DOI https://doi.org/10.51647/kelm.2021.8.2.19

KRYMINALISTYCZNY ASPEKT SPOSOBÓW POPEŁNIANIA WYKROCZEŃ KARNYCH POPEŁNIANYCH PRZY UŻYCIU TECHNOLOGII INFORMATYCZNYCH (CYBERPRZESTĘPCZOŚCI)

Yaroslav Nedilko
aspirant Katedry Postępowania Karnego i Kryminalistyki
Dydaktyczno-Naukowego Instytutu Prawa
Kijowskiego Uniwersytetu Narodowego imienia Tarasa Szewczenki (Kijów, Ukraina)
ORCID ID: 0000-0003-1483-3479
nedilkoyaroslav@gmail.com

Adnotacja. W artykule zbadano cechy sposobu popełniania cyberprzestępstw jako elementu charakterystyki kryminalistycznej i podano definicję jego pojęcia.

W artykule dokonano przeglądu podstawowych podejść naukowców do określenia pojęcia sposób popełnienia wykroczenia karnego, co z kolei dało możliwość przytoczenia nowoczesnej definicji sposobu popełnienia wykroczeń karnych popełnianych przy użyciu technologii informatycznych (cyberprzestępczości). Przeanalizowano genezę sposobów popełniania przestępstw komputerowych i ich przekształcenie w wykroczenia karne popełniane przy użyciu technologii informatycznych (cyberprzestępstwa). Zgodnie z wynikami badań przedstawiono klasyfikację sposobów popełniania wykroczeń karnych popełnianych przy użyciu technologii informatycznych (cyberprzestępczości).

Zauważono, że wykroczenia karne tej kategorii mają charakter dynamiczny (ciągle się zmieniają), co jest dość trudne do wyodrębnienia konkretnych sposobów ich popełnienia.

Słowa kluczowe: charakterystyka kryminalistyczna, sposoby popełniania wykroczeń karnych, cyberprzestępczość.

CRIMINALISTIC ASPECT OF METHODS OF COMMITTING CRIMINAL OFFENSES COMMITTED USING INFORMATION TECHNOLOGIES (CYBERCRIMES)

Yaroslav Nedilko
Postgraduate Student at the Department of Criminal Procedure and Forensic Science
Scientific Research Institute of Law
Taras Shevchenko National University of Kyiv (Kyiv, Ukraine)
ORCID ID: 0000-0003-1483-3479
nedilkoyaroslav@gmail.com

Abstract. The article examines the features of the method of committing cybercrime as an element of forensic characteristics and provides a definition of its concept.

The article considers the main approaches of scientists to the definition of the method of committing a criminal offense, which, in turn, provided an opportunity to provide a modern definition of the method of committing criminal offenses committed using information technology (cybercrime). The genesis of ways of committing computer crimes and their transformation into criminal offenses committed with the use of information technology (cybercrime) is analyzed. According to the results of the study, the classification of methods of committing criminal offenses committed with the use of information technology (cybercrime) is given.

It is noted that criminal offenses of this category are dynamic (constantly changing), which makes it difficult to identify specific ways of committing them.

Key words: forensic characteristics, ways of committing criminal offenses, cybercrime.

КРИМІНАЛІСТИЧНИЙ АСПЕКТ СПОСОБІВ ВЧИНЕННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ЩО ВЧИНЯЮТЬСЯ З ВИКОРИСТАННЯМ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ (КІБЕРЗЛОЧИНІВ)

Ярослав Неділько
аспірант кафедри кримінального процесу та криміналістики
Навчально-наукового інституту права
Київського національного університету імені Тараса Шевченка (Київ, Україна)
ORCID ID: 0000-0003-1483-3479
nedilkoyaroslav@gmail.com

Анотація. У статті досліджено особливості способу вчинення кіберзлочинів як елементу криміналістичної характеристики та надано визначення цього поняття.

Розглянуто основні підходи вчених до визначення поняття «спосіб вчинення кримінального правопорушення», що своєю чергою дало змогу навести сучасне визначення способу вчинення кримінальних правопорушень, що вчиняються з використанням інформаційних технологій (кіберзлочинів). Проаналізовано генезис способів вчинення комп'ютерних злочинів та їх трансформацію в кримінальні правопорушення, що вчиняються з використанням інформаційних технологій (кіберзлочини). За результатами дослідження наведено класифікацію способів вчинення кримінальних правопорушень, що вчиняються з використанням інформаційних технологій (кіберзлочинів).

