МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ДНІПРОПЕТРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

КАФЕДРА ЕКОНОМІЧНОЇ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

ВИКОРИСТАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Матеріали
Всеукраїнського науково-практичного семінару
(м. Дніпро, 28 листопада 2019 р.)

Дніпро – 2019

УДК 351.74 + 004.9
В 43

Рекомендовано до друку Науково-методичною радою Дніпропетровського державного університету внутрішніх справ (протокол № 4 від 24.12 2019)

В 43 Використання сучасних інформаційних технологій в діяльності Національної поліції України: матеріали Всеукраїнського науково-практичного семінару (28 листопада 2019 р., м. Дніпро). – Дніпро: Дніпропетровський державний університет внутрішніх справ, 2019. – 140 с. *(у авторській редакції)*

ISBN 978-617-7665-10-5

У матеріалах семінару розглянуто актуальні питання використання сучасних інформаційних технологій у діяльності як Національної поліції, так і інших правоохоронних органів України.

Для викладачів та здобувачів вищої освіти спеціалізованих ЗВО, фахівців у галузі кібербезпеки.

СКЛАД ОРГАНІЗАЦІЙНОГО КОМІТЕТУ
Всеукраїнського науково-практичного семінару "Використання сучасних інформаційних технологій в діяльності Національної поліції України"

Голова оргкомітету – **Наливайко Лариса Романівна**, проректор університету, д.ю.н., професор, Заслужений юрист України;
Заступник голови оргкомітету – **Рижков Едуард Володимирович,** завідувач кафедри економічної та інформаційної безпеки, к.ю.н., доцент;

Члени оргкомітету:
Марченко Олена Вікторівна - начальник відділу організації наукової роботи, д.філос.н., доцент; **Шнурко Яна Вікторівна** - завідувач відділення зв'язків з громадськістю; **Самотуга Андрій Валерійович** - к.ю.н., доцент, заступник завідувача редакційно-видавничого відділення; **Косиченко Олександр Олександрович** – відповідальний секретар семінару, доцент кафедри економічної та інформаційної безпеки; к.т.н., доцент; **Мирошниченко Володимир Олексійович** – доцент кафедри економічної та інформаційної безпеки, к.т.н., доцент; **Краснобрижий Ігор Володимирович** – доцент кафедри економічної та інформаційної безпеки, к.ю.н.; **Махницький Олександр Васильович –** старший викладач кафедри економічної та інформаційної безпеки; **Гавриш Олег Степанович** - старший викладач кафедри економічної та інформаційної безпеки; **Тютченко Світлана Миколаївна –** старший викладач кафедри економічної та інформаційної безпеки.

ISBN 978-617-7665-10-5

ЗМІСТ

ТЕЗИ ВИСТУПІВ

Фоменко А.Є. - ректор Дніпропетровського державного університету внутрішніх справ, кандидат юридичних наук;
Вишня В.Б. - професор кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ, доктор технічних наук, професор.

СИСТЕМИ УПРАВЛІННЯ НАРЯДАМИ ПАТРУЛЬНОЇ СЛУЖБИ

Одним із важливих елементів в реформування та розбудови Національної поліції України є створення мобільних патрульних нарядів, які першими реагують на виклик про допомогу, або повідомлення про вчинене правопорушення чи злочин. Тому доцільно розглянути ефективність реагування на сповіщення підрозділів Національної поліції України (у подальшому – поліція) та відпрацювання нарядами мобільної патрульної служби отриманого завдання [1].

В основу вдосконалення системи управління нарядами мобільної патрульної служби, зокрема управління каналами відеопотоків між диспетчером і патрульним поліцейським, пропонується, шляхом уведення нових зв'язків елементів, забезпечити можливість відображення у диспетчера інформації, яка попадає в об'єктив відеорегістратора патрульного поліцейського Це дозволяє диспетчеру в режимі реального часу оперативно контролювати дії патрульного поліцейського в процесі відпрацювання поставленого завдання і, при необхідності, своєчасно втручатися в його роботу, та за рахунок цього підвищити ефективність та безпеку діяльності патрульного наряду (рис. 1)

Відомо, що короткострокова навчальна підготовка поліцейських для мобільної патрульної служби, не завжди дає достатньо знань для якісного виконання патрульним нарядом поставлених перед ними завдань. Тому, з метою поліпшення взаємодії диспетчера і поліцейських мобільних патрульних нарядів, в Дніпропетровському державному університеті внутрішніх справ (ДДУВС) було запропоноване рішення, коли, по прибуттю наряду на місці події або злочину, патрульний поліцейський включає перший канал передачі відеопотоків від особистого відеорегістратора патрульного до планшету, який працює в стандарті «Wi-Fi», та другий канал передачі – від планшету до блоку диспетчера системи оповіщення, який побудований по технології 4G або 5G, що забезпечує можливість висвітлення на моніторі диспетчера місця події з об'єктива особистого відеорегістратора патрульного при відпрацюванні завдання (рис. 1). Це дозволяє черговому диспетчеру, в разі необхідності, вмішуватися в хід виконання завдання нарядом, оперативно коригувати

дії наряду, виключити випадки некваліфікованих дій [1].

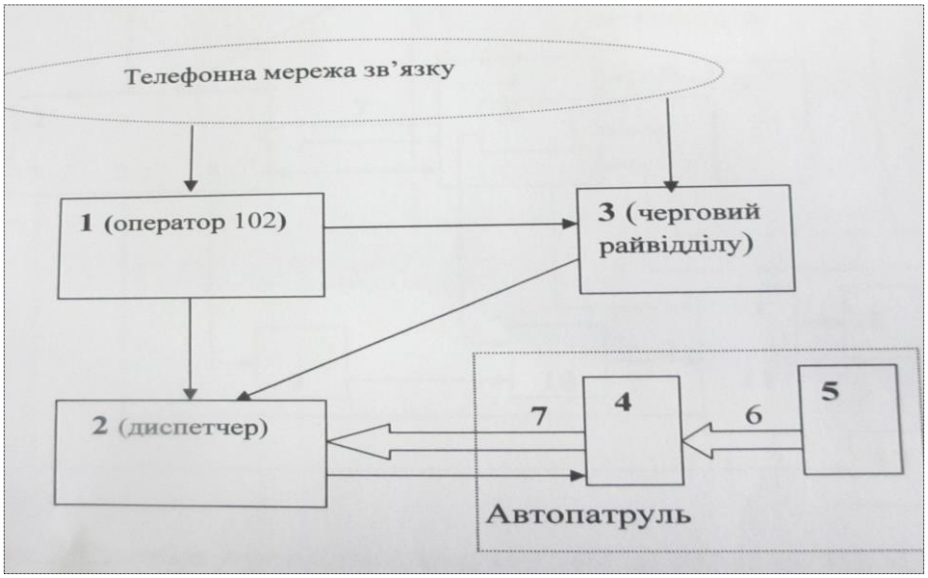


Рис.1. Система управління нарядами патрульної служби з відео каналами.
Де: 1- оператор 102, 2- диспетчер, 3- черговий районного відділу поліції,, 4- планшет мобільного патрульного наряду з системою супутникового GPS-позиціонування, 5 - особистий відеорегістратор патрульного, 6 та 7- перший та другий канали передачі відео потоку.

На жаль, в існуючої системі управління відсутня можливість автоматичного включення каналів передачі відеопотоків по прибуттю наряду на місце події, що не дозволяє виключити вплив людського фактору при активізації каналів системи.

Тому для подальшого вдосконалення системи управління нарядами мобільної патрульної служби, нами пропонується забезпечити можливість автоматичного включення каналів передачі відеопотоків і відображення на моніторі у диспетчера інформації з об'єктиву особистого відеорегістратора патрульного при відпрацюванні завдання, залишив, при цьому, можливість особистого управління цими каналами диспетчером і патрульним.

Для цього, у відому систему управління нарядами мобільної патрульної служби (рис. 1), введено додатково блок прийому координат події, модуль порівняння, логічну схему АБО, блоки формування сигналу на відкриття та закриття першого і другого каналів передачі відео потоків. На рис. 2 представлена схема запропонованої системи управління нарядами мобільної патрульної служби [2].

Схема системи включає блок 1 оператора 102, вхід якого приєднаний до телефонної мережі зв'язку, а перший та другий виходи підключені відповідно до першого входу блока 2 диспетчера та першого входу блока 3 чергового райвідділу поліції, другий вхід якого зв'язаний з телефонною мережею зв'язку. В той же час, вихід блоку 3 чергового райвідділу поліції підключений до другого входу блока 2 диспетчера, третій вхід якого (сумісний з виходом) приєднаний до планшету 4 мобільного патрульного наряду, який осна-

щений системою 8 супутникового GPS-позиціонування, та на якому побудовано перший канал передачі відеопотоку 6 від особистого відеорегістратора патрульного 5 до планшету 4 та другий канал передачі відеопотоку 7 від планшету 4 до блоку диспетчера 2.

