УДК 343.98
DOI https://doi.org/10.32782/pyuv.v6.2022.33

А. М. Вейц
orcid.org/0000-0002-7454-1534
аспірант кафедри криміналістики
Національного університету «Одеська юридична академія»

КРИМІНАЛІСТИЧНА КЛАСИФІКАЦІЯ КІБЕРЗЛОЧИНІВ, ВЧИНЕНИХ ЗА УЧАСТЮ СЛУЖБОВОЇ ОСОБИ АБО ТАКОЇ, ЯКА ЗДІЙСНЮЄ ПРОФЕСІЙНУ ДІЯЛЬНІСТЬ, ПОВ'ЯЗАНУ З НАДАННЯМ ПУБЛІЧНИХ ПОСЛУГ

Електронна освіта, електронна медицина, електронна комерція, а також багато інших суспільно-політичних та соціально-економічних сфер діяльності сучасного суспільства консолідовані із виконанням організаційно-розпорядчих чи адміністративно-господарських функцій певними службовими особами. Тому все частіше не діє класична схема протидії кіберзлочинності, що представлена послідовністю «бачити кібер-аномалії та атаки, їх аналізувати, реагувати, захищати, запобігати» [1]. Через вчинення кіберзлочинів за участю службової особи технологія такої злочинної діяльності зазнає суттєвої трансформації. Такий кіберзлочин утворюється ланцюгом злочинних дій. Розмаїття складів кіберзлочинів в кримінально-правовому сенсі та їх різновидів в криміналістичному зумовлює необхідність розв'язання щодо них класифікаційного завдання.

Питання криміналістичної класифікації кіберзлочинів розглядали багато науковців (В. М. Бутузов, С. А. Буяджи, А. Ф. Волобуєв, І. О. Воронов, С. В. Демедюк, М. В. Карчевський, О. І. Котляревський, М. О. Кравцова, О. М. Лепеха, М. Ю. Літвінов, О. І. Мотлях, І. М. Осика, Л. П. Паламарчук, Д. В. Пашнєв, А. В. Реуцький, О. А. Самойленко та інші), але це здійснювали без врахування в цілому специфіки учасників злочинної діяльності. **Метою цієї статті** є здійснення криміналістичної класифікації кіберзлочинів, вчинених за участю службової особи або такої, яка здійснює професійну діяльність, пов'язану з наданням публічних послуг, визначення критеріїв такої систематизації злочинів.

Класифікація (лат. clasis – розряд і fasere – робити) – це особливий випадок застосування логічної операції поділу обсягу поняття, який являє собою деяку сукупність поділу (поділ будь-якого класу на види, поділ цих видів тощо [2, с. 177]. Вибір підстави класифікації кримінальних правопорушень залежить від цілей, що ставляться перед такою класифікацією, а вони, у свою чергу, підлеглі цілям і завданням відповідної науки. Криміналістичну класифікацію злочинів В. Ю. Шепітька називає необхідною умовою ефективного пізнання окремої методики та розроблення криміналістичних рекомендацій [3]. Найчастіше підставами такої класифікації обираються кримінально-правові та криміналістичні ознаки конкретної злочинної діяльності.

Криміналістична класифікація кіберзлочинів, вчинених за участю службової особи або такої, яка здійснює професійну діяльність, пов'язану з наданням публічних послуг, передбачає розгляд комплексу злочинів вказаної групи та виділення класифікаційних підгруп злочинної діяльності. Необхідність в цьому пояснюється тим, що кожний епізод такої діяльності повинен одержати свою кримінально-правову оцінку і націлити слідчого на коло обставин, що підлягають встановленню. Як кіберзлочини, так й злочинна службова діяльність, складається з різноманітних кримінальних правопорушень, що відіграють в утворюваному комплексі злочинів при кваліфікації різну за значенням роль, зокрема є основні та допоміжні (додаткові) злочини.

Основними злочинами, що розглядаються в такому комплексі, є кіберзлочини, переважно передбачені ст. 361–363-1 КК України. Частіше за все саме вони виконують роль базових, безпосередньо їх вчинення призводить до досягнення бажаного результату злочинної діяльності. Але в цьому сенсі потрібно акцентуватися на декількох важливих для цього дослідження позиціях.