Зауважено, що кримінальні правопорушення зазначеної категорії мають динамічний характер (постійно змінюються), через що досить складно виокремити конкретні способи їх вчинення.

Ключові слова: криміналістична характеристика, способи вчинення кримінальних правопорушень, кіберзлочин.

Вступ. У процесі розслідування будь-якого кримінального правопорушення особливу увагу привертає спосіб його вчинення. Як на практиці, так і в теоретичних надбаннях точаться різні дискусії стосовно цього питання.

Спосіб вчинення кримінального правопорушення в різний час досліджували такі вчені, як Р.С. Бєлкін, П.Д. Біленчук, О.М. Дуфенюк, С.М. Зав'ялов, Г.Г. Зуйков, О.Н. Колесниченко, С.В. Матусовський, М.В. Салтевський, М.П. Яблоков та інші.

Одним із важливих і визначальних елементів у структурі криміналістичної характеристиці кримінальних правопорушень, що вчиняються з використанням інформаційних технологій (кіберзлочинів), є спосіб вчинення. Метою дослідження є виявлення особливостей способу вчинення кримінальних правопорушень, що вчиняються з використанням інформаційних технологій (кіберзлочинів), як елементу криміналістичної характеристики та визначення цього поняття.

Основна частина. Взагалі термін «спосіб» в етимологічному розумінні визначається як певна дія, прийом або система прийомів, яка дає змогу зробити, здійснити що-небуть, досягти чогось (Бусел, 2001: 1179).

В юридичній науці спосіб вчинення кримінального правопорушення досліджується в кримінально-правовому, кримінально-процесуальному, криміналістичному напрямах, що впливає на його визначення. В.Є. Корноухов доречно підкреслює, що в кримінальному праві спосіб вчинення пов'язаний з іншими елементами об'єктивної сторони кримінального правопорушення і відбиває караність діяння, а також виступає як кваліфікуюча ознака. У кримінально-процесуальному праві значення способу вчинення належить до обставин, які підлягають доказуванню. У криміналістиці за допомогою способу вчинення розшукують осіб, які вчинили кримінальне правопорушення, з'ясовують закономірності механізму слідоутворення, а також знаходження інших слідів, що стосуються вчиненого діяння (Корноухов, 2000: 172–173).

У криміналістичній науці спосіб вчинення кримінального правопорушення вчені почали вивчати в середині XX століття.

З огляду на відсутність єдності думок із цього питання В.О. Коновалова зазначає, що проблема способу вчинення кримінального правопорушення як одна з ключових у криміналістиці залишається дискусійною. Це викликано різними підходами вчених до інтерпретації понятійного апарату, зокрема до змісту понять «спосіб вчинення» і «спосіб приховання» (Коновалова, 2001: 7).

Вважається, що першими визначення поняття способу вчинення «умисного злочину» навели А.І. Вінберг та Б.М. Шавер, які розглядали його як складник предмета криміналістики та стверджували, що використання знань про спосіб вчинення застосовується для виявлення слідів, встановлення злочинців і розкриття вчинених ними кримінальних правопорушень. Саме визначення вони трактували так: це дії, безпосередньо спрямовані на досягнення злочинних наслідків, включаючи дії щодо проникнення злочинця на місце вчинення, прийоми, які злочинець використовував, особливо стосовно предмета замаху, місце, час, знаряддя кримінального правопорушення (Шавер, Вінберг, 1950: 199; Шавер, 1952: 34).

Вперше структуру способу вчинення «умисного злочину» розкриває Е.Д. Куранова, яка стверджує, що це комплекс дій із підготовки, вчинення і приховання злочину, вибраних винними відповідно до наміченої мети і тих умов, за якими реалізується злочинний намір (Куранова, 1962: 165–167).

О.Н. Колесниченко сформулював власну криміналістичну концепцію способу вчинення кримінального правопорушення, під якою пропонує розуміти спосіб дій злочинця, що виявляється в певній послідовності, сполученні окремих дій, прийомів, що застосовуються суб'єктом. Цікавим є те, що вчений запропонував розглядати окремо спосіб готування, спосіб вчинення і спосіб приховання кримінального правопорушення (Колесниченко, 1965: 18).