Окрім того система додатково включає блок 9 прийому координат (адреси) події (завдання), вхід якого підключено до виходу блоку 2 диспетчера, а вихід блоку 9 прийому зв'язаний с другим входом модуля порівняння 10, перший вхід якого підключений до виходу системи 8 супутникового GPS-позиціонування. Вихід модуля порівняння 10 підключено до входу логічної схеми АБО 11, другий вхід якої приєднаний до виходу планшету 4, а третій – до другого виходу блоку 2 диспетчера, при тому, що вихід логічної схеми АБО 11 підключений до входу блока 12 формування сигналу відкриття каналів 6 та 7 передачі відеопотоків, вихід якого поступає на перший вхід планшету 4, другий вхід якого підключено до виходу блока 13. Формування сигналу закриття каналів передачі відеопотоків вхід якого зв'язаний з третім виходом блоку 2 диспетчера.

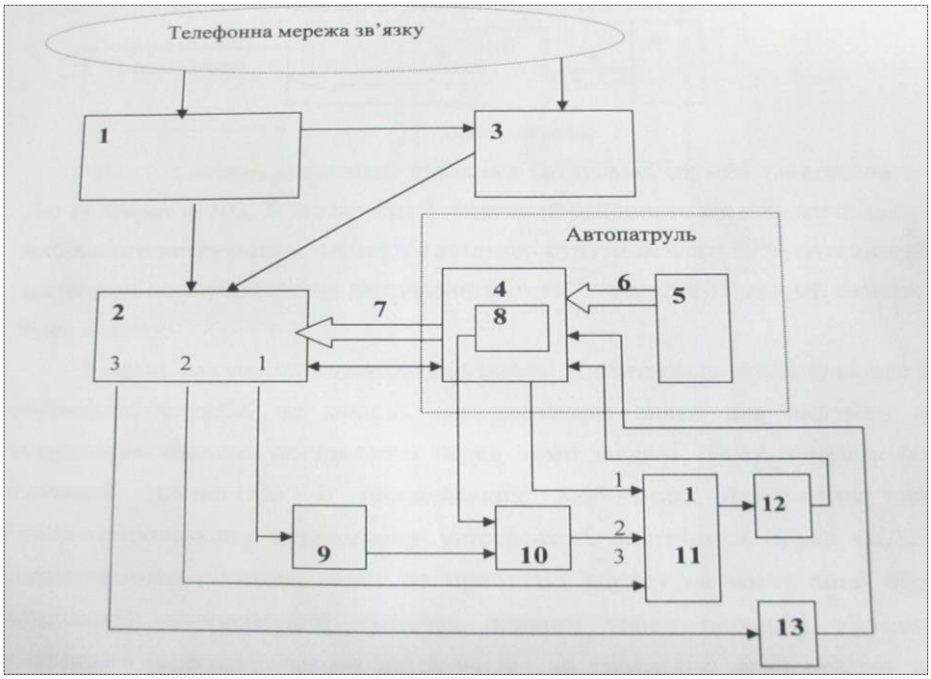


Рис.2 Система управління нарядами мобільної патрульної служби з різними способами підключення відеоканалів диспетчер - патрульний поліцейський.

Де: 1- оператор 102, 2- диспетчер, 3- черговий районного відділу поліції, 4- планшет мобільного патрульного наряду, 5- особистий відеорегістратор патрульного, 6 та 7- перший та другий канали передачі відеопотоку, 8- система супутникового GPS-позиціонування, 9- блок прийому координат, 10-модуль порівняння, 12 та 13- блоки формування сигналу відкриття та закриття каналів передачі відеопотоку відповідно.

Система реалізується в такий спосіб. Сповіщення поліції про злочини та події, або виклик допомоги, що здійснюються за телефоном 102, приймаються і обробляються оператором 102 (блок 1). В результаті створюється

електронна картка повідомлення, яка відразу надходить до блоку 2 диспетчера – чергового відповідального за управлінням мобільними нарядами патрульної поліції, який призначає вільний екіпаж мобільного патруля для реагування на повідомлення. Одночасно, електронна картка повідомлення надсилається черговому (блок 3) райвідділу поліції, до території якого відноситься звернення, яке реєструється у журналі "Єдиного обліку злочинів і правопорушень" райвідділу. Слід відмітити, що повідомлення громадян може поступити безпосередньо на телефон чергової частини райвідділу (блок 3). В цьому разі воно реєструється в журналі райвідділу і пересилається до оперативного диспетчера (блок 2) для реагування.

Виділеному диспетчером 2 мобільному патрульному наряду (автопатруль) пересилається на планшет 4 завдання та на блок 9 прийому координати місця події. Наряд приступає до виконання отриманого завдання. Місце знаходження наряду постійно відслідковується системою 8 супутникового GPS-позиціонування і відповідний сигнал подається на перший вхід модуля порівняння 10. По прибутті наряду на місце вказане в повідомлені громадян в планшеті 4 фіксується час прибуття, а сигнали на обох входах модуля порівняння 10 співпадають і на його виході формується сигнал, який поступає на перший вхід логічної схеми АБО 11 і далі на вхід блоку 12 формування сигналу відкриття каналів передачі відеопотоків. На виході блока 12 формується сигнал, який поступає на перший вхід планшету 4 і автоматично активізуються канали передачі відеопотоків 6 і 7 відповідно між особистим відеорегістратором 5 патрульного і планшетом 4 та між планшетом 4 і блоком 2 диспетчера. С цього моменту на монітор диспетчера передається відеоінформація місця події з об'єктиву особистого відеорегістратора 5 патрульного. По завершенню виконання завдання в планшеті 4 робиться відповідна відмітка, яка надсилається в блок 2 диспетчеру, з виходу якого, через блок 13 формування сигналу закриття каналів на другий вхід планшету 4 поступає сигнал на відключення каналів 6 і 7 передачі відеопотоку.

Слід відмітити, що окрім автоматичного включення каналів передачі відео потоків 6 і 7, система допускає особисту активізацію каналів 6 і 7 за командою диспетчера подачею сигналу з другого виходу блока 2 диспетчера на третій вхід логічної схеми АБО 11 і далі, з її виходу, через блок 12 формування сигналу відкриття каналів передачі відеопотоків, на перший вхід планшету 4. За командою патрульного – подачею сигнал з виходу планшету 4 другий вхід схеми АБО 11 і далі, з її виходу, через блок 12 формування сигналу відкриття каналів передачі відеопотоків, на перший вхід планшету 4.

Висновок. Перевагою запропонованої системи управління нарядами мобільної патрульної служби з відео потоками є можливість автоматичного включення каналів передачі відеопотоків з міста події або злочину до диспетчера, бо, інколи, патрульним приходиться негайно вмішуватися в ліквідацію обставин, що виникли при правопорушеннях. Важливим аспектом діяльності системи є також можливість, у любий момент, активізувати канали передачі відеопотоків безпосередньо командою диспетчера або патрульного, що поси-

лює надійність функціонування визначеної операції системи.

Наведені структурні рішення систем управління нарядами патрульної поліції відпрацьовуються в університеті в рамках навчальних занять «Інформаційна технічна платформа професійно-ділової ігри «Лінія 102»» курсантами, магістрами, співробітниками поліції в рамках підвищення кваліфікації та стажування.

Використані джерела:

1. Система управління нарядами мобільної патрульної служби /Вишня В.Б., Глуховеря В.А., Золотоноша О.В., Рижков Е.В.// Патент України на корисну модель № 118449. Україна. Бюл. №15, 10.08.2017.
2. Система управління нарядами мобільної патрульної служби /Вишня В.Б., Фоменко А.Є.// Патент України на корисну модель № 125582 Україна. Бюл. №9, 10.05.2018.

Бочковий О.В. - провідний фахівець науково-дослідної лабораторії з проблем попередження, припинення та розслідування злочинів територіальними органами НП України Луганського державного університету внутрішніх справ імені Е.О. Дідоренка, кандидат юридичних наук, старший науковий співробітник.

ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ УКРАЇНИ МАКЕТНОГО ТИПУ

Останнім часом, стала нормою організація різного роду медійних семінарів та нарад для презентації новітніх ідей та перспективних планів. При цьому, якщо раніше такі перформанси були притаманні приватним суб'єктам для популяризації своїх творінь, то сьогодні, це норма для усіх без виключення державних установ з обов'язковим висвітленням на сторінці у Фейсбук.

Будучи учасником міжнародного семінару з протидії фінансовим злочинам у лютому 2017 року, який проходив у Національній академії внутрішніх справ, від представників іноземних правоохоронних органів, які виступали як консультанти, почув вражаючу фразу: «ми втрачаємо зацікавленість у консультаціях, адже нічого, з того, що ми даємо, не впроваджується».

Дане спостереження й вплинуло на формулювання назви тез. Якщо проводити аналогію інформаційного забезпечення та машинобудування, то складається враження, що у нас є красивий макет автомобіля з анонсованими технічними характеристиками, але він не їздить, адже фактично у нього відсутній двигун та трансмісія.

