УДК 343.98

О. В. Бородай

ОСОБА ЗЛОЧИНЦЯ ЯК ЕЛЕМЕНТ КРИМІНАЛІСТИЧНОЇ ХАРАКТЕРИСТИКИ НЕСАНКЦІОНОВАНОГО ВТРУЧАННЯ В РОБОТУ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН (КОМП'ЮТЕРІВ), АВТОМАТИЗОВАНИХ СИСТЕМ, КОМП'ЮТЕРНИХ МЕРЕЖ ЧИ МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ

На підставі аналізу наукових досліджень, практики органів досудового розслідування висвітлено питання, що стосуються особи злочинця як елементу криміналістичної характеристики несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. Виведено типові характерні риси особи злочинця, розглянуто криміналістичний аспект особи злочинця у взаємозв'язку з іншими елементами криміналістичної характеристики й установлено зв'язок між певними рисами особи злочинця та обстановкою, слідами, способом учинення злочину та його приховуванням.

Ключові слова: особа злочинця, криміналістична характеристика, кіберзлочин, несанкціоноване втручання, електронно-обчислювальні машини, комп'ютери, автоматизовані системи, комп'ютерні мережі, мережі електрозв'язку.

Постановка проблеми. Високий темп розвитку комп'ютерних технологій, а також їх інтеграція в усі сфери життя, глобалізація інформаційних процесів і поява глобальних комп'ютерних мереж призвели до виникнення нового виду злочинів, пов'язаних з використанням комп'ютерів, інформаційних технологій та глобальних мереж, а саме кіберзлочинів.

Сьогодні на фоні істотного зростання злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку не проведено ґрунтовних досліджень у сфері криміналістики, які б узагальнювали слідчу практику і, базуючись на наукових підходах, виділяли загальні риси, властиві для осіб, які вчинюють різні види кіберзлочинів.

Винятком не є і такий вид кіберзлочинів, як несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, передбачений ст. 361 КК України.

У зв'язку з цим співробітники правоохоронних органів, які залучені до розслідування цієї категорії злочинів, найчастіше, не володіючи повною й достовірною інформацією про характерні особливості та риси осіб, які їх учинили, стикаються з труднощами, особливо на початковому етапі проведення розслідування.

У результаті ситуації, що склалася, ефективність досудового розслідування зменшується, про що також свідчить офіційна статистика Генеральної прокуратури України за період з початку 2016 року по квітень 2017 року, згідно з якою лише приблизно по 30% кримінальних проваджень за статтями 361 - 363-1 КК України за цей звітний період були прийняті процесуальні рішення [1].

Аналіз останніх досліджень і публікацій. Загальні питання вивчення криміналістичної характеристики злочинів, а також вивчення безпосередньо питань криміналістичної характеристики кіберзлочинів у різні часи вивчали такі вчені, як Р. С. Бєлкін, Р. Л. Ахмедшин, М. В. Салтевський, В. Ю. Шепитько, М. С. Прохоров, В. К. Гавло, П. Д. Біленчук, В. Б. Вехов, В. В. Крилов, В. В. Кравчук, С. В. Кригін, В. М. Кулик, О. А. Самойленко, О. В. Курман та інші.

Криміналістична характеристика будь-якого злочину передбачає наявність певних елементів, одним з яких є особа злочинця. Криміналістичне вивчення стосовно особи злочинця в кримінальних провадженнях полягає як у встановленні даних, що відображають сутність особи, яка вчинила злочин, у розрізі до вимог чинного кримінального та кримінально-процесуального законодавства, так і у виявленні комплексу значущих ознак цієї особи, які можуть бути використані для її встановлення, розшуку та викриття.

Зміст особи злочинця як елементу криміналістичної характеристики полягає у визначенні особи як певної системи, властивості та ознаки якої знаходять відображення в навколишньому середовищі та використовуються під час розслідування злочинів.

Зокрема, Р. Л. Ахмедшин зазначав, що криміналістичне вивчення особи злочинця має бути переважно орієнтовано на особу як носія соціально-психологічних характеристик, виражених в її криміналістично значущих поведінкових реакціях, що відображаються в конкретних умовах злочинної події [2, с. 10]. М. В. Салтевський виділяв серед властивостей особи злочинця фізичні, біологічні та соціальні [3, с. 422]. Своєю чергою В. Ю. Шепітько зазначив, що особа злочинця має певні дані демографічного характеру, деякі моральні якості та психологічні особливості [4, с. 258].