Такої думки дотримується і О.М. Дуфенюк, яка розділяє окремо спосіб готування, вчинення і приховання кримінального правопорушення як елемента криміналістичної характеристики та звертає увагу, що не кожен вид кримінального правопорушення охоплює всі три стадії, оскільки деякі з них можуть вчинятися взагалі без підготовчого етапу або маскування слідів протиправного діяння (Благута, Сибірна та ін., 2012: 237).

Проте Г.Г. Зуйков вважає, що спосіб вчинення кримінального правопорушення – це система дій із готування, вчинення і приховання, детермінованих умовами зовнішнього світу і психофізіологічними якостями особистості, що можуть бути пов'язані з вибірковим використанням відповідних знарядь або засобів і умов місця і часу, й об'єднаних загальним протиправним задумом (Зуйков, 1970: 205).

Однак Р.С. Бєлкін зауважує, що твердження Г.Г. Зуйкова є правильним для тих випадків, коли готування, вчинення і приховання кримінального правопорушення відбувається за єдиним задумом, коли всі ці дії тісно

пов'язані між собою в єдину систему, і, ще не вчинивши кримінальне правопорушення, суб'єкт має чітку програму дій щодо його приховання. Але так буває не завжди. Дії щодо вчинення і приховання можуть бути розірвані за суб'єктом, коли приховує не той, хто його вчинив, а інша особа без відома суб'єкта, який і не вчиняв дій із приховання кримінального правопорушення. Ці дії можуть відрізнятися за задумом, коли цілі приховання спочатку не переслідувалися, а виникли вже після вчинення кримінального правопорушення через непередбачені обставини або такі, що змінилися. Роблячи висновок, вчений стверджує, що приховання може існувати самостійно як система дій зі знищення, маскування або фальсифікації слідів – як матеріальних, так і ідеальних (Бєлкін, 2001: 735).

Водночас, на погляд П.Д. Біленчука, В.К. Лисиченка та Н.І. Клименко, недоцільно до криміналістичної характеристики способу вчинення зараховувати сукупність відомостей про дії злочинця, спрямовані на маскування (приховання) кримінального правопорушення і його слідів, оскільки це є частиною способу вчинення (Біленчук, Лисиченко, Клименко, 2001: 365).

Своєю чергою способи вчинення кримінального правопорушення М.С. Уткін пропонує поділяти на: 1) повноструктурні, або найкваліфікованіші (готування, вчинення і приховання); 2) менш кваліфіковані, або усічені першого типу (вчинення і приховання); 3) менш кваліфіковані, або усічені другого типу (готування і вчинення); 4) некваліфіковані, або спрощені, що складаються лише з дій із вчинення кримінального правопорушення (Уткін, 1975: 6).

Натомість М.А. Погорецький, Д.Б. Сергєєва і З.М. Топорецька переконані, що спосіб вчинення кримінального правопорушення – це послідовність дій суб'єкта, спрямована на досягнення поставленої мети (певного злочинного результату), це усе те, що характеризує дії злочинця в процесі підготовки (підшукання місця, вибір предмета посягання, готування знарядь і засобів, необхідних для здійснення злочинної цілі тощо), вчинення й приховання слідів кримінального правопорушення (Погорецький, Сергєєва, Топорецька, 2015: 27).

Незважаючи на відсутність єдності думок щодо трактування способу вчинення кримінального правопорушення та враховуючи наведені позиції науковців, на нашу думку, для кримінальних правопорушень, що вчиняються з використанням інформаційних технологій (кіберзлочинів), є характерними дії, що включають готування, вчинення та приховання.

Загалом, на наш погляд, спосіб вчинення кримінальних правопорушень зазначеної категорії – це сукупність послідовних умисних протиправних дій суб'єкта (суб'єктів) у кіберпросторі, що включає дії з готування, вчинення та приховання, спрямовані на досягнення певного злочинного результату з використанням інформаційних технологій.