По-перше, визначитися який зміст терміна «кіберзлочин» вважати основним для цілей цієї класифікації. Транснаціональний та організаційний аспект вчинення такого злочину, відмінності підходів у національному законодавстві впливають на перелік злочинів, які фактично відносять дослідники до категорії «кіберзлочин». Для цілей класифікації кіберзлочинів, вчинених за участю службової особи або такої, яка здійснює професійну діяльність, пов'язану з наданням публічних послуг, ми будемо спиратися на суто законодавчий критерій класифікації. За змістом Конвенції про кіберзлочинність, яку Україна ратифікувала 7 вересня 2005 року, усі запропоновані нею склади кримінальних правопорушень, що утілено в КК України, ми відносимо до категорії «кіберзлочин», зокрема: ст. ст. 163, 176, 185, 190, 200, 301, 361–363-1 КК України.

По-друге, на підставі аналізу слідчо-судової практики ми можемо констатувати, що у наведеному переліку кримінальних правопорушень за участю службових осіб або таких, що здійснюють професійну діяльність, пов'язану із наданням публічних послуг, вчиняються переважно злочини, передбачені ст. ст. 200, 361–363-1 КК України. При цьому не залишимо без уваги й злочині суміжні з цими кримінальними правопорушеннями. В окремих з них часто фігурують невстановлені особи, які виходячи з матеріалів справ мали доступ до інформації, що зберігається в електронних ресурсах з обмеженим доступом, відповідно реальною є версія щодо віднесення останніх до категорії службових осіб.

Додаткові злочини залежатимуть від конкретної сфери людської (суспільної) діяльності, в якій вчиняється кіберзлочин за участю службової особи або такої, яка здійснює професійну діяльність, пов'язану з наданням публічних послуг. Спроби класифікації з цієї підстави вже мали місце в криміналістичній науці, але вони стосувались суто службових злочинів. Так, О. В. Пчеліна при класифікації злочинів у сфері службової діяльності, запропонувала 11 підгруп таких злочинів: 1) злочини, що пов'язані з реалізацією функцій нагляду та контролю; 2) злочини, що пов'язані з охороною та захистом прав, свобод і законних інтересів людини та громадянина; 3) злочини, що пов'язані соціальним забезпеченням; 4) злочини, що пов'язані наданням житлово-комунальних послуг; 5) злочини, що пов'язані наданням освітніх послуг; 6) злочини, що пов'язані наданням медичних послуг і послуг оздоровлення та відпочинку; 7) злочини, що пов'язані з наданням транспортних послуг, наданням послуг зв'язку; 8) злочини, що пов'язані з наданням послуг з фізичної культури і спорту; 9) злочини, що пов'язані з видачею дозволів, ліцензій і патентів; 10) злочини, що пов'язані з господарюванням; 11) злочини, що пов'язані з формуванням, розподілом, використанням бюджетних коштів і розпорядженням іншим державним, комунальним майном тощо [4]. Навіть кримінальний закон чітко передбачає перелік злочинів у сфері службової діяльності та професійної діяльності, пов'язаної з наданням публічних послуг. Вказана кримінально-правова диференціація поділяється на чотири групи, залежно від того, яким саме суспільним відносинам спричиняється шкода. Перша об'єднує злочини у сфері службової діяльності, яка здійснюється тільки в органах державної влади, місцевого самоврядування і юридичних особах публічного права (статті 364, 365, 368, 368-2, 369, 369-2 КК). До другої входять злочини, вчинювані у сфері службової діяльності, яка здійснюється лише в юридичних особах приватного права (статті 364-1, 365-1, 368-3 КК). Третя група об'єднує злочини, які можуть бути вчинені у сфері службової діяльності, що здійснюється в юридичних особах як публічного, так і приватного права (статті 366, 367, 370 КК). До четвертої групи входять злочини, які вчиняються у сфері професійної діяльності, пов'язаної з наданням публічних послуг (статті 365-2, 368-4 КК). Однак, потрібно акцентувати, що кримінальний закон при цьому не передбачає чіткого переліку злочинних діянь службових осіб. Такі злочини знаходяться в різних розділах КК України, об'єднує їх лише загальна ознака об'єктивної сторони – вчиняються вони шляхом зловживання службовим становищем. Зокрема тут мова йде про наступні склади кримінальних правопорушень:

