у працездатному віці, якій притаманна девіантна поведінка і зловживає алкогольними напоями. Здебільшого вказана особа має певний соціальний зв'язок зі злочинцем або спільних друзів чи знайомих.

Зважаючи на викладене, можна зробити висновок, що елемент «особа потерпілого» тісно пов'язаний з особою злочинця.

Список використаних джерел

1. Кримінальний процесуальний кодекс України : закон від 12.04.2012 р. № 4651-VI // Відомості Верховної Ради України – 2013. № 9-13 ст. 88. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/4651-17/page3
2. Кримінальний кодекс України : закон від 05.04.2001 р. № 2341-III // Відомості Верховної Ради України. – 2001. № 25-26, ст.131 [Електронний ресурс]. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/2341-14.
3. Франк Л. В. Виктимология и виктимность / Л. В. Франк. – Душанбе : Ирфон, 1972. – С. 34.
4. Катеринчук К. В. Кримінально-правові та кримінологічні заходи запобігання катуванням: дис. ...канд. юрид. наук : спец. 12.00.08 / К. В. Катеринчук. – К., 2009. – 239 с.

Ключові слова: катування, особа потерпілого, віктимність, елемент криміналістичної характеристики, особа злочинця.

Науковий керівник: к.ю.н., Гресь Ю. О.

Максимчук Юлія Вікторівна

студентка 4 курсу Інституту кримінальної юстиції
Національного університету «Одеська юридична академія»

ОСОБЛИВОСТІ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ ТА ПРОТИДІЇ ЇХ ВЧИНЕННЯ

На сьогодні проблема боротьби з кіберзлочинністю є надзвичайно актуальною. Це передусім пов'язано з розвитком і вдосконаленням комп'ютерних систем, електронно-обчислювальних машин, автоматизованих систем, а також поширенням використання комп'ютерних технологій, мережі Інтернет у всіх сферах діяльності людини. До кіберзлочинів може бути віднесено будь-який злочин, вчинений в електронному середовищі.

Кіберзлочинність не обмежується рамками злочинів вчинених у глобальній інформаційній мережі Інтернет, вона поширюється на всі види злочинів, вчинених в інформаційно-телекомунікаційній сфері, де інформація, інформаційні ресурси, інформаційна техніка можуть виступати предметом злочинних посягань, середовищем, в якому

відбуваються правопорушення і засобом або знаряддям злочину. Це і створення з метою використання, збуту шкідливих програмних чи технічних засобів, перешкоджання роботі комп'ютерних систем, несанкціоноване втручання в роботу комп'ютерних і телекомунікаційних мереж, викрадення даних з обмеженим доступом, електронне вимагання та інші.

Розслідування таких злочинів ускладнюється їх підвищеною латентністю. У злочинців є можливість змінити, приховати комп'ютерні дані, що можуть буду доказами. Існує проблема огляду комп'ютерних систем, технічних пристроїв, на яких міститься інформація. Також ускладненою є процедура вилучення, дослідження та фіксації слідів вчинення кіберзлочинів. Цьому сприяє недостатнє технічне забезпечення органів досудового розслідування, оперативних підрозділів. Для розкриття подібних правопорушень обов'язковим є залучення спеціалістів та експертів, що мають спеціальні знання у комп'ютерно-технічній сфері [2, с. 102-103].

При розслідуванні такого виду злочинів слідчий має звертати особливу увагу на особу злочинця. Важливо підкреслити, що особам, які вчиняють злочини у комп'ютерній сфері, притаманний високий рівень інтелектуального розвитку, професіоналізм, висока зацікавленість новими комп'ютерними технологіями. Більшість таких осіб знають декілька мов програмування, мають значний досвід роботи на комп'ютері, в минулому до кримінальної відповідальності не притягувався. мають розвинене формально-логічне мислення, можуть використовувати комп'ютерний жаргон. Також суб'єктом злочину можуть бути «білокомірцеві злочинці», які вчиняють злочини, пов'язані безпосередньо з їх службовою діяльність, шляхом використання доступу до певних комп'ютерних інформаційних систем та електронних баз даних. Такі особи зазвичай керуються корисливими мотивами.

Проведенню слідчих дій має обов'язково передувати ретельна підготовка, що включає: визначення часу, місця проведення; підготовку комп'ютерно-технічних засобів, в тому числі технічних засобів фіксації результатів проведення слідчої дії, вивчення матеріалів кримінального провадження.

Першочерговим завданням слідчого на початковому етапі розслідування кіберзлочинів є аналіз інформаційного середовища вчинення злочину:

– визначення типу електронно-обчислювальної машини (носія), де зберігалася або оброблялася комп'ютерна інформація, до якої здійснено неправомірний доступ (Web-сервер, персональний комп'ютер, мобільний телефон, електронна кредитна карта), що визначить напрямок всього подальшого розслідування;

– встановлення типу операційної системи комп'ютера (сервера), до якого здійснено неправомірний доступ (Unix, Linux, Netware, Windows), а також використаного для вчинення злочину програмного

забезпечення, що значною мірою допоможе звузити коло можливих підозрюваних;

– визначення апаратного та програмного забезпечення, яке піддалося впливу в ході неправомірного доступу, а також інформації про засоби і знаряддя вчинення такого доступу, що дозволить скласти об'єктивну картину слідів злочину [1, с. 181-182].

Зростання кількості кіберзлочинів вимагає вжиття заходів щодо їх запобігання та протидії вчинення. Необхідним є належне законодавче закріплення такого виду правопорушень. У Кримінальному кодексі України зазначені види злочинів визначаються розділом XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». Також у жовтні 2017 року був прийнятий ЗУ «Про основні засади забезпечення кібербезпеки в Україні», який набирає чинності 09.05.2018.

Ефективними способами протидії кіберзлочинності можуть бути: вдосконалення методів та прийомів розслідування, розробка нових способів виявлення та дослідження обставин вчинення таких злочинів, забезпечення технічної оснащеності органів досудового розслідування. Важливою умовою боротьби з кіберзлочинністю є підготовка фахівців належної кваліфікації для збільшення ефективності розслідування та розкриття злочинів даної специфіки.

Список використаних джерел

1. Бурбело Б.А. Криміналістичні основи протидії кіберзлочинності//Актуальні питання розслідування кіберзлочинів: матеріали Міжнародної науково-практичної конференції, 10 грудня 2013р. – Харків : Харківський національний університет внутрішніх справ, 2013. – С.179-182.
2. Організаційно-правові та тактичні основи протидії злочинності у сфері високих інформаційних технологій: [навч. посіб] / В.М. Бутузов, В.Д. Гавловський, Л.П. Скалозуб та ні. - К. : Нац. акад. СБУ України, 2011. – 404 с.
3. Кримінальний кодекс України: Закон від 05.04.2011 № 2341-III // Відомості Верховної Ради України (ВВР), 2011, № 25-26, с. 197.
4. Про основні засади забезпечення кібербезпеки України: Закон від 05.10.2017 № 2163-VIII // Відомості Верховної Ради України, 2017 р., № 45 // набирає чинності 09.05.2018.

Ключові слова: кіберзлочинність, кіберзлочин, мережа Інтернет, електронно-обчислювальна машина, операційна система, програмне забезпечення.

Науковий керівник: к.ю.н., доцент кафедри криміналістики Паляничко Д. Г.