Кубишин Ігор Ігорович
студент 3-го курсу ННІ № 3
Національної академії внутрішніх справ
Науковий керівник: **Сокиран Ф.М.**
професор кафедри криміналістики та
судової медицини, к.ю.н., доцент

ДЕЯКІ ЕЛЕМЕНТИ КРИМІНАЛІСТИЧНОЇ ХАРАКТЕРИСТИКИ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, УЧИНЕНИХ З ВИКОРИСТАННЯМ ШКІДЛИВИХ ПРОГРАМНИХ ЧИ ТЕХНІЧНИХ ЗАСОБІВ

Реалії сьогодення свідчать про гостру потребу в якісній та ефективній протидії злочинності, у тому числі кримінальним правопорушенням, учиненим з використанням шкідливих програмних чи технічних засобів.

Сучасний стан інформатизації суспільства створює нові, раніше не знайомі вітчизняному законодавству про кримінальну відповідальність, форми протиправної поведінки, відкриває нові «горизонти» для професійної злочинності.

Вчинення протиправних посягань з використанням шкідливих програмних чи технічних засобів, окрім високої теоретичної підготовки, потребує використання злочинцями сучасних технічних засобів. Загальна система криміналістичної характеристики кримінальних правопорушень, учинених звикористанням шкідливих програмних чи технічних засобів включає базові елементи (дані про), що притаманні кримінальним правопорушенням цієї категорії. Варто віднести до системи таких елементів: дані про об’єкт протиправного посягання; дані про предмет протиправного посягання; дані про обстановку вчинення кримінального правопорушення (місце, час, інші умови); дані про особу злочинця; дані про особу потерпілого; дані про механізм кримінального правопорушення; дані про способи підготовки кримінального правопорушення.[1, с.112-113].

Програмні засоби нерозривно повязані із функціонуванням ЕОТ (електронно - обчислювальна техніка), вони сприяють посиленню розумових здібностей людини, швидкому опрацюванню значного масиву інформації, виконанню складних і специфічних обчислень, що відповідає вимогам науково-технічного прогресу [2, с.90].

За конструктивними особливостями ШПЗ (шкідливий програмний засіб) може бути як нескладним програмним засобом з обмеженим функціоналом, призначеним для виконання окремих, конкретно визначених дій, так і складним програмним комплексом зі значною кількістю модулей, частини яких, залежно від програмно значущих подій або вказівк користувача, оператора (розробника), можуть підключатися (завантажуватися через мережу) для використання за певним цільовим призначенням (наприклад, ШПЗ виявив, що на ЕОТ встановлено програмний

засіб «клієнт-банк», але для перехоплення інформації необхідно встановити певний модуль) [3, с.354]. У більшості випадків метою такого виду кримінальних правопорушень є вигода. Останнім часом вони вчиняються також за політичними мотивами (шпіонаж, тероризм), через дослідницький інтерес (студенти, професіонали-програмісти), із хуліганських мотивів та з метою помсти.

Виділяють три основні групи потерпілих від кримінальних правопорушень, учинених з використанням шкідливих програмних чи технічних засобів: 1) власники комп'ютерної системи; 2) клієнти, які користуються їх послугами; 3) інші особи [4, с.73].

Криміналістичну характеристику кримінальних правопорушень, учинених з використанням шкідливих програмних чи технічних засобів, варто уявляти як «шаблон», котрий необхідно накладати на вихідні дані розслідуваного кримінального правопорушення для виокремлення окремого із загального з метою визначення напрямку і завдань розслідування та конструювання дій [5, с.219]. Алгоритми, які використовуються при розслідуванні кримінальних правопорушень, учинених з використанням шкідливих програмних чи технічних засобів, не мають однозначної (жорсткої) структури. Пояснюється це індивідуальним відображенням події кримінального правопорушення в просторі. Вирішення низки завдань, які виникають у процесі розслідування, за допомогою алгоритмів сприяють прийняттю ефективних тактичних рішень.