Щоб не бути голослівним проаналізуємо світову практику інформаційно-аналітичного забезпечення правоохоронної діяльності. Так, ще у далекому

2001 році в англійському журналі «Police» опублікована стаття про використання сучасних інформаційних технологій у роботі фінансових слідчих. Адже давно відомо, що практично кожна особа залишає за собою електронний слід інформації (наприклад, у Великобританії загальна кількість баз даних, де громадяни можуть залишити електронний слід, у 2001 році становила близько трьохсот, сьогодні ця цифра значно більша). Перед слідчими постає завдання зібрати дані з цих баз відносно конкретної особи, потім відфільтрувати з цих відомостей такі, що відповідають параметрам розслідування, тобто, інакше кажучи, перевірити отриману інформацію стосовно більш широкого контексту розслідування для того, щоб звести воєдино всі відомості і провести аналіз, згідно з яким необхідно діяти далі [1; 2]. Правоохоронні органи зарубіжних країн широко використовують автоматизовані інформаційно-пошукові системи, які дозволяють значно оптимізувати розкриття та розслідування злочинів, учинених членами організованих угруповань [3, С. 57].

Більше того, новітні технології дають змогу активно та продуктивно протидіяти транснаціональній злочинності за рахунок відсутності кордонів у глобальній мережі. Значно полегшується взаємодія та обмін даними між правоохоронними органами різних країн. Наприклад, розшукуваний злочинець може бути встановлений шляхом застосування однієї з програм ідентифікації особи по фото чи відео зображенню [4; 5; 6].

Донедавна фантастичні уявлення щодо прогнозування злочинності знаходять своє відображення у реальних дослідженнях. Зокрема, у США та Японії вже почали тестувати програми передбачення злочинів із залученням штучного інтелекту [7; 8]. Ми є свідками виникнення нових відносин у сфері комп'ютерних технологій й робототехніки, більшість приватних та державних структур переходять на автоматичне адміністрування, запроваджується технологія блокчейн, тощо.

Будь-який сучасний сенсор може транслювати мільйони терабайт даних та 5 тис. годин відео високої чіткості за добу. Ця інформація збирається гігапіксельними камерами та сотнями сенсорів. Вже існують технології, котрі допомагають автоматично аналізувати величезні масиви текстів, причому проводити не структурний аналіз та пошук ключових слів, а семантичний. Система фактично розуміє зміст текстів. У перспективі цей самий підхід може використовуватись для аналізу відео- та статичного зображення, а також звуку.

Й при цьому, в Україні відсутній єдиний інформаційний простір. Навіть в рамках підрозділів Національної поліції України бази даних містять інформацію у несумісних форматах. Тільки з 2017 року почала діяти єдина база даних патрульної поліції по усій Україні, а до цього часу для отримання інформації з іншої області надсилались окремі запити, які оброблялись у ручному режимі.

У той же час, на наших очах відбувається збір, накопичення та використання інформації, отриманої з соціальних мереж. Адже ні для кого не секрет, що Google записує наші розмови, які здійснюються за допомогою про-

грамних продуктів, а Facebook вмикає камери та мікрофони мобільних пристроїв для збору інформації в комерційних цілях. Загроза витоку такої інформації чи потрапляння її до рук зловмисників також, нажаль, може мати місце [9].

При цьому, знову повертаючись до 2001 року, були спроби йти у ногу з часом в царині інформаційних технологій. Одним з прикладів успішного використання інформаційно-технічних досягнень в правоохоронній сфері була інформаційно-аналітична система «Сова», розроблена ще на початку 2000-х в УМВС України в Луганській області. Принциповою особливістю системи була інтеграція в єдиний інформаційний масив усіх наявних в УМВС відомчих інформаційних ресурсів (у тому числі масиви даних оперативно-розшукової діяльності) і бази даних інших відомств [10]. Повною мірою були реалізовані функції багатобазової структури: оператор системи міг підключити для забезпечення багатофакторного аналізу будь-яку базу даних, розташовану в будь-якій географічній точці. Система складала в одне ціле фрагменти інформації, отримані з різних джерел, та перетворювала їх у зрозумілі наочні графічні схеми [11, с. 265]**.** Завдяки відпрацьованим технологіям, за 9 місяців 2010 року тільки трьома співробітниками одного з підрозділів УІТ УМВС в Луганській області (відділу «ОРІОН») було розкрито 297 тяжких і особливо тяжких злочинів, розслідування яких традиційними методами виявилося невдалим [12; 13, С. 10].

Єдиним та основним «недоліком» даної системи, який не дозволив їй працювати на загальнодержавному рівні була її невідповідність тодішнім державно-політичним умовам. Адже можливості системи дозволяли в автоматичному режимі виявляти приховані зв'язки осіб, які займали високе положення у злочинній ієрархії й повідомляти про злочинні ризики у осіб, які займали відповідальні державні посади. Такі системи успішно діють у західних країнах та вдало виявляють корупційні правопорушення, але запровадження подібних в Україні тоді було не на часі. Зрештою, систему, під аггравовані лозунги захисту прав та свобод громадян, спочатку значно обмежили в можливостях, а потім, у 2014 році законсервували.

Таким чином, враховуючи сучасний рівень злочинності та наше стремління до євроінтеграції потрібно переглянути підходи до запровадження сучасних інформаційно-аналітичних систем у діяльність правоохоронних органів, зменшивши при цьому бюрократичний вплив на вказані процеси та, на кінець, перейшовши від макету до практичного застосування.

Використані джерела:

1. Police. – 2001. – September. – P. 24–27.
2. Выявление преступников с помощью информационных технологий // Борьба с преступностью за рубежом. Информбюллетень. – М: ВИНИТИ, 2003. – № 6. – С. 19-23.
3. Гуславский В.С. Информационно-аналитическое обеспечение раскрытия и расследования преступлений: монография / В.С. Гуславский, Ю.А. Задорожный, Б.Г. Розовский. – Луганск: Элтон-2, 2008. – 287 с.
4. Поиск человека по фотографи – это реальность URL: http://softopirat.com/main/399-

poisk-cheloveka-po-fotografii-yeto-realnost.html.
5. По фото в соцсети можно узнать о человеке все! URL: http://3rm.info/publications/13829-po-foto-v-socseti-mozhno-uznat-o-cheloveke-vse.html
6. Создана программа для поиска человека в Интернете по фото URL: http://zhzh.info/blog/2011-11-13-3096.
7. Илюхин Олег. В США втайне от граждан испытали технологию предсказания преступлений URL:https://hitech.vesti.ru/article/781523/
8. Японская полиция будет использовать искусственный интеллект для предсказания преступлений URL: http://tass.ru/obschestvo/4910175
9. К. Шиян. Google постоянно подслушивает вас через микрофон. Вот как найти эти записи! URL: https://lifter.com.ua/628/Google-postoyanno-podslushivaet-vas-cherez-mikrofon-Vot-kak-nayti-eti-zapisi
10. Інформаційно-аналітичне забезпечення оперативно-розшукової діяльності: монографія / [В.А. Буржинський, М.Г. Вербенський, В.С. Гуславський, та ін.]. – Луганськ: РВВ ЛДУВС ім. Е.О. Дідоренка, 2009. – 110 с.
11. Орлов Ю.Ю. Застосування оперативної техніки в оперативно-розшуковій діяльності міліції (теорія і практика): монографія / Ю.Ю. Орлов. — К.: Київський нац. ун-т внутрішніх справ, 2007. – 559 с.
12. Задорожний Ю.А. Информационные технологии в ОРД: опыт и проблемы или проблемы и опыт? / Ю.А. Задорожний, Б.Г. Розовский // Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка. - 2011. – № 4. – 219-228
13. Єфіменко В.В. Стислий аналіз оперативної обстановки в Луганській області та проблема підвищення професіонального рівня співробітників карного розшуку // Вісник ЛДУВС ім. Е.О. Дідоренка Спец. Випуск № 2 у двох частинах. Частина 1. Луганськ, 2009. – С.10-13.

Брисковська О. М. - провідний науковий співробітник наукової лабораторії з проблем протидії злочинності Національної академії внутрішніх справ, кандидат юридичних наук, старший науковий співробітник

ВАЖЛИВІСТЬ ВИКОРИСТАННЯ СОЦІАЛЬНО-ПСИХОЛОГІЧНОЇ ХАРАКТЕРИСТИКИ ІНТЕРНЕТ-ШАХРАЯ У РОЗСЛІДУВАННІ ЗЛОЧИНІВ ВЧИНЕНИХ В ІНТЕРНЕТ ПРОСТОРІ

В умовах сьогодення в нашій країні ми можемо спостерігати якісну зміну кримінального світу: у своїй злочинній діяльності кримінальні структури використовують найсучасніші досягнення науки і техніки, комп’ютерні системи та новітні інформаційні технології. Іншими словами у всьому світі відбувається процес інтенсивної інтелектуалізації злочинності[1, с. 170]. Суттєві зміни відбуваються і в діяльності правоохоронних органів. Зокрема на основі інформаційних технологій упроваджуються потужні інформаційно-пошукові системи, удосконалюється система управління та інформаційно-аналітичного забезпечення Національної поліції, розробляються нові методи

збирання й аналізу інформації, розширюються можливості спеціальних технічних засобів тощо [2].

