емпіричній площині в умовах повномасштабного військового вторгнення у сферах адміністративного права та процесу, фінансового, морського та митного права, організації та вдосконалення судоустрою, прокуратури, інших правоохоронних органів, адвокатури. Висвітлено питання кримінального права, кримінально-процесуальних аспектів кримінального провадження та кримінологічних особливостей протидії злочинності в умовах воєнного стану, криміналістики, судової експертизи, психології та медицини у забезпеченні судочинства, цивільного та сімейного права, інтелектуальної власності та патентної юстиції, цивільного судочинства, господарського права та процесу. Розглянуто актуальні питання діяльності сучасних бібліотек у закладах вищої освіти, фізичної підготовки здобувачів вищої освіти.

Збірник розраховано на наукових та науково-педагогічних працівників, здобувачів вищої освіти, практичних працівників у сферах юридичної, економічної, соціологічної, політологічної, психологічної, філологічної наук, журналістики та кібербезпеки тощо.

УДК 005.332.2(4):316.42(477)"364""20"(062.552)

ISBN 978-617-8263-37-9 (у 2 т.)
ISBN 978-617-8263-40-9 (т. 2)

ВЕЙЦ АРКАДІЙ МИХАЙЛОВИЧ

Національний університет «Одеська юридична академія», аспірант кафедри криміналістики

СЛІДОВА КАРТИНА ПРИ ВЧИНЕННІ КІБЕРЗЛОЧИНІВ ЗА УЧАСТЮ СЛУЖБОВОЇ ОСОБИ АБО ТАКОЇ, ЯКА ЗДІЙСНЮЄ ПРОФЕСІЙНУ ДІЯЛЬНІСТЬ, ПОВ'ЯЗАНУ З НАДАННЯМ ПУБЛІЧНИХ ПОСЛУГ

При вчиненні кіберзлочинів не має державних кордонів. Вони можуть бути скоєні в будь-який час з будь-якої точки землі із задіянням будь-якої мережі, в тому числі із використанням або посяганням на інформаційні ресурси будь-якої держави. При цьому злочинна діяльність у кіберпросторі являє собою систему об'єднаних загальними мотивами і цілями злочинних дій, операцій та епізодів, розрахована на відносно тривалий період і підготовку, що включає в себе планування, здійснення, маскування та протидію її викриттю [1]. Тож, вдалим прикриттям злочинної діяльності стає статус злочинця – службова особа. Саме офіційна можливість доступу до певної інформації з обмеженим доступом або до електронних ресурсів дозволяє злочинцю тривалий час бути відсутнім у полі зору правоохоронців, яким вже відомі окремі факти такої злочинної діяльності. У цьому сенсі особливо важливим буде розуміння типової слідової картини вчинення кіберзлочинів за участю службовові особи або такої, яка здійснює професійну діяльність, пов'язану з наданням публічних послуг.

Сліди як елемент криміналістичної характеристики ми розглядаємо у значенні складного утворення, що включає в себе сліди-предмети, сліди-відображення, сліди-речовини. Аналіз матеріалів судово-слідчої практики підтверджує, що механізм слідоутворення аналізованої злочинної діяльності за участю службової особи тісно пов'язаний з механізмом вчинення самого злочину. Тому для систематизації слідів, які вказують на залучення до злочинної діяльності в кіберпросторі службової особи, доцільно поділити їх на дві умовні групи:

1) основні сліди вчинення кіберзлочину (типова слідова картина);

2) додаткові сліди вчинення кіберзлочину (за певних ситуаційних обставин щодо участі службової особи).

Сліди виявлені у комп'ютері (у його системному блоці на жорсткому диску «вінчестері»), машинних носіях інформації (магнітно-оптичних дисках, магнітних стрічках тощо) є завжди основними слідами-відображеннями, до них традиційно відносять:

1) зміни у файловій системі: копії чужих файлів (при неправомірному доступі); файли, де зафіксовано звернення до сайтів Інтернету; файли із шкідливими програмами; програмне забезпечення для підбору паролів неправомірного доступу в Інтернет, або іншого проникнення в комп'ютерні мережі, а також містить функції зі знищення, блокування, модифікації або копіювання інформації, порушення роботи ЕОМ, системи ЕОМ, мережі; ознаки, що свідчать про

застосування спеціальної програми для незаконного проникнення в комп'ютерну мережу (ознаки внесення до програми змін, спрямованих на подолання інформаційного захисту) тощо;

2) зміни конфігурації комп'ютерного обладнання: невідповідність внутрішнього пристрою комп'ютера технічної документації на нього (внесення в конструкцію комп'ютера вбудованих пристроїв, додаткових жорстких дисків, пристроїв для розширення оперативної пам'яті, зчитування оптичних дисків тощо); наявність додаткових блоків із ворожими функціями; нестандартні периферійні пристрої та ін. У разі використання при скоєнні злочину телекомунікаційних мереж для встановлення джерела «нападу» цифрові сліди містяться в кожному пристрої у ланцюжку комунікації. Такі відомості можна отримати від провайдерів послуг (Інтернету, телекомунікаційних засобів, наземної лінії зв'язку, стільникового та супутникового зв'язку, приватної мережі), що стосуються місця відправлення повідомлення, тривалості, характеру діяльності при повідомленні (виключаючи його зміст та адресата).