Існує чимало проблем правового та експертного забезпечення розслідування кримінальних правопорушень, учинених з використанням шкідливих програмних чи технічних засобів, які зумовлені складністю виявлення цих високотехнологічних кримінальних правопорушень, високим рівнем їх латентності, недосконалістю статистичного обліку, відсутністю комплексної підготовки фахівців відповідного рівня, що ускладнюють узагальнення слідчої, судової та експертної практики.

Список використаних джерел

1. Чорноус Ю. М. Криміналістичне забезпечення розслідування злочинів : монографія. Вінниця : ТОВ «Нілан-ЛТД», 2017. 492 с.
2. Ричка Д.О. Комп'ютерні віруси - шкідливі програмні засоби, рушійна сила модифікації. *Науковий вісник Херсонського державного університету.* Херсон, 2018. Вип. 1. Том 2. С. 89-93.
3. Кунинець А.І., Грицюк Ю.І. Інформаційні загрози та проблеми забезпечення інформаційної безпеки промислових компаній. *Науковий вісник НЛТУ України.* 2013. Вип. 23.2. С. 352-360.
4. Волобуєв А.Ф. Основи методики розслідування злочинів, вчинених у кіберпросторі. Одеса : ТЕС, 2020. 372 с.
5. Бородай О. В. Особа злочинця як елемент криміналістичної характеристики несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем,

комп'ютерних мереж і мереж електрозв'язку. *Вісник ЛДУВС ім. Е.О. Дідоренка*. 2018. Вип. 4 (84). С.212-220.

Чичкало Марина Андріївна
студент 3-го курсу ННІ №3
Національної академії внутрішніх справ
Науковий керівник: **Сокиран Ф.М.,**
професор кафедри криміналістики та
судової медицини, к.ю.н. ,доцент

ТЕХНІКО-КРИМІНАЛІСТИЧНЕ ДОСЛІДЖЕННЯ ГРОШОВИХ ЗНАКІВ

Як відомо, гроші є одним із атрибутів ідентифікації нації, символів державотворення і влади, головним об'єктом грошово-кредитної політики країни. Підробка грошей завжди каралася законом, але, незважаючи на це, фальшивомонетники постійно намагаються підробити банкноти. У свою чергу, держави працюють над шляхами вдосконалення характеристик своїх банкнот проти підробки.

В даний час, коли кількість користувачів вільно конвертованої валюти перевищує мільйони, а через комерційні банки і інші структури щодня проходить мільйони доларів, євро, фунтів стерлінгів, завдання швидкого і надійного визначення можливих підроблених банкнот стає першочерговим.

Практично всі виявлені підроблені грошові знаки виготовлені поліграфічним способом або із застосуванням кольорового копіювально-розмножувальної техніки в виробничих умовах. Це забезпечує досить високу їх якість, вимагає наявності у співробітників правоохоронних органів і банківської системи спеціальних знань для виявлення підробок, що вказує на необхідність оволодіння методикою дослідження грошових знаків на основі застосування новітніх технічних і програмних засобів.

Впровадження нових паперових банкнот, хоча і зменшує кількість підробок, але відсоток підробок, які майже не відрізнити від реальних грошей дуже великий. Сьогодні існує безліч способів підробки грошей і багато літератури про технологію виготовлення справжніх банкнот і, звичайно, сучасні високотехнологічні принтери та сканери. Тому дана тема є надзвичайно актуальна.

Елементи захисту валюти, та самі зображення, гарантують якість та захисту від підробок. Захист може створюватися за допомогою поліграфічних засобів та фізико-хімічних методів [1, с. 48].

Для надійного захисту від підробок валюти оформляють складними зображеннями, такими як візерунки, розетки та інші складні конструкції [2].

Техніко-криміналістичне дослідження грошових знаків забезпечується вивченням систем захисту грошових знаків, методики встановлення підробки грошових знаків та знанням сучасного обладнання, яке використовується при дослідженні грошових знаків.