Варто звернути увагу, що в науковій літературі упродовж тривалого часу домінувало поняття «комп'ютерний злочин». Це пов'язано з найменуванням у XIX столітті словом «комп'ютер» (англійською слово «computer» означає «той, що вираховує») (Computer. Oxford Learner's Dictionaries, 2021) механічного, а пізніше цифрового, аналогового і електронного обчислюваного пристрою, який злочинці використовують для досягнення своїх злочинних намірів. Проте науково-технічний прогрес зумовлює подальший стрімкий розвиток і широке використання в усіх сферах суспільного життя новітніх інформаційних технологій (комп'ютерної техніки, глобальних інформаційних мереж та їх ресурсів, мобільних засобів комунікації та інших технічних засобів).

У цьому аспекті обґрунтованою є позиція науковців, які стверджують, що разом із розвитком новітніх технологій поняття «комп'ютерні злочини» трансформувалось у поняття кримінальних правопорушень (злочинів), що вчиняються з використанням інформаційних технологій (кіберзлочини) (Біленчук, Лисиченко, Клименко, 2001: 434). Дефініція «кіберзлочинність» відповідає і міжнародним стандартам.

З поняттям «комп'ютерний злочин» пов'язувалось і вивчення способів їх вчинення.

Так, свого часу Ю.М. Батурін, узагальнивши конкретні дії злочинців із доступу до засобів комп'ютерної техніки, запропонував класифікувати способи вчинення комп'ютерних злочинів на п'ять груп:

– вилучення засобів комп'ютерної техніки;
– перехоплення інформації;
– несанкціонований доступ до засобів комп'ютерної техніки;
– маніпуляція даними і керуючими командами;
– комплексні методи (Батурін, 1991: 18–34).

На дві великі групи дії злочинців поділяє О.Х. Волинський. До першої групи він зараховує злочинні діяння, що здійснюються без використання комп'ютерних пристроїв як інструмента для проникнення ззовні в інформаційні системи, чи вплив на них. Зокрема, викрадення машинних носіїв інформації у вигляді блоку чи елементів ЕОМ тощо. До другої групи пропонує зараховувати діяння з використанням комп'ютерних та комунікаційних пристроїв як інструмента для проникнення в інформаційні системи, чи вплив на них (Волинський, 1999: 585–586).

Розмірковуючи над способами вчинення кримінальних правопорушень зазначеної категорії, Л.П. Паламарчук цілком слушно зауважує, що спосіб вилучення засобів комп'ютерної техніки передбачає фізичне вилучення, а тому його слід зараховувати до злочинів проти власності. На переконання науковця слід виділяти п'ять груп способів вчинення злочинів зазначеної категорії:

1) незаконне втручання в роботу ЕОМ (комп'ютера), системи та комп'ютерної мережі;
2) незаконне перехоплення комп'ютерної інформації;
3) маніпуляції з комп'ютерною інформацією;
4) використання шкідливих програм;
5) комплексні методи, тобто використання одночасно кількох методів (Паламарчук, 2004: 50).

В.Б. Вєхов резонно зазначає, що майже всі способи вчинення цих кримінальних правопорушень мають індивідуальні ознаки, за якими їх можна розпізнати та класифікувати в окремі групи. Зазвичай їх основою є дії злочинця, спрямовані на отримання різного роду доступу до засобів комп'ютерної техніки. Усі ці дії здійснюються кваліфікованими і хитрими способами маскування, що ускладнює їх виявлення, розслідування та розкриття (Вехов, 1996).

Натомість із розвитком сучасних інформаційних технологій почали змінюватися і форми злочинної діяльності. Це зумовило виникнення нового поняття «кримінальні правопорушення, що вчиняються з використанням інформаційних технологій (кіберзлочини)».

Спробу класифікації типових способів вчинення кримінальних правопорушень у кіберпросторі робить О.А. Самойленко, поділяючи їх на:

1) способи злочинних дій, пов'язаних із функціонуванням соціально орієнтованих мереж, діяльність яких заснована на так званій вікі(viki)-технології;

2) способи злочинних дій, пов'язаних із функціонуванням технології BitTorrent, створеної для передавання великих за обсягом файлів одним користувачем іншому;

3) способи злочинних дій, пов'язаних із функціонуванням сервісів електронної дошки оголошень;

4) способи злочинних дій, пов'язаних із функціонуванням технологій електронної комерції, створених для здійснення торгівлі через Інтернет;

5) способи злочинних дій, пов'язаних із функціонуванням технології електронної розсилки;

6) способи злочинних дій, пов'язаних із функціонуванням технологій електронних платіжних систем;

7) способи злочинних дій, пов'язаних із функціонуванням технології зберігання та обробки інформації;

8) способи злочинних дій, пов'язаних із функціонуванням шкідливого програмного забезпечення (Самойленко, 2020: 140–155).