Будь-які матеріальні сліди дають можливість у межах криміналістичної характеристики встановлювати кореляційні зв'язки із механізмом, але виявлені при окремих обставинах комплекси слідів можуть вказувати на залучення до вчинення злочину службової особи. Ситуаційна обумовленість слідової картини зумовлена тим, що за участю службової особи вчиняються лише окремі категорії кіберзлочинів за певних обставинах, у певний час і певних місцях. Сліди пам'яті ми не розглядаємо в цьому контексті, адже вони є надто різноманітними, суттєво залежать від суб'єктивних даних про особу як їх носія, вони практично не піддаються встановленню кореляційних зв'язків.

Акцентуємо, що основні кіберзлочини, що вчиняються за участю службової особи або такої, яка здійснює професійну діяльність, пов'язану з наданням публічних послуг, є: 1) несанкціонованими втручаннями в роботу комп'ютерних технологій (без мети збуту або розповсюдження інформації з обмеженим доступом, пов'язані зі сферами публічної служби або з такою метою щодо інформації, яка обробляється в державних інформаційних ресурсах); 2) несанкціонованими діями з інформацією (поєднані з заволодіннями майном у сфері підприємницької діяльності або з професійною діяльністю; 3) незаконними діями з платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення, пов'язані зі зловживанням та перевищенням влади або службових повноважень в сфері кредитно-фінансової діяльності [2]. Тож, обстановка вчинення таких злочинів буде характеризуватися неналежним підходом в установі, підприємстві, організації до управління інформаційною безпекою та відсутністю належного ставлення до забезпечення кібербезпеки, оцінки ризиків порушення кібербезпеки.

Не дивлячись на те, що ризик постійно інтегрований у процес прийняття рішень, операційну та інвестиційну діяльність підприємств та установ як приватного, так і державного сектору, ризик сфери захисту інформації є вимірною категорією, яку можна оцінити,

допустити ймовірність конкретної події, передбачити її та здійснити заходи попередження: організаційні, технічні чи управлінські. Тож, додаткові сліди вчинення кіберзлочину за участю службової особи будуть міститись:

– в документації, що засвідчує стан системи кіберзахисту установи, організації, підприємства, записи про початок та закінчення певних інформаційних процесів, режими роботи обладнання, його стан, ремонт тощо (організаційний аспект);

– в інформаційно-телекомунікаційних технологіях сфери захисту, моніторингу та обробки інформації з обмеженим доступом (персональних даних, відомостей, що становлять державну, комерційну, банківську, іншу професійну таємницю). Параметри, які захищають конфіденційність користувача, в більшості технологій сьогодні запрограмовані за замовчуванням. Тож, сучасні пристрої та програми безпосередньо ведуть облік операцій обробки даних, записують інформацію щодо адміністраторів новостворених даних, попереджують адміністратора даних про виправлення, блокування, видалення або знищення всіх або частини даних, накладення тимчасової або повної заборони обробки тощо (технічний аспект);

– сліди людини (рук, взуття, губ), предмети особистого побуту (записники, одяг, посуд, прилади та пристосування). Наявність слідів конкретних осіб в певний проміжок часу, в певному місці, як правило, на конкретному робочому місці можуть служити доказом їхньої причетності до злочину.

Отже, сліди вчинення кіберзлочинів за участю службовові особи або такої, яка здійснює професійну діяльність, пов'язану з наданням публічних послуг, є різноманітними, зумовлені станом кібербезпеки на певному об'єкті захисту та потребують подальшого дослідження в межах класифікаційних підвидів злочину.

Список використаних джерел:

1. Самойленко О. А. До питання механізму вчинення злочинів у кіберпросторі. Теорія та практика судової експертизи і криміналістики : матеріали Всеукраїнської науково-практичної конференції з нагоди 85-річчя доктора юридичних наук, професора Ніни Іванівни Клименко (м. Київ, 27 лютого 2018 року). Київ, Маріуполь, 2018. 412 с. С. 297–298.
2. Вейц А. М. Криміналістична класифікація кіберзлочинів, вчинених за участю службової особи або такої, яка здійснює професійну діяльність, пов'язану з наданням публічних послуг. *Прикарпатський юридичний вісник*. 2022. № 6 (47). С. 170–176.

Ключові слова: механізм слідоутворення, кібербезпека, кіберзлочини, комплекс, слідова картина, службова особа.

Key words: trace formation mechanism, cyber security, cyber crimes, complex, trace pattern, official.