ни різна кількість і різна послідовність психотипів. Ведучий психотип визначає основний мотив, головну мету поведінки, а другий – інструменти досягнення цієї мети.[1] Тобто поведінка конкретного індивідуума може значно ухилятися від стандартної моделі, тому важливо звертати увагу на базову лінію поведінки і контекст при інтерпретації невербальних сигналів.

Отже, первинна інформація про вчинений злочин завжди надходить від місця вчинення злочину і спілкування з людьми (часто різних процесуальних статусів). І в тому, і в іншому випадку у своїй діяльності слідчий повиненкористуватися методом профайлінгу для подальшого успішного встановлення психологічного контакту з особами, які будуть допитані на етапі досудового розслідування шляхом аналізуіх поведінки, характеру і особливості вчиненого злочину, попередньо визначивши психотип особи, який дасть змогу обрати ефективні криміналістичні прийоми.

На практиці оволодіння методом профайлінгу буде дуже доречним для співробітників правоохоронних органів, адже часто не вистачає часу для глибокого вивчення особистості і діяти потрібно швидко за ситуацією, яка склалася. За методом профайлінгу сама людина є джерелом інформації, її дії , рухи, емоції, навіть письмо, можуть розповісти про її мотиви спілкування, цілі і неправду. При проведенні огляду місця події, обшуку і інших слідчих (розшукових) дій цей метод дає підґрунтя в формуванні портрету злочинця, спрогнозувати його поведінку. Це, сприятиме звуженню кола підозрюваних та дає можливість пришвидшити процес досудового слідства.

1. [Електоронний ресурс] : - http://yurpsy.com/files/xrest/2/160.htm

2. [Електронний ресурс] : - http://anna-kulik.ru/3093

3. А.В. Дулов, Введение в судебнуюпсихологию, М., «Юридическаялитература», 1969, с.160

4. Л.Е. Владимиров, Учения об уголовных доказательствах, СПб., 1910, с.294

Байдуж Юлія Ігорівна
студентка юридичного факультету
Дніпропетровського державного
університету внутрішніх справ

Науковий керівник – доцент кафедри
економічної та інформаційної безпеки,
к.т.н., доц. ***Косиченко О.О.***

ПРОБЛЕМИ ЛАТЕНТНОСТІ КІБЕРЗЛОЧИНІВ

На сьогодні комп’ютерні злочини є однією з найдинамічніших груп суспільно небезпечних посягань. Швидко збільшуються показники поширення

цих злочинів, а також постійно зростає їх суспільна небезпечність. Однак, дана група злочинів також характеризується певною латентністю. Дана проблема зумовлена прискореним розвитком науки й технологій у сфері комп'ютеризації, а також постійним і стрімким розширенням сфери застосування комп'ютерної техніки.

Так, вітчизняне законодавство також намагається пристосуватися до реалій сьогодення, приділяючи даному питанню значну увагу у Кримінальному кодексі України, де передбачено самостійний розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж». Однак, на протязі певного проміжку часу, даний розділ змінювався та доповнювався, що свідчить про певну актуальність даного питання та те, що законодавство України динамічно розвивається і не стоїть на місці.

Так, чітко визначено поняття латентності у кримінології, де зазначається, що латентність це частина злочинності, яка складається зі злочинів, що фактично були вчинені, але не отримали відображення у офіційній загальнонаціональній кримінально-правовій статистиці.

Існування латентної злочинності сприяє формуванню невірного уявлення про реальну суспільну небезпечність і масштаби злочинності та призводить до похибок у прогнозуванні злочинності, плануванні заходів з протидії їй, до невірного розрахунку матеріального й кадрового забезпечення правоохоронних органів та інших негативних наслідків.

Ми повністю погоджуємося із даним визначенням, адже ніщо інше не ставить в оману суспільство як невірне уявлення про реальну суспільну небезпеку певних злочинів.

Важливим залишається розкриття змісту поняття кіберзлочинності. Так, кіберзлочинність - це злочинність у так званому «віртуальному просторі». Віртуальний простір можна визначити як простір, що моделюється за допомогою комп'ютера інформаційний, у якому перебувають відомості про особи, предмети, факти, подіях, явищах і процесах, представлені в математичному, символьному або будь-якому іншому виді й рухи, що перебувають у процесі, по локальних і глобальних комп'ютерних мережах, або відомості, що зберігаються в пам'яті будь-якого фізичного або віртуального устрою, а також іншого носія, спеціально призначеного для їхнього зберігання, обробки й передачі.

Так, загалом більшість кіберзлочинів, на нашу думку, є латентними. Адже для того щоб попереджати та розкривати даний вид злочинів потрібно не тільки бути досвідченим у цій справі, але й мати певні технологічні можливості, які на даний час правоохоронним органам не доступні.

Окрім того, з'ясовано, що цей вид злочинів у нашій країні має дуже високий рівень латентності: вони приховані від офіційної статистики. Показники стосовно злочинів, які вчиняються з використанням комп'ютерних технологій, розпорошені у відомчих обліках. За експертними оцінками, рівень ла-

тентності кіберзлочинності становить 90–95 %.