Погодимося з думкою В. К. Гавла, який підкреслював, що криміналістику та її методику цікавлять такі відомості про особу суб'єкта злочину, які вказують на закономірні зв'язки між ним і вчиненим злочином, що проявляються зовні, у різних наслідках скоєного. У цьому плані особу треба вивчати як слідоутворювальний об'єкт, джерело інформації про вчинений злочин і як засіб його розкриття [5, с. 197].

Проте попри дослідження цієї проблематики різними вченими низка окремих питань, зокрема стосовно характерних рис осіб, які вчинюють злочини та пов'язані з несанкціонованим утручанням у роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, а також щодо взаємозв'язку між особою злочинця та іншими елементами криміналістичної характеристики цього злочину досі не висвітлені в достатньому обсязі та є дискусійними.

Формування цілей. Автор має на меті дослідити питання стосовно особи злочинця як елементу криміналістичної характеристики злочину, передбаченого ст. 361 КК України, та визначити їх взаємозв'язок з іншими елементами в їх поєднанні.

За допомогою методу узагальнення незалежних характеристик, на базі особистого досвіду та матеріалів вивчених кримінальних проваджень

потрібно визначити та сформулювати висновки щодо характерних рис особи злочинця як елементу криміналістичної характеристики несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

Крім того, викладене вище дає змогу стверджувати про потребу комплексного дослідження проблем розслідування зазначеної категорії злочинів, розробки методики, яка враховує новітні досягнення криміналістики та інших наук, що в сукупності з іншими обставинами визначає актуальність обраної для дослідження теми, її перспективність і практичну значущість.

Виклад основного матеріалу. Аналізуючи вивчення криміналістичної характеристики особи злочинця в контексті розслідування кіберзлочинів, наведемо деяку класифікацію. Скажімо, О. А. Самойленко пропонує такі типи особи злочинця, що вчиняє злочин з використанням обстановки кіберпростору: 1) злочинець-користувач початкового рівня; 2) злочинець-користувач; 3) злочинець-упевнений користувач; 4) злочинець-досвідчений користувач; 5) злочинець-користувач професіонал [6, с. 200].

О. В. Курман виділяє декілька груп осіб, які здійснюють несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку: 1) працівники підприємств, установ, організацій – конкурентів; 2) працівники, які вчиняють незаконні дії з інформацією на замовлення, перебуваючи з її власником (уповноваженим органом) у трудових відносинах; 3) працівники, які збирають інформацію для себе (про всяк випадок); 4) особи, професійна або службова діяльність яких чи інші законні підстави обумовлюють виникнення певних правовідносин цивільно-правового характеру з власником інформації; 5) особи, які не перебувають у жодних цивільно-правових чи трудових відносинах з власником, але вчиняють незаконні дії через «спортивний інтерес», бажання заявити про себе, прорекламувати свої можливості та уміння, на замовлення сторонніх осіб (для передачі конкурентам чи вчинення шантажу) [7, с. 130].

Така класифікація особи злочинця може мати місце при розслідуванні несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, де іншими елементами криміналістичної характеристики зазначеного злочину виступають: виток, втрата, підробка, блокування інформації, спотворення процесу обробки інформації та порушення встановленого порядку маршрутизації інформації, а також обстановка, сліди, способи вчинення злочину і його приховування.

У зв'язку з цим було б неправильним при розслідуванні цієї категорії злочинів розглядати криміналістичний аспект особи злочинця у відриві від вищевказаних елементів криміналістичної характеристики, оскільки саме вони дають змогу в багатьох ситуаціях істотно обмежити та звузити коло осіб, які можуть бути причетні до вчинення злочину.

Скажімо, вивчаючи обстановку скоєння злочину, треба обов'язково звернути увагу на наявність і спосіб підключення електронно-обчислювальної техніки (ЕОТ), у роботу якої було здійснено несанкціоноване втручання до комп'ютерних мереж і мереж електрозв'язку. Відразу ж можна виділити три основні ситуації: 1) ЕОТ не підключена до будь-яких мереж; 2) ЕОТ підключена до локальної мережі; 3) ЕОТ підключена до глобальної мережі Інтернет.