Невпинне розширення Інтернету відбувається в процесі кардинальної трансформації сфер праці, споживання, дозвілля та політики. Однак те, що часто називають кіберпростором – є цариною комп'ютеризованої взаємодії, та дає можливість вчиняти широкий спектр потенційно злочинних діянь, як старих, так і нових, Інтернет виступає провідником злочинності [3].

Кількість кіберзлочинів в Україні щороку зростає на кілька тисяч. Найпоширеніший вид злочину – шахрайство в мережі Інтернет. Кіберполіцейським вдалося виявити 2798 таких шахрайств, з яких у 2314 випадках були пред'явлені підозри про вчинення злочину. Найчастіше шахраї створюють сайти і продають неіснуючий товар, дуже багато злочинів, які стосуються виманювання інформації з карток та онлайн-кредитування [4]. Скарги пов'язані з шахрайством в Інтернеті, як на внутрішньому, так і на міжнародному рівні, з кожним роком постійно зростають [5]. Викрадають кошти з банківських карток, дані з комп'ютерів, інформацію з телефонів, запускають віруси-вимагачі, шантажують компанії та провертають криптоафери – це далеко не повний перелік злочинів, які вчиняють кібершахраї.

За статистичними даними більшість кіберзлочинів проти власності (79%) – це шахрайства, як правило вчиняються чоловіками (94%), і лише в рідкісних випадках жінками (6%). Як правило, такі злочини вчиняються особами, які офіційно не перебувають в шлюбі і не мають дітей. Кількість неодружених осіб із загального числа становить 70%, в той час, як одружених – 30%. Як показує судова практика, 51% осіб які вчинили кіберзлочини не мають постійного місця роботи, як правило такі особи і вчиняють шахрайства. Серед решти 49% більшу частину займають менеджери нижчої та середньої ланки, рідше зустрічаються посадові особи і програмісти. Так, якщо середній вік шахрая у матеріальному світі становить від 26–39 років, то середній вік кібершахрая варіюється від 18 до 35 років. Взагалі вік кібершахрая може варіювати від 18–45 років, а соціальне становище в суспільстві, від студента до співробітника державної установи або фірми. [6, с. 106].

Встановити особу злочинця у віртуальному світі надзвичайно складно, а в окремих випадках – практично не можливо. Оскільки злочинець особисто не контактує із своєю жертвою, а здійснює свої злочинні дії шляхом телефонних розмов, SMS та Інтернет листуванням. Щоб спіймати шахрая, необхідно думати, як шахрай, знати його психологічні особливості поведінки [7]. Це дає можливість зрозуміти методологію формування шахрайства з урахуванням основних його елементів – це мотив, можливість, раціональність. Психологічна характеристика інтернет-шахрая надасть можливість визначити основні соціально-психологічні риси притаманні суб'єктам злочинної діяльності в сфері вчинення інтернет-шахрайств, оптимізувати процес виявлення кола осіб, серед яких доцільно вести пошук злочинця, і точніше викрити конкретного правопорушника [8]. Виявлення психологічних даних про особу злочинця є одним із головних факторів не тільки в розслідуванні злочину, але

і в організації заходів протидії і профілактиці комп'ютерних злочинів[9]. Основними ознаками інтернет-шахрайства є високий ступінь латентності (що більшою мірою пояснюється ставленням жертв); багатоманітність способів вчинення шахрайства (зумовлено широким спектром послуг в мережі Інтернет); глобальний характер (інформаційний простір, на відміну від фізичного, не має чітких кордонів і обмежень), складнощі виявлення та запобігання [10].

Існує також певний набір особливостей особистості, які обумовлюють вибір конкретної злочинної діяльності, яку шахрай збирається здійснювати. А тому від виду інтернет-шахрайства яке вчиняє злочинець можливо визначити психологічні властивості особи та запропонувати психологічний портрет таким особам. Таким чином, при розслідуванні конкретних злочинів коло можливих суб'єктів можна істотно звузити.

«Професійні» звички і почерк злочинців виражаються у певних способах, методах, прийомах вчинення злочинів. Це свідчить про особливості його соціально-психологічного портрета: досвід, професія, вік, стать, знання і т.д. Профілювання злочинців та шахрайства є практичним інструментом для використання слідчими на постійній основі при розслідуванні шахрайств і вимагає об'єднання даних та інформації з різних джерел, включаючи особисті відомості про злочинця, інформацію про спосіб дії, мотив злочинця та можливість вчинити злочин [11].

Підсумовуючи вище сказане, можна надати *опосередкований типовий портрет особи яка вчиняє шахрайства в мережі Інтернет без врахування окремого виду інтернет-шахрайства*: це чоловік, який ніде не працює, або не має постійного місця роботи, віком від 20 до 35 років, офіційно не одружений, не має дітей, соціально благополучний, не притягався до кримінальної відповідальності, не конфліктний, не зловживає спиртним який позитивно характеризуються за місцем проживання, впевнений в собі, інтелектуально розвинутий, ввічливий, справляє позитивне враження на оточуючих, артистична, творча особа, якому притаманний егоцентризм, зневага до інтересів і думок окремих членів суспільства, відсутність жалю до жертви (через відчуття віртуальності), схильність до авантюризму, в більшості випадків постійний ризик є фізіологічно необхідним для особи шахрая, їм властива рішучість, знижена тривожність, при цьому притаманна терпимість, обережність, розвинута уява.

Доцільно було б розробити соціально-психологічні портрети (певний набір особливостей особистості) кіберзлочинців відповідно до відповідних видів Інтернет злочинів.

Формування банку типових моделей різних категорій злочинців дозволить оптимізувати процес виявлення кола осіб, серед яких найбільш вірогідний пошук злочинця [12]. Зібрані в процесі розслідування відомості про особу злочинця, про його кримінальну поведінку і злочинні дії, створюють фактичну базу для прийняття обґрунтованих правових рішень для його переслідування. Отже, створені комплекси для комп'ютерної та аналітичної розвідки якими оснащені оперативні та інформаційно-аналітичні підрозділи Націона-

льної поліції потребують вдосконалення шляхом створення багатоцільових інформаційних підсистем, інтеграції та систематизації інформаційних обліків на всіх рівнях, забезпечення їх повноти, оновлення, своєчасного наповнення, розширення, вірогідності та безпеки, продовжувати розроблення нових методів збирання і аналізу інформації. Слід підкреслити, що здатність до інформаційно-аналітичної роботи потрібна не лише працівникам інформаційно-аналітичних підрозділів, а й усім без винятку суб'єктам оперативно-розшукової діяльності, які виконують інформаційно-аналітичну роботу як спеціальну оперативно-розшукову функцію [13]

Використані джерела

1. Шорохова Г. М. Організаційно-правові аспекти використання сучасних інформаційних технологій у службовій діяльності територіальних органів поліції *Порівняльно-аналітичне право* № 3. 2017 С. 170–176
2. А. В. Мовчан, "Актуальні проблеми підготовки фахівців у галузі застосування сучасних інформаційних технологій", Науковий вісник Національної академії внутрішніх справ, № 1, 2012. . с. 40-46
3. Internet Fraud. (n.d.). The SAGE Encyclopedia of the Internet. doi:10.4135/9781473960367.n144
4. Олександр Гринчак. Що варто знати про кіберзлочинців в Україні URL : https://www.radiosvoboda.org/a/details/29031166.html
5. Computer and Internet Fraud: A Risk Identification Overview. (2003). Computer Fraud & Security, 2003(6), 6–9. doi:10.1016/s1361-3723(03)06008-1
6. Піцик Ю.М. Аналіз особистості кіберзлочинця який вчиняє злочини проти власності у кіберпросторі *Науковий вісник Міжнародного гуманітарного університету. Серія.: Юриспруденція.,* 2017 № 26., С. 105–107.
7. How to Act Like a Fraudster: To Catch a Fraudster, You Need to Think Like One. (2013). Detecting Fraud in Organizations, 155–183. doi:10.1002/9781118555972.ch4
8. Азжеурова Г. Г., Степанов Ю. В. Некоторые особенности личности «комп'ютерного преступника» Протидія злочинності у сфері інтелектуальної власності та комп'ютерних технологій органами внутрішніх справ: стан, проблеми та шляхи вирішення : матеріали
9. Голубєв В. О. Криминалистическая характеристика субъектов преступной деятельности в сфере использования компьютерных технологий URL :www.crime-research.org/
10. Чернявський С С. Інтернет шахрайство як об'єкт дослідження правових наук С. 100-103 (С. 100) Протидія злочинності у сфері інтелектуальної власності та комп'ютерних технологій органами внутрішніх справ: стан, проблеми та шляхи вирішення : матеріали всеукраїнської науково-практичної конференції, (м. Донецьк, 12 листопада 2010 р.) Донецький юрид. Ін-т ЛДУВС ім. Е.О. Дідоренка. – Донецьк: ДЮІ ЛДУВС, 2010.
11. Fraud Profiling Your Organization. (2015). Profiling the Fraudster, 197–204. doi:10.1002/9781118929773.ch20
12. Никифорчук В. Д. Характеристика особи кіберзлочинця *Правові реформи в Україні* Ч. 1, 2013 С. 181 С. 180–181. URL : http://elar.naiau.kiev.ua/bitstream/f
13. А. С. Овчинский, "Информация и оперативно-розыскная деятельность", М., ИНФРА-М, 97 с., 2002.