Перш за все, слід виділити наступні чинники, які зумовлюють латентність кіберзлочинів: низький рівень спеціального технічного оснащення правоохоронних органів сучасними засобами комп'ютерної техніки та комп'ютерними технологіями; відсутність знань та навичок виявлення, розкриття та розслідування кіберзлочинів через обмеження доступу до відповідних методик, тактики та техніки; низький рівень інформаційної культури, підготовленості широкого кола кадрів правоохоронних органів та суддів щодо притягнення винних до кримінальної відповідальності; недовіра потерпілих до правоохоронних органів (пов'язане з вищезазначеними чинниками) і т. ін.

Однак, органи державної влади в межах своїх повноважень намагаються не тільки розкрити дані злочини, але й попередити їх виникнення.

Так, серед заходів державно-правового характеру, які застосовують для попередження та виявлення латентних кіберзлочинів, можна виділити такі як:

- створення Урядом України спеціальних організаційних структур з питань координації напрацювання державної політики у сфері організаційно-правового забезпечення входження нашої держави у світове інформаційне суспільство.
- ініціація ряду нормативно-правових актів: Концепції національної інформаційної політики та інформаційної безпеки України; а також Стратегії впровадження національної інформаційної політики на розгляд Верховної Ради України (Відповідно до Указу Президента України від 6 грудня 2001 р. № 1193 Уряду доручено).

Однак, даних превентивних заходів вже не достатньо, з кожним роком шкода збільшується, а злочини стають все більш «вишуканими». Найпоширенішими кіберзлочинами є злом баз даних компаній та урядових організацій, виведення з ладу промислових об'єктів. До цього, наприклад, призвела атака вірусу на іранську АЕС у Бушері. Також широко відомі крадіжки інновацій або технологій і, нарешті, банальна крадіжка грошей.

Для забезпечення кібербезпеки існують різноманітні міжнародні договори (угоди), так у 2002 році Організація Об'єднаних Націй видала резолюцію Генеральної Асамблеї, де були прийняті «Елементи для створення глобальної культури кібербезпеки». В документі зазначається 9 основних взаємодоповнюючих елементів, які держави-учасники повинні дотримуватися, серед них: обізнаність, відповідальність, реагування, етика, демократія, оцінка ризику, проектування та впровадження засобів забезпечення безпеки, управління забезпеченням безпеки та переоцінка.

Отже, вважаємо, що кіберзлочинність - це проблема, з якою зіштовхнулась планета у 21 столітті, і яка обіцяє рости та поглинати все більше ресурсів. Загалом майже вся кіберзлочинність має латентний характер, що відрізняє її від більшості злочинів та у той же час робить однією з найнебезпечніших у світі. На наш погляд, вже не достатньо існуючих заходів для виявлення та попере-

дження кіберзлочинів, зараз вітчизняне законодавство потребує ґрунтовної реформації у частині виявлення кіберзлочинів, що у майбутньому має на меті не тільки зменшення, але й повне винищення такого явища як латентна кіберзлочинність. Проблема профілактики і стимулювання кіберзлочинності в Україні – це комплексна проблема. Сьогодні закони повинні відповідати вимогам, що пред'являються сучасним рівнем розвитку технологій. Вважаємо, що пріоритетним напрямком має бути організація взаємодії і координація зусиль правоохоронних органів, спецслужб, судової системи, забезпечення їх необхідною матеріально-технічною базою, адже на даний час, дана проблема потребує координації не тільки у середині країни, але й об'єднання країн для досягнення спільної мети – знищення кіберзлочинності як явища.

1. Довбиш Н. Кіберзлочинність в Україні [Електронний ресурс]: - [Режим доступу]: https://www.science-community.org/ru/node/16132
2. Гавловський В.Д. Кіберзлочинність як чинник державної інформаційної політики України [Електронний ресурс]: - [Режим доступу]: http://www.crime-research.ru/library/Gavlovsk.htm
3. Голіна В.В. Поняття та кримінологічна характеристика кіберзлочинності [Електронний ресурс]: - [Режим доступу]: http://lib-net.com/book/105_Kriminologiya_Zagalna_ta_Osobliva_chastini.html
4. Комасюк І.С. Кіберзлочинність і сьогодення [Електронний ресурс]: - [Режим доступу]: http://ukrainepravo.com/legal_publications/essay-on-it-law/it_law_komasyuk_cybercrime/

Бакало Вікторія Олександрівна
курсант факультету підготовки фахівців
для органів досудового розслідування
Дніпропетровського державного
університету внутрішніх справ

Науковий керівник – старший викладач
кафедри кримінального права та кримінології,
к.ю.н., с.н.с. ***Березняк В.С.***

ДЕЯКІ ПИТАННЯ ЗАПОБІГАННЯ ЗЛОЧИНАМ, ЯКІ ВЧИНЯЮТЬСЯ ВІДНОСНО ОСІБ ПОХИЛОГО ВІКУ

За статистичними даними, Україна належить до «демографічно старих» країн світу, перед державою першочерговим є питання захисту осіб похилого віку від протиправних посягань та проведення профілактики щодо викорінення кримінальних та адміністративних правопорушень стосовно осіб похилого віку. Досліджуючи статистичні дані, виявлено, що станом на червень 2017 року, по відношенню до осіб похилого віку, які стали жертвами внаслі-