Відштовхуючись від цих відомостей, можна в деяких випадках істотно звузити коло можливих підозрюваних і виділити типи осіб злочинців за способом здійснення несанкціонованого втручання:

1. Злочинець мав безпосередній (фізичний) доступ до ЕОТ. Тоді доцільно було б визначити коло осіб, які могли мати доступ до ЕОТ з урахуванням установлених часу та місця скоєння злочину (прикладом може бути ситуація, коли співробітник підприємства, якого, на його думку, незаслужено звільняють, проникає в дата-центр і, з помсти, використовуючи шкідливе програмне забезпечення, маючи безпосередній доступ до ЕОТ, знищує всю інформацію на серверах компанії).

2. Злочинець мав доступ до ЕОТ у локальній мережі і з її допомогою здійснив несанкціоноване втручання в роботу ЕОТ, що міститься в тій само локальній мережі. У цьому випадку є можливість з'ясувати в адміністратора локальної мережі обмежений список точок підключення ЕОТ, які входять у мережу, а також фізичні (реальні) і IP-адреси точок підключення до мережі. Маючи таку інформацію, можна встановити обмежене коло осіб, які працюють у локальній мережі (прикладом може послужити ситуація, коли комірник на підприємстві, де комп'ютери об'єднані в закриту локальну мережу, для приховування нестачі товару підключається за допомогою одного з комп'ютерів у цій мережі до сервера із системою обліку товарообігу, за допомогою шкідливого програмного забезпечення зламує її захист і змінює дані про кількість товару на складі).

3. Злочинець здійснив несанкціонований доступ та втручання в роботу ЕОТ, що підключена до глобальної мережі Інтернет, за допомогою невстановленої ЕОТ, яка також підключена до глобальної мережі Інтернет. Така ситуація є найскладнішою для вирішення, оскільки в теорії несанкціонований доступ та втручання в роботу ЕОТ мало змогу здійснити необмежене коло осіб по всьому світу при наявності підключення до глобальної мережі Інтернет (прикладом може послужити ситуація, коли хакер розіслав електронною поштою шкідливе програмне забезпечення, що здійснило шифрування даних на жорстких дисках комп'ютерів підприємства, призвело до блокування інформації, після чого вимагає гроші за відновлення можливості доступу до цієї інформації).

Зіткнувшись з останньою ситуацією, треба розглянути особу злочинця в прив'язці до слідової картини й способу вчинення злочину. Потрібно з'ясувати, чи використовував злочинець шкідливе програмне забезпечення, бекдори (з англ. backdoor – чорний хід, тобто уразливості в коді програмного забезпечення) або ж несанкціоноване втручання здійснили потерпілі чи

користувачі ЕОТ через недотримання елементарних правил забезпечення кібербезпеки.

Для цього під час огляду ЕОТ за участю фахівця крім іншої інформації, яка має значення для проведення розслідування, треба встановити також, чи залишилися на зламаній ЕОТ сліди шкідливого програмного забезпечення, чи не пошкоджений реєстр з інформацією щодо останніх дій користувача, чи здійснювалося підключення ЕОТ до мережі безпосередньо або через маршрутизатор, чи використовується в маршрутизаторі стандартний логін і пароль або вони змінені, чи присвоєно точці підключення до мережі статичну або динамічну IP-адресу, а також які налаштування підключення до мережі використовуються; яку MAC-адресу має мережеве обладнання користувача, чи був злочинцем проведений повний вайп (від англ. wipe – стирати, знищувати, видаляти) інформації на носіях, вайп операційної системи або її часткове пошкодження, а також чи можливо відновити дані.

Отже, проаналізувавши отриману на початковому етапі розслідування інформацію, можна буде виділити кілька типів особи злочинця за знаннями у сфері комп'ютерних наук:

1. Злочинці, які мають базові навички у сфері комп'ютерних наук, використовують готове шкідливе програмне забезпечення, інструкції, уроки по зламу, що є в загальному доступі (наприклад, при отриманні від спеціаліста або експерта інформації про те, яке шкідливе програмне забезпечення використовувалося для несанкціонованого втручання і маніпуляцій з інформацією, у спосіб додаткових консультацій з фахівцями і особистим пошуком можна дізнатися, що це програмне забезпечення. Така інформація може стати корисною для доказування, якщо під час обшуків у осіб, які можуть бути причетні до скоєння злочину, при огляді їх комп'ютерів буде встановлено, що вони відвідували інтернет-ресурси, де можна скачати це програмне забезпечення).