Вважаємо, що досить складно виокремити всі способи вчинення цих кримінальних правопорушень, оскільки з розвитком інформаційних технологій цей вид злочинної діяльності буде стрімко змінюватися, спричиняючи виникнення нових способів. Однак, враховуючи реалії сьогодення, на наш погляд, можна говорити про найбільш типові та поширені нині способи вчинення кримінальних правопорушень, що вчиняються з використанням інформаційних технологій (кіберзлочинів). З огляду на рекомендації, запропоновані Агентством Європейського Союзу з мережевої та інформаційної безпеки (ENISA) (Reference Incident Classification Taxonomy, 2018), можна виділити такі способи:

1) використання шкідливих програм;

2) збір інформації (сканування, сніфінг, використання методів соціальної інженерії), що здійснюється з використанням інформаційних технологій;

3) несанкціоноване втручання та спроба несанкціонованого втручання;

4) вчинення DoS/DDoS атаки та створення бот-нетів;

5) шахрайство, вчинене з використанням інформаційних технологій;

6) поширення шкідливого контенту (спам, погрози, створення, поширення, збут дитячої порнографії, заклики до вчинення насильства, домагання), що вчинене з використанням інформаційних технологій;

7) порушення авторських чи суміжних прав із використанням інформаційних технологій;

Коротко охарактеризуємо кожен із наведених способів.

Так, до першої групи слід зарахувати дії зі створення шкідливого програмного забезпечення (або вдосконалення вже наявного), придбання чи збут, а також його використання з метою отримання незаконного доступу до системи чи цих засобів інформаційних технологій.

У світі є досить велика різноманітність шкідливого програмного забезпечення: віруси, хробаки, рекламне ПЗ, «троянський кінь» (троян), руткіти, keylogger (кейлогери), шпигунські програми тощо, які використовуються залежно від мети злочинця.

Слід зауважити, що у вітчизняному законодавстві відсутнє визначення поняття шкідливого програмного забезпечення.

На думку В.Б. Вехова, з криміналістичного погляду шкідливе програмне забезпечення має такі ознаки:

1) програма здатна знищити, блокувати, модифікувати або копіювати інформацію чи нейтралізувати систему захисту інформації на засобах інформаційних технологій;

2) програма не здійснює попереднього повідомлення власника чи користувача засобу інформаційних технологій про характер своїх дій;

3) програма не запитує згоди у власника чи користувача засобу інформаційних технологій на реалізацію свого призначення – алгоритму роботи (Вехов, 2021: 121–122).

Другу групу становлять дії, спрямовані на отримання інформації зловмисником. Сюди належать дії несанкціонованого перехоплення та аналіз мережевого трафіку (sniffing) задля отримання будь-якої інформації із засобів інформаційних технологій (Перехват данных по сети, 2017). Також злочинці можуть використовувати методи соціальної інженерії – психологічні маніпулювання з метою спровокувати особу до певних дій чи розголошення конфіденційної інформації (Социальная инженерия, 2007).

Третя група – втручання в систему чи мережу шляхом використання певних вразливостей програмного забезпечення чи вхід у систему через підбір логінів та паролів, а також здійснення несанкціонованого доступу до системи або компонента в обхід системи доступу (Перехват данных по сети, 2017).

До четвертої групи належать створення бот-нетів та вчинення DoS-, DDoS-атак. Під бот-нетом треба розуміти комп'ютерну мережу, що складається з деякої кількості хостів, із запущеними ботами – автономним

програмним забезпеченням (Ботнет, 2010). Злочинці використовують шкідливі ПЗ для зараження якомога більшої кількості засобів інформаційних технологій, створення бот-нетів, щоб ці пристрої потім використовувати у своїх протиправних намірах. Якщо бот-нети складаються з досить великої кількості пристроїв, їх злочинці використовують для вчинення DDoS-атак.