Бурак Н.Є. - доцент кафедри управління проектами, інформаційних технологій та телекомунікацій Львівського державного університету безпеки життєдіяльності, кандидат технічних наук.

МОДЕЛЬ ІНФОРМАЦІЙНОЇ АРХІТЕКТУРИ МОБІЛЬНОГО ДОДАТКУ ФІКСАЦІЇ ПОРУШЕНЬ ПРАВИЛ ДОРОЖНЬОГО РУХУ

У сучасному мирі розвитку та росту рівня урбанізації міст важливий фактор відіграє транспортна мобільність суспільства. Ця властивість забезпечується наявністю власних та громадських автотранспортних засобів. З кожним роком кількість таких засобів зростає, що сприяє виникненню ряду проблем, пов'язаних із дотриманням водіями правил дорожнього руху. Однією із таких проблем є порушення правил паркування автотранспорту. Інфраструктура міст не в змозі ефективно забезпечити комфортне використання автомобілів, якщо їх власники не дотримуватимуться встановлених норм та правил.

Аналіз стану існуючої системи паркування транспортних засобів у великих містах, зокрема у м. Львів [1], свідчить про не відповідність організаційних, нормативно-правових та фінансових умов функціонування системи паркування потребам міста та європейським стандартам, а також про не спроможність забезпечити належне функціонування механізму саморозвитку простору для паркування.

Здатність швидко опрацювати інформацію та оперативно прийняти міри щодо реагування на неї дають змогу забезпечити високий рівень безпеки та комфорту проживання громадян. Сьогодні, інформаційні технології інтегрувались практично у всі процеси діяльності, тому їх використання, особливо особистих засобів комунікації – смартфонів, у з метою удосконалення систем контролю дотримання правил дорожнього руху є перспективним напрямом розвитку ІТ-сфери та підвищення рівня залучення населення до покращення благоустрою та комфорту проживання та пересування містом.

Сьогодні існує проблема ігнорування фактів порушення працівниками відповідних структур. Патрулі поліції часто не помічають явні факти порушень через людський фактор чи неможливість перебувати усюди одночасно. Телефонні звернення громадян також часто просто «губляться» серед великої кількості повідомлень. Саме тому, при наявності величезної кількості порушень, покараними залишається тільки невелика частина порушників. Як результат – така поведінка входить в норму, що веде до неприємних наслідків.

На допомогу поліції, приходять сучасні інформаційні технології, зокрема розробки мобільних та веб-додатків для громадян, які можуть своєчасно повідомити про скоєне правопорушення, а працівники Національної поліції – швидко відреагувати на його ліквідацію чи затримання порушника.

На Рис. 1 зображено інфраструктурну схему розроблювального додатку

для платформи Android "Good Parking". Даний додаток реалізуватиме політику взаємодії суспільства та правоохоронних органів у плані фіксації порушень правил дорожнього руху, зокрема паркування [2].

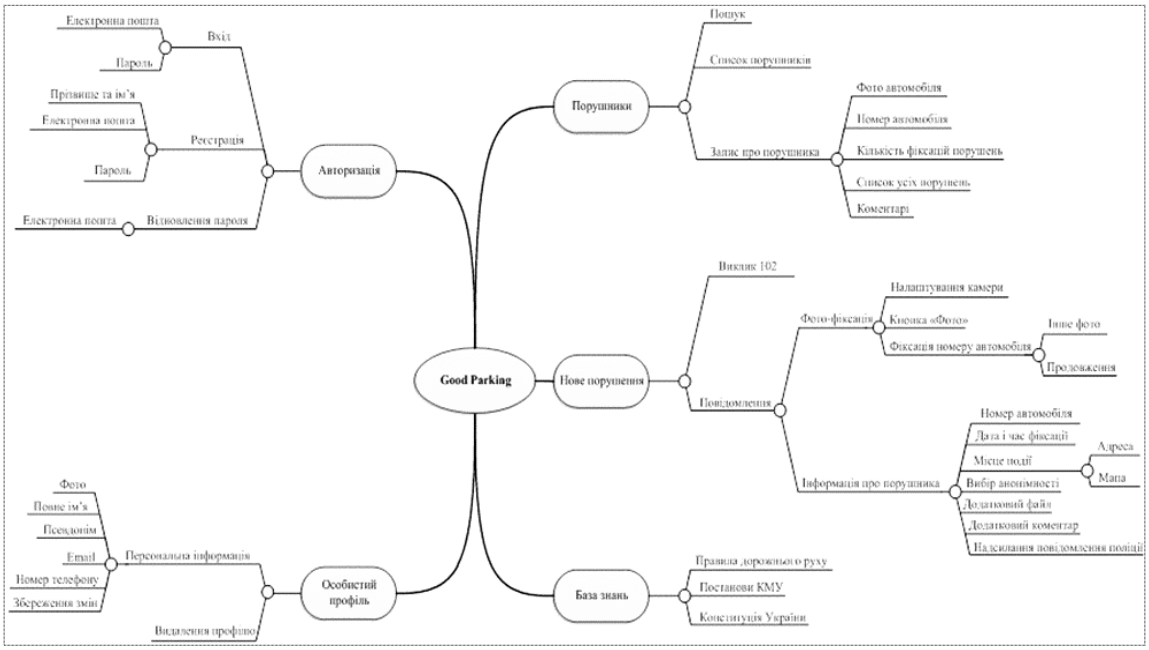


Рис. 1. Інформаційно-архітектурна модель мобільного додатку "Good Parking"

Даний додаток матиме змогу фіксувати порушення, оформити інформацію про нього, приєднати геолокаційні дані для швидкого визначення місця, розпізнати номерні знаки, ввести історію правопорушень автовласниками, а також повідомити підрозділи Національної поліції про виявлений факт.

У якості методу розпізнавання номерних знаків використовується Google Cloud Vision [3], оскільки він оснований на сучасному алгоритмі розпізнавання текстів Tesseract. Для визначення позиції координат місця скоєного порушення застосовано сервіс географічних карт Google Maps

Вирішення проблеми притягнення до відповідальності правопорушників можливе шляхом використання сучасних інформаційних систем побудованих на основі поєднання засобів комунікації, смартфонів, планшетних ПК тощо у якості фото-, відеодоказів. Результатом функціонування таких систем буде налагоджений канал комунікації між громадянами та службою патрульної поліції, що дасть змогу оперативно повідомляти про порушення правил паркування, а найближчий до місця події патруль швидко зреагувати на звернення.

Використані джерела:

1. Юлія Сабадишина: Як налагодити систему паркування у Львові: 20 пропозицій. [Електронний ресурс]. – Режим доступу: http://tvoemisto.tv/news/yak_nalagodyty_systemu_parkuvannya_u_lvovi_20_propozytsiy_75787.html (2016).
2. Бурак Н.Є. Управління інтеграцією мобільного додатку фотофіксації правопору-

шень в інформаційну систему Національної поліції / Н. Є. Бурак, Н. Р. Ханас // Управління проектами, програмами, портфелями : Тези доповідей ІІІ Міжнародної науково-практичної конференції : [у 2т.]. – Одеса, 2018. – Том 2. – С. 22–24.
3. Google Cloud Platform (Vision) – Powerful Image Analysis. [Електронний ресурс]. – Режим доступу: https://cloud.google.com/vision/.

Буткова О. Я. - аспірант кафедри державно-правових дисциплін Луганського державного університету внутрішніх страв
ім. Е. О. Дідоренка

ГРОМАДСЬКА ЕКСПЕРТИЗА ЯК ДЖЕРЕЛО ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ОРГАНІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

Громадські експертизи відіграють важливу роль в інформаційному забезпеченні органів Національної поліції та сприяє відкритості та прозорості у діяльності органів державної влади у рамках утвердження демократії участі [6]. Під інформаційно-аналітичним забезпеченням розуміється комплекс заходів щодо збирання, отримання, зберігання, користування, обробки та накопичення інформації з подальшим її аналізом з метою прогнозування або підведення підсумків діяльності і корегування в залежності від цього подальших управлінських рішень [9; с. 204].