Не можна також залишити без уваги думку відомого американського фахівця по боротьбі з фішингом (phishing від англ. fishing – рибна ловля; один з видів інтернет-шахрайства, метою якого є отримання доступу до конфіденційних даних користувачів) Ленса Джеймса, який уважає, що в XXI столітті найбільшого поширення серед комп'ютерних злочинців отримали скрипткіддіс (script kiddies) [8, с. 42]. До їх головних особливостей він відносить юний вік, непрофесійні хакерські здібності, наявність вільного часу, наполегливість у досягненні поставленої мети, використання вже готових кодів, розроблених фахівцями [8, с. 43].

Крім того, при огляді ЕОТ або допиті свідків, потерпілих може з'ясуватися, що в маршрутизаторі, за допомогою якого здійснюється доступ ЕОТ до мережі Інтернет, використовуються стандартний логін і пароль виробника обладнання (наприклад, «admin»/«admin»), і несанкціонований доступ був здійснений у спосіб простого підбору пароля.

2. Злочинці, які мають навички у сфері комп'ютерних наук, що не володіють певним досвідом програмування, але здатні адаптувати готові програмні рішення відповідно до своїх потреб, уміють знаходити нові або

використовувати відомі уразливості в програмному забезпеченні (наприклад, злочинець може використовувати готові програмні рішення для здійснення несанкціонованого доступу до ЕОТ на базі Kali Linux – дистрибутива на базі операційної системи Linux для проведення тестування на проникнення й аудиту безпеки). У цьому випадку при порівнянні результатів комп'ютерно-технічної експертизи або інформації від фахівця про спосіб несанкціонованого втручання з можливостями, що надає зазначений дистрибутив, можна скласти уявлення про досвід злочинця, а також отримати відомості про те, на що треба звернути увагу під час проведення обшуків.

3. Злочинці, які мають фундаментальні знання у сфері комп'ютерних наук, зокрема й програмування, самостійно розробляють шкідливе програмне забезпечення й знаходять нові, складні в реалізації, способи для здійснення несанкціонованого втручання в роботу ЕОТ. Наприклад, коли експерт не може ідентифікувати шкідливе програмне забезпечення, що використовувалося при несанкціонованому доступі до ЕОТ, а антивірусні бази ще не містять його сигнатури (від англ. signature – підпис; у цьому випадку мається на увазі цифровий підпис, за допомогою якого антивірусне програмне забезпечення визначає шкідливе програмне забезпечення) або ці сигнатури були додані недавно й шкідливого програмного забезпечення немає в загальному доступі.

Розкриття злочинів, учинених останнім типом злочинців, представляє особливу складність, оскільки вони знають, що роблять, роблять це добре й уміло приховують сліди.

Частково треба погодитися з ученими, які вважають, що формальне застосування підходу для типізації особи злочинця, який діє з використанням обстановки кіберпростору, за професійним рівнем не матиме практичного сенсу з позицій формулювання типових версій про особу злочинця. Адже професійний рівень користувача не відображає всього спектра ознак злочинця, активно задіяних у процесі детермінації механізму злочину [6, с. 195].

Однак потрібно зробити поправку на те, що відомості про особу злочинця як елементу криміналістичної характеристики злочинів дають слідчому можливість скласти уявлення про певну групу осіб, до якої може належати злочинець, а виділення типових рис кіберзлочинців допомагає оптимізувати процес їх виявлення й проведення розслідування. До того ж відомості про особу злочинця в структурі криміналістичної характеристики злочинів можуть бути покладені в основу криміналістичної методики їх розслідування.

Висновки. Отже, у результаті проведеного дослідження на підставі інформації, якою володіє слідчий на початковому етапі розслідування, з урахуванням обстановки, слідів, способу вчинення злочину та його приховування, запропоновано класифікацію особи злочинця за певними критеріями, а саме:

За способом доступу до ЕОТ:

1. Злочинець мав безпосередній (фізичний) доступ до ЕОТ.