DoS-атака – це напад на комп'ютерну систему з наміром заблокувати цей ресурс, зробивши його недоступним для користувачів. DDoS-атака – це напад, який відбувається одночасно з досить великої кількості IP-адрес, і її називають розподіленою (DoS-атака, 2005).

Так, від великої DDoS-атаки постраждали парламент Бельгії, Інтернет-провайдер та правоохоронні органи. Через цю атаку парламенту Бельгії довелося перенести засідання, а поліцейські сайти Брюсселю та Антверпену були недоступними. Також недоступними на деякий час виявились системи онлайн-запису на вакцинацію від COVID-19 (Massive DDoS Attack Disrupts Belgium Parliament, 2021).

До п'ятої групи належить поширене в наш час Інтернет-шахрайство (електронне шахрайство). Це вид шахрайства з використанням мережі Інтернет та засобів інформаційних технологій (комп'ютерів, телефоні, планшетів тощо). Слід зазначити також про телефонне шахрайство, яке останнім часом почастішало. Зловмисники використовують різні прийоми для виманювання коштів: телефонують пізно вночі, стверджуючи, що ваш родич потрапив у лікарню і йому необхідні кошти; представляються представником банку і просять сказати реквізити банківської карти; повідомляють, що ви виграли в лотерею і необхідно вказати всі банківські дані для перерахунку коштів вам на карту, тощо.

Шоста група вчинення кримінальних правопорушень, що вчиняються з використанням інформаційних технологій (кіберзлочинів), передбачає поширення шкідливого контенту (спаму, погроз, створення, поширення, збут дитячої порнографії, заклики до вчинення насильства, домагання), яке може негативно вплинути на психологічний стан особи чи осіб.

Сьома група способів вчинення – це незаконне копіювання, поширення або публікація програмного забезпечення, ігор та все, що захищено авторським чи суміжним правом через кіберпростір чи за допомогою засобів інформаційних технологій.

Висновки. Безперечно, інтенсивний розвиток новітніх технологій зумовлює зловмисників прилаштовуватись і вигадувати нові способи незаконного використання інформаційних технологій у своїх злочинних намірах. Тому знання про типові способи вчинення кримінальних правопорушень із використанням інформаційних технологій як одного з елементів криміналістичної характеристики кримінальних правопорушень, що вчиняються з використанням інформаційних технологій (кіберзлочинів), сприяє більш ефективній організації їх розслідування. Насамперед визначення способу вчинення в поєднанні з іншими елементами криміналістичної характеристики зазначених кримінальних правопорушень дає змогу слідчому отримати інформацію про обставини вчиненого, скласти реальний план розслідування і визначитись із конкретними напрямами пошуку слідів протиправного діяння.

Список використаних джерел:

1. Батурин Ю.М., Жодзишский А.М. Компьютерная преступность и компьютерная безопасность. Москва : Юридическая литература, 1991. 157 с.
2. Белкин Р.С. Курс криминалистики : учебное пособие для вузов. 3-е изд., доп. Москва : ЮНИТИ-ДАНА, 2001. 837 с.
3. Біленчук П.Д., Лисиченко В.К., Клименко Н.І. та ін. Криміналістика : підручник / За ред. П.Д. Біленчука. Київ : Атіка, 2001. 544 с.
4. Благута Р.І, Сибірна Р.І., Бараняк В.М., Дуфенюк О.М. та ін. Криміналістика : навчальний посібник / за заг. ред. Є.В. Пряхіна. Київ : Атіка, 2012. 496 с.
5. Ботнет. URL: https://uk.wikipedia.org/wiki/%D0%91%D0%BE%D1%82%D0%BD%D0%B5%D1%82.
6. Великий тлумачний словник сучасної української мови / уклад. і голов. ред. В.Т. Бусел. Київ-Ірпінь : ВТФ «Перун», 2001. 1440 с.
7. Вехов В.Б. Компьютерные преступления: способы совершения, методика расследования. Москва, 1996. 182 с. URL: https://lawbook.online/kriminalisticheskaya-metodika-uchebnik/sposobyi-soversheniya-kompyuternyih-30023.html.
8. Вехов В.Б., Зуев С.В. Цифровая криминалистика : учебник для вузов. Москва, 2021. 417 с.
9. Волынский А.В. Криминалистика : учебник. Москва : Закон и право, ЮНИТИ-ДАНА, 1999. 615 с.
10. Зуйков Г.Г. Криминалистическое учение о способе совершения преступления : дис. ... д-ра юрид. наук. Москва, 1970. 395 с.
11. Колесниченко А.Н. Общие положения методики расследования отдельных видов преступлений. Харьков : Издательство Харьковского юридического института, 1965. 28 с.
12. Коновалова В.О. Вбивство: мистецтво розслідування : монографія. Харків : Факт, 2001. 311с.
13. Корноухов В.Е. Курс криминалистики. Общая часть. Москва : Юристь, 2000. 784 с.
14. Куранова Э.Д. Об основных положениях методики расследования отдельных видов преступлений. Вопросы криминалистики. 1962. № 6-7. С. 152–167.
15. Паламарчук Л.П. Криміналістичне забезпечення розслідування незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж : дис. ... канд. юрид. наук : 12.00.09. Київ, 2004. 214 с.
16. Погорецький М.А., Сергєєва Д.Б . та ін. Розслідування окремих видів злочинів : навчальний посібник. Київ : Алерта, 2015. 536 с.
17. Перехват данных по сети. URL: https://www.anti-malware.ru/threats/network-traffic-interception.
18. Самойленко О.А. Основи методики розслідування злочинів, вчинених у кіберпросторі : монографія. Одеса. 2020. 372 с.