Повноваження поліції у сфері інформаційно-аналітичного забезпечення передбачені ст. 25 Закону України “Про Національну поліцію”, що включають, зокрема, формування бази (банки) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України; користування базами (банками) даних Міністерства внутрішніх справ України та інших органів державної влади; здійснення інформаційно-пошукової та інформаційно-аналітичної роботу; здійснення інформаційної взаємодії з іншими органами державної влади України, органами правопорядку іноземних держав та міжнародними організаціями [4].

Поліція наповнює та підтримує в актуальному стані бази (банки) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України, зокрема, стосовно: виявлених кримінальних та адміністративних правопорушень, осіб, які їх учинили; осіб, які скоїли адміністративні правопорушення, провадження у справах за якими здійснюється поліцією; зареєстрованих кримінальних та адміністративних корупційних правопорушень, осіб, які їх учинили, та результатів розгляду цих правопорушень у судах тощо.

Об’єктом інформаційного забезпечення органів Національної поліції є інформація, необхідна поліції для виконання покладених на неї завдань, отримана з різних джерел. Згідно ст. 1 Закону України «Про інформацію» інформація - будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [3]. Одним із джерел

інформаційного забезпечення поліції є громадська експертиза діяльності органів виконавчої влади, яка також слугує одним з засобів щодо протидії корупції у діяльності Національної поліції [7].

Відповідно до Порядку сприяння проведенню громадської експертизи діяльності органів виконавчої влади затвердженого Постановою Кабінету Міністрів України від 5 листопада 2008 р. N 976 (далі – Порядок № 976) громадська експертиза діяльності органів виконавчої влади є складовою механізму демократичного управління державою, який передбачає проведення інститутами громадянського суспільства, громадськими радами оцінки діяльності органів виконавчої влади, ефективності прийняття і виконання такими органами рішень, підготовку пропозицій щодо розв'язання суспільно значущих проблем для їх врахування органами виконавчої влади у своїй роботі [5]. У наукові літературі громадська експертиза діяльності органів публічної влади визначається як «здійснення громадськістю комплексного дослідження у формі аналізу, оцінки та прогнозування результатів діяльності чи бездіяльності органів публічної влади, ефективності прийняття та виконання ними рішень з метою підготовки обґрунтованого експертного висновку з конкретними пропозиціями щодо вирішення суспільно важливих проблем для їх подальшого врахування органами публічної влади у своїй роботі» [8].

Складовими громадської експертизи є: аналіз ходу і результатів програми, заходів, втілення того чи іншого нормативно-правового акту, рішення органу влади, а також причин відхилення від запланованого. оцінювання ефективності прийняття та виконання органом виконавчої влади рішень, підготовка пропозицій щодо розв’язання суспільно значущих проблем для їх врахування органами виконавчої влади у своїй роботі [2; с. 29].

Предметом громадської експертизи діяльності органу виконавчої влади можуть бути: проекти актів органів виконавчої влади та їх посадових осіб з питань, що стосуються дотримання прав, свобод і законних інтересів людини і громадянина; стан виконання відповідним органом виконавчої влади та їх посадовими особами законодавства України; стан виконання органами виконавчої влади та їх посадовими особами державних та місцевих програм, що фінансуються за рахунок бюджетних коштів; діяльність посадових осіб органів виконавчої влади щодо виконання ними своїх посадових обов'язків; інша діяльність органів виконавчої влади та їх посадових осіб, пов'язана з виконанням функцій держави [1; с. 13-14]. За результатами громадської експертизи ініціатор зазначеної експертизи готує експертні висновки.

При досліджені предмету громадської експертизи може бути виявлено ряд порушень, які можуть слугувати підставою для відкриття адміністративного чи кримінального провадження правоохоронними органами. Тим самим, експертні висновки можуть слугувати джерелом отримання інформації органами Національної поліції.

Згідно з положеннями Порядку № 976 орган виконавчої влади після надходження експертних пропозицій надсилає в письмовій та електронній формі Секретаріату Кабінету Міністрів України для розміщення на урядово-

му веб-сайті у рубриці "Громадянське суспільство і влада": інформацію про найменування, прізвище, ім'я, по батькові керівника, поштову адресу, контактні дані ініціатора громадської експертизи, предмет та строки її проведення; експертні пропозиції, подані ініціатором громадської експертизи; затверджені органом виконавчої влади заходи для реалізації експертних пропозицій; відповідь органу виконавчої влади ініціатору громадської експертизи про результати розгляду експертних пропозицій та заходи для їх реалізації [5].

Таким чином, громадські експертизи є важливою передумовою щодо покращення інформаційного забезпечення органів Національної поліції України. На веб-сайті Кабінету Міністрів України розміщується інформація стосовно проведених громадських експертиз, яка слугують своєрідною базою даних та може виступати джерелом інформаційного забезпечення органів Національної поліції України.

Використані джерела:

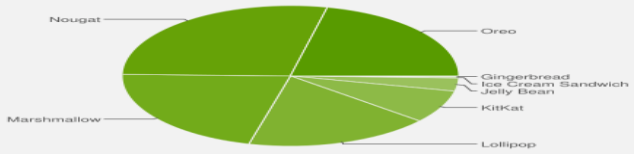
1. Громадська експертиза діяльності органів виконавчої влади: крок за кроком / М. Лациба, О. Хмара, О. Орловський ; Укр. незалеж. центр політ. дослідж. К. : [Агентство “Україна”], 2010. 96 с.
2. Громадська експертиза та громадський моніторинг діяльності органів влади : навч. пос. / Купрій В., Паливода Л. К. : Макрос, 2011. 200 с.
3. Закон України «Про інформацію» від 02 жовтня 1992 р. URL: https://zakon.rada.gov.ua/laws/show/2657-12/print.
4. Закон України «Про Національну поліцію» від 02 липня 2015 р. URL: https://zakon.rada.gov.ua/laws/show/580-19.
5. Порядок сприяння проведенню громадської експертизи діяльності органів виконавчої влади затвердженого Постановою Кабінету Міністрів України від 5 листопада 2008 р. N 976. URL: https://zakon.rada.gov.ua/laws/show/976-2008-%D0%BF.
6. Нестерович В.Ф. Принципи відкритості та прозорості у діяльності органів державної влади як важлива передумова для утвердження демократії участі. *Філософські та методологічні проблеми права*. 2016. № 4. С. 67-78.
7. Нестерович В.Ф. Конституційно-правові види громадської експертизи в Україні. *Експерт: Парадигми юридичних наук і державного управління*. 2018. № 2. С. 67-76.
8. Нестерович В.Ф. Роль громадськості у формуванні та реалізації державної антикорупційної політики в Україні. *Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка*. 2016. № 3. С. 5-13.
9. Управління органами Національної поліції України : підручник / за заг. ред. д-ра юрид. наук, доц. В. В. Сокуренка; [О. М. Бандурка, О. І. Безпалова, О.В. Джафарова та ін. ; передм. В. В. Сокуренка] ; МВС України, Харків. нац. ун-т внутр. справ. Харків: Стильна типографія, 2017. 580 с.

Гавриш О.С. – старший викладач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ

ОСОБЛИВОСТІ БЕЗПЕЧНОГО ВИКОРИСТАННЯ СУЧАСНИХ СМАРТФОНІВ

Як відомо, операційні системи розробляються людьми. У мобільній платформі Google на сьогоднішній день виявлено безліч помилок, деякі з цих помилок являють собою повноцінні уразливості і можуть використовуватися як для несанкціонованого доступу до файлової системи смартфона, так і для поширення шкідливого ПЗ [1].

Version	Codename	API	Distribution
2.3.3 - 2.3.7	Gingerbread	10	0.2%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	0.3%
4.1.x	Jelly Bean	16	1.1%
4.2.x		17	1.5%
4.3		18	0.4%
4.4	KitKat	19	7.6%
5.0	Lollipop	21	3.5%
5.1		22	14.4%
6.0	Marshmallow	23	21.3%
7.0	Nougat	24	18.1%
7.1		25	10.1%
8.0	Oreo	26	14.0%
8.1		27	7.5%



Якщо вірити офіційній статистиці Google, на сьогоднішній день серед версій Android найбільш поширена Nougat - редакція мобільної платформи за номером 7.0 і 7.1 встановлена в сукупності на 28,2% пристроїв. Другу позицію впевнено займає Android 8.0 і 8.1 Oreo з показником 21,5%. На третьому місці закріпилася шоста версія Marshmallow - вона працює на 21,3% девайсів. Android 5.0 і 5.1 Lollipop встановлені сумарно на 17,9% пристроїв, а замикає групу лідерів Android 4.4 KitKat з показником 7,6% користувачів.

Згідно з інформацією з сайту cvedetails.com [2], на сьогоднішній день в Android налічується 2146 вразливостей, при цьому число виявлених багів початок експоненціально зростати приблизно з 2014 року.