- у сфері власності: привласнення, розтрата майна або заволодіння ним шляхом зловживання службовим становищем (ст. 191 КК України);
- у сфері громадської безпеки: викрадення, привласнення, вимагання вогнепальної зброї, бойових припасів, вибухових речовин чи радіоактивних матеріалів або заволодіння ними шляхом шахрайства або зловживання службовим становищем (ст. 262 КК України);
- у сфері обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів: викрадення, привласнення, вимагання наркотичних засобів, психотропних речовин або їх аналогів чи заволодіння ними шляхом шахрайства або зловживання службовим становищем (ст. 308 КК України); викрадення, привласнення, вимагання прекурсорів або заволодіння ними шляхом шахрайства або зловживання службовим становищем (ст. 312 КК України); викрадення, привласнення, вимагання обладнання, призначеного для виготовлення наркотичних засобів, психотропних речовин або їх аналогів, чи заволодіння ними шляхом шахрайства або зловживання службовим становищем та інші незаконні дії з таким обладнанням (ст. 313 КК України);
- у сфері державної влади, місцевого самоврядування та об'єднань громадян: викрадення, привласнення, вимагання документів, штампів, печаток, заволодіння ними шляхом шахрайства чи зловживання службовим становищем або їх пошкодження (ст. 357 КК України);
- у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж: викрадення, привласнення, вимагання комп'ютерної інформації або заволодіння нею шляхом шахрайства чи зловживання службовим становищем (ст. 362 КК України);
- у сфері несення військової служби: викрадення, привласнення, вимагання військовослужбовцем зброї, бойових припасів, вибухових речовин, засобів пересування, військової та спеціальної техніки чи іншого військового майна, а також заволодіння ними шляхом шахрайства

або зловживання службовим становищем (ст. 410 КК України); зловживання військовою службовою особою владою або службовим становищем (ст. 423 КК України); перевищення військовою службовою особою влади чи службових повноважень (ст. 424 КК України);

- у сфері службової діяльності: зловживання владою або службовим становищем (ст. 364 КК України); перевищення влади або службових повноважень працівником правоохоронного органу (ст. 365 КК України). Такий розподіл службових злочинів в Особливій частині КК України вказує на те, що характер та обсяг повноважень службової особи має важливе значення саме в межах окремої групи злочинів, виділеної за критерієм суспільної небезпечності злочинів.

На нашу думку прагнення прискорити обіг традиційних паперових документів, підвищити доступність надання послуг клієнту зумовлює однаковий рівень комп'ютеризації як державного і громадського апарату, так й апарату управління підприємствами, установами і організаціями (не залежно від форми власності). Тому щодо кіберзлочину для досягнення злочинного результату не має вирішального значення відомча чи галузева належність державного органу, форма власності підприємсва чи установи, службова особа яких залучена до злочинної групи. Механізм такої злочинної діяльності зумовлений також сферою діяльності службової особи у широкому розумінні (у значенні ч. 3, 4 ст. 18 КК), характером та обсягом її повноважень.

Потрібно також пам'ятати, що само по собі активне створення та модернізація органів забезпечення кіберзахисту (на рівні різних відомств, установ, підприемств та організацій створення центрів (відділів) забезпечення кібербезпеки або кіберзахисту) виступає одним з важливих детермінантів злочинної діяльності службових осіб в кіберпросторі, визначає стабільність, епізодичність та складність кіберзлочинів, адже, на підставі аналізу матеріалів судово-слідчої практики, ми можемо стверджувати, що на більше ніж половину службових осіб – учасників кіберзлочину – були покладені функції захисту інфорормації з обмеженим доступом.

Тож, на підставі аналізу матеріалів судово-слідчої практики, виходячи з кримінально-правової сутності досліджуваного виду злочинів, сфери діяльності службової особи та обсягу її повноважень (як сукупний критерій криміналістичної класифікації таких злочинів), ми можемо виділити наступні п'ять видів кіберзлочинів за участю службової особи або такої, яка здійснює професійну діяльність, пов'язану з наданням публічних послуг.

1. Несанкціоновані втручання в роботу комп'ютерних технологій без цілі сбуту або розповсюдження інформації з обмеженим доступом, пов'язані зі сферами публічної служби. Термін «публічна служба» на законодавчому рівні визначено ст. 4 Кодекса адміністративного судочинства України, згідно цій статті публічна служба – це діяльність на державних політичних посадах, професійна діяльність суддів, прокурорів, військова служба, альтернативна (невійськова) служба, дипломатична служба, інша державна служба, служба в органах влади Автономної Республіки Крим, органах місцевого самоврядування. Всі службові особи (на державних, політичних посадах, в органах місцевого самоврядування, в мілітаризованих службах (у Збройних Силах України, Службі безпеки України, органах поліції, державній прикордонній службі тощо), судді), за участю яких з різних мотивів вчиняється кіберзлочн, мають доступ до тих чи інших державних інформаційних ресурсів.