19. Социальная инженерия. URL: https://ru.wikipedia.org/wiki/%D0%A1%D0%BE%D1%86%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D0%B8%D0%BD%D0%B6%D0%B5%D0%BD%D0%B5%D1%80%D0%B8%D1%8F.
20. Уткин М.С. Особенности расследования и предупреждения хищений в потребительской кооперации. Сверловск: Издательство Свердловского юридического института, 1975. 57 с.
21. Шавер Б.М., Винберг А.И. Криминалистика. Москва : Юриздат, 1950. 324 с.
22. Шавер Б.М. Криминалистика. Москва : Юриздат, 1952. 412 с.
23. Computer. Oxford Learner's Dictionaries URL: https://www.oxfordlearnersdictionaries.com/definition/english/computer.
24. DoS-атака. URL: https://uk.wikipedia.org/wiki/DoS-%D0%B0%D1%82%D0%B0%D0%BA%D0%B0
25. Massive DDoS Attack Disrupts Belgium Parliament. URL: https://threatpost.com/ddos-disrupts-belgium/165911/.
26. Reference Incident Classification Taxonomy. URL: https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy.

References:

1. Baturin Y.M., Zhodzishsky A.M. Kompiuternaia prestupnost y kompiuternaia bezopasnost [Computer crime and computer security]. Moscov : Yurydycheskaia lyteratura, 1991. 157 рю [in Russian].
2. Belkin R.S. Kurs krymynalystyky: ucheb. posobye dlia vuzov [Course of criminalistics: Textbook. the manual for high schools]. Moscov: UNITY-DANA, 2001. 837 p. [in Russian].
3. Bilenchuk P.D., Lisichenko V.K., Klimenko N.I. and others. Kryminalistyka: Pidruchnyk [Criminalistics: textbook]. Kiev. Atika, 2001. 544 p. [in Ukrainian].
4. Blahota R.I., Sibirny R.I., Baranak V.M., Dufenyk O.M., etc. Kryminalistyka : navch. posib. [Criminalistics: [Textbook.]. Kiev: Atika, 2012. 496 p. [in Ukrainian].
5. Botnet. URL: https://uk.wikipedia.org/wiki/%D0%91%D0%BE%D1%82%D0%BD%D0%B5%D1%82 [in Ukrainian].
6. Busel V.T. Velykyi tlumachnyi slovnyk suchasnoi ukrainskoi movy [Big explanatory dictionary of the modern Ukrainian language]. Kiev-Irpen: VTF "Perun", 2001. 1440 p. [in Ukrainian].
7. Vekhov V.B. Kompiuternue prestuplenyia: sposobu sovershenyia, metodyka rassledovanyia [Computer crimes: methods of Commission, methods of investigation]. M. 1996. 182 p. URL: https://lawbook.online/kriminalisticheskaya-metodika-uchebnik/sposobyi-sovershheniya-kompyuternyih-30023.html [in Russian].
8. Vekhov V.B. Tsyfrovaia krymynalystyka : uchebnyk dlia vuzov [Digital forensics: a textbook for universities]. Moskva. 2021. 417 p. [in Russian].
9. Volynskiy A.V. Krymynalystyka : uchebnyk. [Criminalistics: textbook] Moscov : Zakon i pravo, YuNYTY-DANA, 1999. 615 p. [in Russian].
10. Zuikov G.G. Krymynalystycheskoe uchenye o sposobe sovershenyia prestuplenyia [Criminalistic teaching about the method of committing a crime]. Candidate's thesis. 1970. 395 p [in Russian].