Не так просто оцінити, скільки з перерахованих пристроїв вчасно отримали оновлення безпеки, які виправили вразливості, але це явно далеко не всі з них. Мало того: не всі вразливості взагалі виявляються закритими, тим більше в старих версіях, офіційна підтримка яких припинена. Проблему посилюють виробники пристроїв, які часто не поспішають випускати оновлення.

Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2009	5	3								1					
2010	1	1	1												
2011	9	1	1		1					3	2	3			
2012	8	5	4	2							1				1
2013	7	1	2	2	2					1	1	3			
2014	13	2	4	1		1				1	2	2			1
2015	125	56	70	63	46					20	19	17			
2016	525	106	73	92	38					48	99	250			
2017	842	87	206	162	32			1		31	115	36			
2018	611	32	84	150	12	3	1	1		17	64	3			
Total	2146	294	445	472	131	4	1	2		122	303	314			2
% Of All		13.7	20.7	22.0	6.1	0.2	0.0	0.1	0.0	5.7	14.1	14.6	0.0	0.0	

Найперша вразливість Android.

Найперша вразливість Android була виявлена ще в жовтні 2008 року в прошивці комунікатора HTC T-Mobile G1. Під час перегляду веб-сторінок з певним вмістом помилка в ПО дозволяла виконати шкідливий код, що відслідковує використання клавіатури гаджета. Теоретично таким чином можна було реалізувати кейлоггер, який фіксує натискання кнопок, і збирати інформацію, що вводиться користувачем при веб-серфінгу інформацію. Ця вразливість була небезпечною тільки для однієї-єдиної моделі комунікатора, але саме її наявність наочно показало: Android - не так безпечна і захищена система, як вважалося раніше.

З ростом популярності операційної системи ентузіасти і дослідники відшукували всі нові і нові помилки в різних її версіях. Безумовно, в рамках однієї статті ми не зможемо охопити всі дві тисячі з гаком вразливостей, виявлених за весь час існування Android. Тому зосередимося тільки на найцікавіших і небезпечних з них, причому - тільки в актуальних на даний момент версіях Android (тих, що зараз ще можуть зустрітися в житті).

Самим «ненадійним» виявилося четверте покоління Android, починаючи з версії 4.4 KitKat. З нього, мабуть, і почнемо наш огляд вразливостей, виявлених в різний час в цій платформі.

BlueBorne CVE: CVE-2017-1000251, CVE-2017-1000250, CVE-2017-0781, CVE-2017-0782, CVE-2017-0785 і CVE-2017-0783.

Уразливі версії Android: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0

Для експлуатації потрібно: атакуючий повинен знаходитися на відстані не більше десяти метрів від уразливого пристрою, а на уразливому пристрої потрібно включити Bluetooth.

Можливий результат: виконання довільного коду з привілеями ядра системи, витік даних. Це не окрема вразливість, а цілий набір помилок в стеці Bluetooth сучасних операційних систем, серед яких значиться і Android. Сер-

йозні помилки містяться в коді системної функції l2cap_parse_conf_rsp ядра Linux, причому їх можна виявити у всіх версіях ядра, починаючи з 3.3. Якщо в системі включена захист від переповнення стека CONFIG_CC_STACKPROTECTOR, їх використання призводить до виникнення критичної помилки в роботі ядра.

Уразливість CVE-2017-1000251 виявлена в модулі ядра під назвою L2CAP, який відповідає за роботу стека протоколу Bluetooth. Ще одна уразливість в стеці цього протоколу отримала позначення CVE-2017-0783. Якщо на атакуємому смартфоні включена підсистема Bluetooth, з її допомогою можна віддалено передати на нього спеціальним чином сформовані пакети інформації. Такі пакети можуть містити шкідливий код, який виконається в Android з привілеями ядра системи. При цьому для реалізації атаки не буде потрібно попередньо сполучати пристрої або включати на них режим виявлення. Досить, щоб атакуючий знаходився на відстані не більше десяти метрів від уразливого пристрою.

Оскільки взаємодіють з протоколом Bluetooth компоненти ОС за замовчуванням мають високі системні привілеї, експлуатація цих вразливостей теоретично дозволяє отримати повний контроль над атакуємим смартфоном і планшетом, включаючи доступ до Вашого пристрою, підключенням мереж і файлової системи. Також за допомогою BlueBorne технічно можна реалізовувати атаки типу man-in-the-middle.

До BlueBorne також відносять вразливість CVE-2017-1000250 в стеці BlueZ Linux протоколу Service Discovery Protocol (SDP). Експлуатація уразливості CVE-2017-1000250 може привести до витоку даних. Вразливості CVE-2017-0781, CVE-2017-0782 і CVE-2017-0785 відносяться до самої ОС Android, при цьому за допомогою перших двох шкідливий додаток може отримати в системі привілеї ядра, а остання дозволяє реалізувати витік даних.

Для усунення вразливостей BlueBorne 9 вересня 2017 року компанія Google випустила оновлення безпеки.

Використані джерела:

1. Самые опасные уязвимости старых версий Android. [Електронний ресурс]. - Режим доступу: https://xakep.ru/2019/02/07/forgotten-android/
2. Vulnerability in the kernel code of the Android operating. [Електронний ресурс]. - Режим доступу: systemhttps://www.cvedetails.com/

Гребенюк А.М. – доцент кафедри, кандидат технічних наук, доцент;
Рибальченко Л.В. – доцент кафедри, кандидат економічних наук, доцент (кафедра економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ)

ВИКОРИСТАННЯ БЕЗПІЛОТНИКІВ ДЛЯ ПОТРЕБ ПОЛІЦІЇ

В теперішній час дуже активно стали використовувати безпілотні літальні апарати (БПЛА, рідше БЛА; Безпілотники, дрони, квадрокоптери - цими термінами називають невеликі літальні апарати, керовані людиною із землі). Безпілотники вже використовуються для картографічної зйомки, телетрансляцій, кінозйомки, реклами, метеорологічних спостережень, вантажоперевезень, моніторингу безпеки на об'єктах і в місті та для спостережень за протяжними об'єктами (залізницями або лініями електропередач).

Поліція і рятувальники все частіше замислюються про використання безпілотників в повсякденній практиці. А десь вже пройшли перші впровадження і накопичений досвід в різних ситуаціях, що вимагають уваги силових структур або рятувальників. Зокрема, в Лондоні мають намір переслідувати злочинців за допомогою БЛА - це дешевше і безпечніше для поліції і оточуючих, ніж при використанні мотоциклів і гелікоптерів.

За кордоном поліцейські безпілотники часто виконують неординарні завдання. Наприклад, в Японії поліцейські протестували безпілотник, який буде боротися проти безпілотників-порушників. Завдання поліцейського квадрокоптера - накинути спеціальну сітку на "літаючого порушника", який залетів на об'єкт, що охороняється. У країнах ЄС поліцейські теж постійно експериментують з безпілотниками: обладнують їх пристроями для розпилення сльозогінного газу або влаштовують навчальну погоню за злочинцем в міських умовах. Що стосується переслідування підозрюваних, то поліцейські за кордоном прийшли до висновків, що використання безпілотника набагато вигідніше гелікоптера. А насамперед, важливим є те, що безпілотник часто непомітний для правопорушника.

До сих пір в Україні, на жаль, найширша сфера застосування БПЛА - це військові операції. Використання безпілотника обходиться в кілька десятків разів дешевше, ніж утримання військового винищувача, а небезпека для життя військових пілотів і військових операторів БПЛА не можна порівняти.

Українська поліція опановує сучасні методи боротьби зі злочинністю. У 2017 році створено підрозділ аеророзвідки поліції, який допомагає не тільки виявляти факти злочинів, а і затримувати зловмисників.

Так, на сьогоднішній день, органом управління безпілотної авіації Національної поліції - Управління організації діяльності підрозділів поліції на

воді та повітряної підтримки Національної поліції, розроблено та затверджено навчальну програму безпілотних авіаційних комплексів І класу за базовим кваліфікаційним рівнем І. Також складено відповідний навчально-тематичний план. Навчання поліцейських проходить на базі Державної установи «Львівський спеціалізований центр підготовки поліцейських» [1, 2].

Застосування безпілотних літальних апаратів, оснащених оптичними, масштабуючими або телевізійними камерами, дозволяє правоохоронним органам бути більш ефективними. Технологія безпілотників і камер дозволяє керівникам підрозділів мати більше інформації та своєчасно реагувати на зміну оперативної ситуації. Повітряні спостережні пункти також дозволяють більш повно оцінити і реконструювати місця після аварії або місця злочину, щоб допомогти зрозуміти графік подій для кожного інциденту. У випадках з озброєними бандитами або в ситуаціях із заручниками, безпілотник може спостерігати загрози із безпечного місця, дозволяючи правоохоронним органам на місці діяти з більшою безпекою, надає правоохоронним органам інструменти, необхідні для належного реагування на надзвичайні ситуації, коли ситуаційна обізнаність є ключовою.