Така підгрупа злочинів класифікується традиційно за сукупністю статей КК України, зокрема: ст. 361 (а також ст. 362, якщо підчас слідства встановлено конкретну службову особу, залучену до вчинення злочину, яка безпосередньо мала право доступу до предмета посягання, та використала конфіденційну інформацію, пов'язану із цим), а також ст. 368, або ст. 364, або ст. 376-1 та ст. 366 КК України. Так, наприклад, вироком Личаківського районного суду м. Львова було визнано винним гр. О. Будучи службововою особою, наділеною організаційно-розпорядчими функціями, а також правом доступу до комп'ютерної програми «Діловодство спеціалізованого суду» О. з особистих мотивів під чужим ім'ям та логіном вніс до програми неправдиві відомості про зміну способу та порядку виконання окремих рішень та про визнання дійсним договору про заміну кредитора у зобов'язанні (змінив окремі ухвали суду)[5].

2. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається, обробляється в державних інформаційних ресурсах. Наведена підгрупа злочинів типово класифікується за сукупністю двох статей КК України, зокрема: ст.361-2 та ст. 368 КК України. Показовим в цьому сенсі є кримінальне провадження стосовно гр. К., який, перебуваючи на посаді оперуповноваженого сектору кримінальної поліції, шляхом здійснення доступу до баз даних МВС України отримав та незаконно скопіював в приміщенні службовового кабінету поліції персональні відомості про осіб. Після цього з корисливих мотивів, використовуючи мессенджер «Телеграмм» розміщав оголошення про можливість придбати інформацію з обмеженим доступом, зокрема відомості про персональні дані осіб [6].

3. Несанкціоновані дії з інформацією, що міститься в комп'ютерних технологіях, поєднені

з заволодіннями майном у сфері підприємницької діяльності (в тому числі й кредитно-фінансовій сфері). Наведена підгрупа злочинів типово класифікується за сукупністю двох статей КК України, зокрема: ст. 361-2 та ст. 368 КК України. Підприємництво поширене у всіх сферах економіки, воно поділяється за видами залежно від сфер та галузей економіки, де здійснюється підприємницька діяльність. В кожній такій галузі воно має має істотні властивості за формою і особливо за змістом операцій та способами їх здійснення. На даному етапі розкриття обраного нами предмета дослідження ми підкреслимо, що такі кіберзлочини типово класифікується за сукупністю ст. 362 (іноді також ст. 361) та ст. 191 КК України. Так, наприклад, обвинувачений О., знаходячись на посаді начальника відділення ПАТ КБ «Надра», маючи покладені на нього обов'язки щодо здійснення керівництва діяльністю відділення фінансової установи, вчинив розтрату коштів потерпілого. Кошти були внесені в банк для подальшого перерахування на рахунок організатора прилюдних торгів як гарантійний внесок за участь у прилюдних торгах. О. вніс у програму дані про відміну касової операції та дав усне розпорядження про видачу невстановленим особам вказаних коштів з каси банку [7].

4. Незаконні дії 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. Типово він кваліфікується за ст.ст. 200, 361 та/або 362 та/або 363 КК України. Наведемо приклад з практики. У червні 2016 р. гр. К., працюючи на посаді фахівця з обслуговування клієнтів у відділенні ПАТ КБ «Приватбанк», перевищуючи надані йому повноваження, нехтуючи відмовою клієнта про надання йому кредитної лінії, вніс до авторизованої сиситеми банківської установи заяву про надання кредитної картки, гроші на якої згодом використав на свої потерби [8].

5. Несанкціоновані дії з інформацією, що міститься в комп'ютерних технологіях, пов'язані з професійною діяльністю. Така професійна діяльність здійснюється, або суб'єктом надання публічних послуг, або службовою особою суб'єкта надання телекомунікаційних послуг. Типово злочинна діяльність за участю таких осіб кваліфікується за сукупністю ст.ст. 362 та/або 363, 365-2 КК України (іноді присутня кваліфікація за ст. 361 КК України, за умови, якщо в ході слідства не була встановлена участь конкретної особи, яка підчас своєї професійної діяльності, пов'язаної із наданням публічних послуг, діяла в цілях вчинення кінцевого злочину в кіберпросторі). Такий ланцюг злочинів часто обирають злочинці, які мають на меті вчинення акту кібертероризма, пошкодження державних інформаційних ресурсів, об'єктів критичної інфраструктури. Оскільки така діяльність створює загрозу заподіяння шкоди зовнішній і внутрішній безпеці держави, кінцева їх кваліфікація здійснюється також за статтями Розділу I «Злочини проти основ національної безпеки України» Особливої частини КК України.