11. Kolesnichenko A.N. Obshchye polozhenyia metodyky rassledovanyia otdelnukh vydov prestuplenyi [General provisions of methods of investigation of certain types of crimes]. Kharkiv. 1965. 28 p. [in Russian].
12. Konovalova V.O. Vbyvstvo: mystetstvo rozsliduvannia [Murder: the art of investigation: monograph]. Kharkiv : Fact, 2001. 311 p. [in Ukrainian].
13. Kornoukhov V.E. Kurs krymynalystyky. Obshchaia chast [The Course is criminology]. Moscow: Yurist, 2000. 784 p [in Russian].
14. Kuranova E.D. Ob osnovnukh polozhenyiakh metodyky rassledovanyia otdelnukh vydov prestuplenyi [On the main provisions of the methodology of investigation of certain types of crimes]. Questions of criminalistics. Moscow, 1962. № 6-7, 152–167 [in Russian].
15. Palamarchuk L.P. Kryminalistychne zabezpechennia rozsliduvannia nezakonnoho vtruchannia v robotu elektronno-obchysliuvalnykh mashyn (kompiuteriv), system ta kompiuternykh merezh [Criminalistic support of investigation of illegal interference in the work of electronic computers (computers), systems and computer networks]: dys. ... kand. yuryd. nauk. 2004. 214 p. [in Ukrainian].
16. Pogoretsky M.A., Sergeeva D.B., etc. Rozsliduvannia okremykh vydiv zlochyniv : navchalnyi posibnyk [Investigation of certain types of crimes: a textbook]. Kiev: Alerta, 2015. 536 p. [in Ukrainian].
17. Perekhvat dannukh po sety [Network data interception].URL: https://www.anti-malware.ru/threats/network-traffic-interception. [in Russian].
18. Samoilenko O.A. Osnovy metodyky rozsliduvannia zlochyniv, vchynenykh u kiberprostori : monohrafiia [Fundamentals of methods of investigating crimes committed in cyberspace: a monograph]. Odesa. 2020. 372 p. [in Ukrainian].
19. Sotsyalnaia ynzheneryia [Social engineering]. URL: https://ru.wikipedia.org/wiki/%D0%A1%D0%BE%D1%86%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D0%B8%D0%BD%D0%B6%D0%B5%D0%BD%D0%B5%D1%80%D0%B8%D1%8F [in Ukrainian].
20. Utkin M.S. Osobennosty rassledovanyia y preduprezhdenyia khyshchenyi v potrebytelskoi kooperatsyy [Features of investigation and prevention of theft in consumer cooperation]. Sverlovsk. 1975. 57 p. [in Russian].
21. Shaver B.M., Vinberg A.I. Krymynalystyka [Criminalistics]. Moscow: Yurizdat, 1950. 324 p. [in Russian].
22. Shaver B.M. Krymynalystyka [Criminalistics]. Moscow: Yurizdat, 1952. 412 p. [in Russian].
23. Computer. Oxford Learner`s Dictionaries. URL: https://www.oxfordlearnersdictionaries.com/definition/english/computer [in English].
24. DoS-ataka [DoS attack]. URL: https://uk.wikipedia.org/wiki/DoS-%D0%B0%D1%82%D0%B0%D0%BA%D0%B0 [in Ukrainian]
25. Massive DDoS Attack Disrupts Belgium Parliament. URL: https://threatpost.com/ddos-disrupts-belgium/165911/ [in English].
26. Reference Incident Classification Taxonomy. URL: https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy. [in English].