2. Злочинець мав доступ до ЕОТ у локальній мережі та за її допомогою здійснив несанкціоноване втручання в роботу ЕОТ.

3. Злочинець здійснив несанкціонований доступ та втручання в роботу ЕОТ, що підключена до глобальної мережі Інтернет, за допомогою невстановленої ЕОТ, яка також підключена до глобальної мережі Інтернет.

За рівнем знань у сфері комп'ютерних технологій:

1. Злочинці, які мають базові навички у сфері комп'ютерних наук, використовують готове шкідливе програмне забезпечення, інструкції, що є в загальному доступі.

2. Злочинці, які мають навички у сфері комп'ютерних наук, що не володіють певним досвідом програмування, але здатні адаптувати готові програмні рішення відповідно до своїх потреб, уміють знаходити нові або використовувати відомі уразливості в програмному забезпеченні.

3. Злочинці, які мають фундаментальні знання у сфері комп'ютерних наук, зокрема й програмування, самостійно розробляють шкідливе програмне забезпечення й знаходять нові, складні в реалізації, способи для здійснення несанкціонованого втручання в роботу ЕОТ.

Запропонована класифікація особи злочинця в поєднанні з іншими елементами криміналістичної характеристики зазначених злочинів потребує дальшого вивчення в межах розроблення методики розслідування несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

Проведене дослідження відповідно до його цілей та завдань дало змогу окреслити низку теоретичних і практичних питань, вирішення яких, на наш погляд, може зменшити труднощі на початковій стадії проведення розслідування та сприяти оперативності розкриття злочинів, передбачених ст. 361 КК України.

Використані джерела:

1. Запит до Генеральної прокуратури України щодо статистики кіберзлочинів, зареєстрованих правоохоронними органами в Україні в 2016 році та в січні – квітні 2017 року. Доступ до правди. URL: https://dostup.pravda.com.ua/request/statistika_kibierzlochinnosti_v (дата звернення: 26.11.2018).

2. Ахмедшин Р. Л. Криминалистическая характеристика личности преступника: автореф. дис. … д-ра юрид. наук: спец. 12.00.09. Томск, 2006. 48 с.

3. Салтевський М. В. Криміналістика (у сучасному викладі): підручник. Київ: Кондор, 2005. 588 с.

4. Шепитько В. Ю. Криминалистика: курс лекций. 2-е изд., перераб. и доп. Харьков: ООО «Одиссей», 2005.368 с.

5. Гавло В. К. Теоретические проблемы и практика применения методики расследования отдельных видов преступлений. Томск: Изд. Томского у-та, 1985. 333 с.

6. Самойленко О. А. Типизація особи, що вчиняє злочин, пов'язаний із використанням обстановки кіберпростору (з позицій криміналістичної науки). *Підприємництво, господарство і право*. 2018. № 8. С. 195-201.

7. Курман О. В. Криміналістична характеристика несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів),

автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. *Науковий вісник Херсонського державного університету*. Серія «Юридичні науки». Випуск 4. Том 2. 2017. С. 127-130.

8. Джеймс Л. Фишинг. Техника компьютерных преступлений (пер. с англ. Р. В. Гадицкого). Москва: НТ Пресс, 2008. 320 с.

9. Кримінальний кодекс України: Закон від 05.04.2001 № 2341-III. *Відомості Верховної Ради України* (ВВР), 2001, № 25-26, ст. 131. (із поточними змінами). URL : http://zakon3.rada.gov.ua/laws/show/2341-14 (дата звернення: 26.11.2018).

10. Кримінальний процесуальний кодекс України : Закон від 13.04.2012 № 4651-VI. *Відомості Верховної Ради України* (ВВР), 2013, № 9-10, № 11-12, № 13, ст.88. (із поточними змінами). URL: http://zakon2.rada.gov.ua/laws/show/4651-17 (дата звернення: 26.11.2018).