Звернемо увагу, що у законодавстві України наразі визначеним залишається тільки поняття «електронні публічні послуги», зокрема вказаним поняттям позначають послуги, що надаються органами державної влади, органами місцевого самоврядування, підприємствами, установами, організаціями, які перебувають в їх управлінні, у тому числі адміністративні послуги (у тому числі в автоматичному режимі), які надаються з використанням інформаційно-телекомунікаційних систем на підставі заяви (звернення, запиту), поданої в електронній формі з використанням інформаційно-телекомунікаційних систем (у тому числі з використанням Єдиного державного веб-порталу електронних послуг), або без подання такої заяви (звернення, запиту) [9]. При цьому законодавець не дає вичерпного переліку кола осіб, які здійснюють професійну діяльність у сфері публічних послуг. Лише виходячи зі змісту ст.ст. 365-2 та 368-4 КК України, можна констатувати, що до осіб, які здійснюють професійну діяльність, пов'язану з наданням публічних послуг, належать: аудитор, нотаріус, оцінювач, експерт, арбітражний керуючий, незалежний посередник, член трудового арбітражу, третейський суддя або інша особа, яка не є державним службовцем, посадовою особою органу місцевого самоврядування, але здійснює професійну діяльність, пов'язану з наданням публічних послуг. Обсяг та суть повноважень службової особи залученої до вчинення кіберзлочину в цьому сенсі суттєво буде визначає технологію злочинної діяльності.

Наведемо такий показовий приклад, Так, вироком Шевченківського районного суду м. Києва було засуджено гр. О., який обіймаючи посаду адміністратора безпеки, використовував у мережевому обладненні програмне забезпечення, що не відповідало наведеному в проектній документації. В результаті його злочинних дій 16 жовтня 2014 року на веб-сервері сайту Державної міграційної служби України невстановленими особами бути вчинені несанкціоновані дії з інформацією [10].

Отже, при розробленні криміналістичної класифікації кіберзлочинів, вчинених за участю службової особи або такої, яка здійснює професійну діяльність, пов'язану з наданням публічних послуг, потрібно комплексно використовувати як критерій їх систематизації два чинники: ступінь

суспільної небезпечності злочину (кримінально-правовий критерій) та сферу діяльності службової особи (криміналістичний критерій). В середені основної побудови можна також вдаватися до систематизації вказаної категорії злочинів. Розподілити кожний з п'яти наведених нами видів кіберзлочинів на підвиди доцільно, наприклад, за обсягами повноважень службової особи. Це дозволить в подальшому сформувати максимально деталізовану криміналістичну характеристику злочинів і, відповідно, на її підставі обгрунтовану методику їх розслідування.

Література

1. Пресконференція. Національний координаційний центр кібербезпеки. https://www.rnbo.gov.ua/ua/Diialnist/4658.htm
2. Философский словарь. / Под ред. М.М. Розенталя. Изд. 3-е. М.: Политиздат, 1975. 496 с.
3. Шепитько В.Ю. Криминалистика: курс лекций. – Издание второе, переработанное и дополнительное. Х.», 2005. 368 с.
4. Пчеліна О. В. Теоретичні засади формування та реалізації методики розслідування злочинів у сфері службової діяльності : автореф. ... дис. д-ра юрид. наук : 12.00.09. Харків, 2017. 40 с.
5. Вирок в справі №463/1672/17 від 08 вересня 2018 р. Личаківський районний суд м. Львова. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://www.reyestr.court.gov.ua/
6. Вирок в справі № 569/6003/18 від 25квітня 2018 р. Личаківського районного суду м. Львова *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://www.reyestr.court.gov.ua/
7. Вирок в справі №727/3490/15-к від 02 червня 2015 р. Шевченківський районний суд м. Чернівці *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://www.reyestr.court.gov.ua/
8. Вирок в справі №712/14940/17 від 08 лютого 2018 р. Соснівський районний суд м. Черкаси. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://www.reyestr.court.gov.ua/
9. Про особливості надання публічних (електронних публічних) послуг: Закон України № 1689-IX 15 липня 2021 року. URL: https://zakon.rada.gov.ua/laws/show/1689-20#Text
10. Вирок в справі № 761/11540/16-к від 21 квітня 2016 р. Шевченківський районний суд м. Києва. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://www.reyestr.court.gov.ua/

Анотація

Вейц А. М. **Криміналістична класифікація кіберзлочинів, вчинених за участю службової особи або такої, яка здійснює професійну діяльність, пов'язану з наданням публічних послуг.** – Стаття.