Стаття надійшла до редколегії 26.11.2018

Бородай О. В. Личность преступника как элемент криминалистической характеристики несанкционированного вмешательства в работу электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи

На основании анализа научных исследований, практики органов досудебного расследования освещены вопросы, касающиеся личности преступника как элемента криминалистической характеристики несанкционированного вмешательства в работу электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи. Выведены типичные характерные черты личности преступников, совершивших преступления указанной категории, рассмотрен криминалистический аспект личности преступника во взаимосвязи с другими элементами криминалистической характеристики и установлена связь между определенными чертами личности преступника и обстановкой, следами, способом совершения преступления и его сокрытия.

Ключевые слова: личность преступника, криминалистическая характеристика, киберпреступление, несанкционированное вмешательство, электронно-вычислительные машины, компьютеры, автоматизированные системы, компьютерные сети, сети электросвязи.

Borodai O. The Identity of the Criminal as Element of the Forensic Characteristics of Unauthorized Interference into the Operation of Electronic Computing Machines (Computers), Automated Systems, Computer Networks or Telecommunication Networks

Based on the analysis of the scientific studies and the practice of pre-trial investigation bodies issues relating to the identity of the criminal as an element of the forensic characteristics of unauthorized interference with the operation of electronic computing machines (computers), automated systems, computer networks or telecommunication networks were reviewed. Typical personality traits of criminals who have committed crimes in this category were identified. The forensic aspect of the criminal's personality was studied in conjunction with other elements of the forensic characteristics. An interconnection between certain personality traits of the criminal and the crime setting, traces, method of committing and concealing the crime was established. On the basis of the volume of information that an investigator has at the

initial stage of investigation the typing of the offender's identity by certain parameters was proposed. The typization of criminals who committed unauthorized interference with the operation of electronic computing machines (computers), automated systems, computer networks or telecommunication networks by the way of obtaining access to computer and by knowledge in computer science was proposed in order to make the decision-making process behind the suggestion of investigative versions easier. The research conducted in accordance with its goals and objectives has made it possible to outline a number of theoretical and practical issues, the solution of which may reduce the difficulties in formulating investigative versions at the initial stage of the investigation and facilitate the speed of disclosure and investigation of crimes, connected with unauthorized interference with the operation of electronic computing machines (computers), automated systems, computer networks or telecommunication networks.

Keywords: the identity of the criminal, forensic characteristics, cybercrime, unauthorized interference, unauthorized access, electronic computing machines, computers, automated systems, computer networks, telecommunication networks.

УДК 343.98

В. О. Гусєва

ОСОБЛИВОСТІ ОБСТАНОВКИ ТА СПОСОБУ ВЧИНЕННЯ ЗЛОЧИНУ ЯК ЕЛЕМЕНТІВ КРИМІНАЛІСТИЧНОЇ ХАРАКТЕРИСТИКИ ПОСЯГАНЬ НА ЖИТТЯ ПРАЦІВНИКА ПРАВООХОРОННОГО ОРГАНУ

На підставі аналізу наукової літератури та практики органів досудового слідства розглянуто деякі елементи криміналістичної характеристики посягань на життя працівника правоохоронного органу (обстановка вчинення злочину, способи вчинення та приховування злочину), визначено їх взаємозв'язок, на підставі проведеного дослідження визначено статистичні відомості щодо зазначених елементів криміналістичної характеристики.

Ключові слова: криміналістична характеристика, посягання на життя працівника правоохоронного органу, обстановка місця злочину, способи вчинення та приховування злочину.

Постановка проблеми. Сьогодні значного поширення набувають кримінальні правопорушення, передбачені статтями 342, 343, 345, 347, 348, 349, 350, 352, 353 КК України, що виражаються в посяганнях на життя, здоров'я, майно працівників правоохоронних органів і членів їхніх сімей тощо.

Відповідно злочини, які посягають на життя й здоров'я працівників правоохоронних органів, відносяться до розряду особливо тяжких. Підвищена небезпека таких злочинів обумовлена тим, що вони посягають безпосередньо на нормальну діяльність працівника правоохоронного органу з охорони громадського порядку й забезпечення громадської безпеки, а також на життя та здоров'я цих осіб.

Під посяганням на життя працівника правоохоронного органу треба розуміти вбивство або замах на вбивство. У такому разі суб'єктивна сторона цих злочинів полягає в психічній діяльності особи, що безпосередньо