Статтю присвячено розв'язанню класифікаційного завдання щодо кіберзлочинів, вчинених за участю службової особи або такої, яка здійснює професійну діяльність, пов'язану з наданням публічних послуг. В статті через розкриття змісту відповідної злочинної діяльності здійснюється визначення критеріїв систематизації відповідної категорії злочинів.

Доведено, що при розробленні криміналістичної класифікації кіберзлочинів, вчинених за участю службової особи або такої, яка здійснює професійну діяльність, пов'язану з наданням публічних послуг, потрібно комплексно використовувати як критерій їх систематизації два чинники: ступінь суспільної небезпечності злочину (кримінально-правовий критерій) та сферу діяльності службової особи (криміналістичний критерій). В статті охарактеризовані п'ять основних видів кіберзлочинів за участю службової особи або такої, яка здійснює професійну діяльність, пов'язану з наданням публічних послуг, зокрема: 1) несанкціоновані втручання в роботу комп'ютерних технологій без цілі збуту або розповсюдження інформації з обмеженим доступом, пов'язані зі сферами публічної служби; 2) несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається, обробляється в державних інформаційних ресурсах; 3) несанкціоновані дії з інформацією, що міститься в комп'ютерних технологіях, поєднені з заволодіннями майном у сфері підприємницької діяльності (в тому числі й кредитно-фінансовій сфері); незаконні дії 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; 5) несанкціоновані дії з інформацією, що міститься в комп'ютерних технологіях, пов'язвані з професійною діяльністю. Акцентується, що в середені основної класифікації можна також вдаватися до систематизації вказаної категорії злочинів. Розподілити кожний з вищенаведених видів кіберзлочинів на підвиди доцільно за обсягами повноважень службової особи. Це дозволить в подальшому сформувати максимально деталізовану криміналістичну характеристику злочинів і, відповідно, на її підставі обгрунтовану методику їх розслідування.

Ключові слова: кіберзлочин, криміналістична класифікація, несанкціоновані дії, публічна послуга, службова особа.

Summary

Veits A. M. **Forensic qualification of cybercrimes committed with the participation of an official or a person engaged in professional activities related to the provision of public services.** – Article.

The article is devoted to solving the classification task regarding cybercrimes committed with the participation of an official or one who carries out professional activities related to the provision of public services. In the article, through the disclosure of the content of the corresponding criminal activity, the criteria for the systematization of the corresponding category of crimes are defined.

It has been proven that when developing a forensic classification of cybercrimes committed with the participation of an official or one who carries out professional activities related to the provision of public services, two factors should be comprehensively used as a criterion for their systematization: the degree of public danger of the crime (crime-legal criterion) and the field of activity of the official (forensic criterion). The article describes five main types of cybercrimes involving an official or one who carries out professional activities related to the provision of public services, in particular: 1) unauthorized interference in the operation of computer technologies without the purpose of sale or distribution of information with limited access , related to the spheres of public service; 2) unauthorized sale or distribution of information with limited access, which is stored and processed in state information resources; 3) unauthorized actions with information contained in computer technologies, combined with seizure of property in the

field of entrepreneurial activity (including the credit and financial field); 4) illegal actions with payment cards and other means of access to bank accounts, electronic money, equipment for their production, associated with abuse and excess of power or official authority in the field of credit and financial activity; 5) unauthorized actions with information contained in computer technologies, related to professional activityIt is emphasized that in the middle of the main classification, it is also possible to resort to the systematization of the specified category of crimes. It is advisable to divide each of the above types of cybercrimes into subtypes according to the scope of the authority of the official. This will allow in the future to form the most detailed criminalistic description of crimes and, accordingly, based on it, a reasonable method of their investigation.

Key words: cybercrime, forensic classification, unauthorized actions, public service, official.