Оскільки технологія ще тільки розвивається, з'являється можливість закріплювати на безпілотниках різні датчики і аналізатор, які можуть аналізувати можливі вибухові пристрої або визначити, чи є хмара небезпечною для зони дії підрозділів поліції.

Таким чином, використання безпілотників істотно змінить діяльність підрозділів поліції щодо забезпечення охорони громадського порядку та підвищення безпеки життєдіяльності населення, надасть можливість здійснювати своєчасний та якісний моніторинг оперативності виконання складних завдань, розширить спектр реагування на різні інциденти за дуже короткий час.

Використані джерела:

1. Наказ МВС України від 18.12.2018 № 1026 "Про затвердження Інструкції із застосування органами та підрозділами поліції технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, засобів фото- і кінозйомки, відеозапису". 2018р. [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/z0028-19
2. Нацполіція розпочинає підготовку операторів безпілотників [Електронний ресурс]. – Режим доступу : https://mvs.gov.ua/ua/news/24071 Nacpoliciya_rozpochina_pidgotovku_operatoriv_bezpilotnikiv.htm

Гринченко Є.М. - старший науковий співробітник; доцент;
Демидов З.Г. - старший науковий співробітник;
Колмик О.О. - науковий співробітник (лабораторія з проблем розвитку інформаційних технологій Харківського національного університету внутрішніх справ)

ПРОБЛЕМА НЕСТАЧІ ПРАКТИЧНИХ НАВИЧОК РОБОТИ З ЄРДР

У листопаді 2019 року в закладах вищої освіти системи МВС таких міст, як: Харків, Київ, Дніпро, Донецьк, Львів, Луганськ та Одеса, почалося впровадження в навчальний процес програмного продукту «Навчальний ЄРДР (Єдиний реєстр досудових розслідувань)». Він представляє собою WEB орієнтований програмний продукт, який зовнішньо імітує інтерфейс ЄРДР, та надає можливість курсантам набути практичних навичок роботи з ним. Програмний продукт було створено на замовлення керівництва ХНУВС співробітниками науково-дослідної лабораторії з проблем розвитку інформаційних технологій. Навчальний ЄРДР спочатку створювався для навчання курсантів і студентів ХНУВС, але проблема нестачі практичних навичок роботи з базовою програмою існує у всіх закладах вищої освіти системи МВС. Тому в ХНУВС відбулася робоча зустріч представників закладів вищої освіти системи Міністерства внутрішніх справ з обговорення питання щодо поширення програмного продукту «Навчальний ЄРДР».

У програмі створені кілька ролей: адміністратор, викладач і курсант. Це аналоги слідчого, керівника органу досудового розслідування та адміністратора у реальному ЄРДР. На робочій зустрічі презентували безпосередньо роботу з програмою в ролях курсанта (слідчого) і викладача (керівника органу досудового розслідування).

Роль слідчого дозволяє створювати кримінальні правопорушення і відправляти їх на перевірку – підтвердження керівнику органу досудового розслідування. Після підтвердження роль слідчого повністю імітує таку в реальному ЄРДР. Вона дозволяє здійснювати повний цикл кримінально-процесуальних дій:

- створення кримінального правопорушення;
- підтвердження і реєстрація створеного правопорушення керівником органу досудового розслідування;
- подальша робота зі створеним на основі кримінального правопорушення кримінальним провадженням;
- прийняття у провадження;
- зупинка провадження;
- відкриття матеріалів;

• закриття провадження.

У процесі провадження курсант (слідчий) має можливість додавати до провадження потерпілих, правопорушників, додавати і редагувати надані збитки та наслідки вчинення правопорушення.

При роботі з правопорушниками курсант (слідчий) також має змогу проводити повний цикл кримінально-процесуальних дій, а саме: повідомлення про підозру та зміна підозри. В ході повідомлення про підозру правопорушнику курсант (слідчий) має можливість обрати відносно нього один з декількох запобіжних заходів, який може бути призначений, продовжений в разі необхідності, або скасований в залежності від ходу кримінального провадження.

Також слідчий має можливість додавати до провадження відповідні документи, такі як заяви, рапорти, протоколи, постанови і повідомлення. Всі типи вище перелічених документів додаються до провадження за допомогою їх завантаження на сервер.

Всі перераховані вище дії, вчинені з кримінальним провадженням, а саме: реєстрація самого провадження, додавання до нього потерпілих і правопорушників, обрання щодо правопорушників запобіжного заходу, а також його продовження або скасування, додавання супутніх документів і т.д. будуть відображені та зафіксовані в русі провадження.

Роль викладача (керівника органу досудового розслідування) багато в чому повторює можливості такої для курсанта (слідчого). Однією з принципових відмінностей є можливість реєстрації кримінального провадження, якої у курсанта (слідчого) не має. Саме викладач (керівник органу досудового розслідування) вирішує чи коректно заповнена форма кримінального правопорушення та приймає рішення про її реєстрацію в системі ЄРДР з подальшим створенням кримінального провадження.

Крім того, в навчальній системі ЄРДР на викладача (керівника органу досудового розслідування) покладено завдання реєстрації в системі нових користувачів з роллю курсанта (слідчого), яких система автоматично прив'язує до нього і для яких він є керівником органу досудового розслідування. Також обов’язком викладача (керівника органу досудового розслідування) є видача для зареєстрованих ним курсантів (слідчих) ключів доступу. Також він має можливість редагування та видалення профілів курсантів (слідчих). Для зручності роботи навчальної системи ЄРДР реалізовано принцип, який полягає в тому, що при видаленні профілю курсанта (слідчого) автоматично видаляються усі створені ним правопорушення і провадження.

Адміністратор має найширші можливості в системі. Крім всіх можливостей, які є у курсанта (слідчого) та викладача (керівника органу досудового розслідування), саме адміністратор реєструє в навчальній системі викладачів (керівників органів досудового розслідування) та видає їм ключі доступу. Ключі доступу є аналогом електронно-цифрового підпису в ЄРДР.

Таким чином, програма «Навчальний ЄРДР» дає можливість отримати практичний досвід з роботою ЄРДР і знижує витрати часу на навчання безпосередньо на робочому місці в правоохоронних органах.

Каблуков А. О. - доцент кафедри медичної і фармацевтичної інформатики та новітніх технологій, кандидат технічних наук, доцент;
Страхова О.П. - асистент кафедри медичної і фармацевтичної інформатики та новітніх технологій (Запорізький державний медичний університет)

МОДЕЛЮВАННЯ СЕРЕДОВИЩА ДИСТАНЦІЙНОГО НАВЧАННЯ СПІВПРАЦІВНИКІВ МВС З УРАХУВАННЯМ ЇХ ПОТОЧНОГО ФУНКЦІОНАЛЬНОГО СТАНУ.

Дистанційне навчання являє собою підхід, який має максимально враховувати індивідуальні здібності і потреби особи що навчається [1]. Створюються комп'ютеризовані середовища, які дозволяють реалізувати ідеї дистанційного навчання на практиці. Вони надають можливість адаптувати не лише рівень складності, а й траєкторії вивчення матеріалів. Залежно від ступеня і швидкості засвоєння попереднього матеріалу, на основі обраних варіантів відповіді та / або вибору, сучасні комп'ютеризовані системи дистанційного навчання цікаві тим, що за їх допомогою один і той же матеріал може бути викладений різними способами і засобами.

Для повноти охоплення всіх факторів, принципів, умов здійснення дистанційного навчання, його зручно розглядати як багатокомпонентну систему. Отже, потрібно створити його модель, і розглянути її дієвість. Модель процесу навчання в умовах комп'ютеризованого середовища включає в себе дві змістові частини: модель предметної області і модель співпрацівника МВС-студента. Процес моделювання починається з вибору найбільш репрезентативних моментів на основі аналізу інтелектуальних потреб осіб що навчаються.

Найбільш успішні і широко відомі системи дистанційного навчання використовують моделі студента, які охоплюють всю інформацію про нього: прогрес у вивченні предметної області, рівень засвоєння, поведінку і т.ін. [2]. Модель студента передбачає, що інформація про студента змінюється з часом, включаючи нові елементи і траєкторію вивчення курсу відповідно до етапу проходження курсу студентом. Тобто містить не тільки загальну інформацію про студента, але відстежує всі дії в процесі дистанційного навчання в рамках електронної освітньої системи.

Однак, дистанційні навчальні системи що розвиваються нині не враховують один з основних ознак студента, як найважливішого елемента: його поточний функціональний стан. Втім, від поточного функціонального стану студента залежить його увага, здатність сприймати, запам'ятовувати і засвоювати інформацію, що надається, орієнтування в інформаційних потоках; виживаність знань студента, що виникають як результат його пізнавальної діяльності.

Пропонована нами модель дистанційного навчання включає елемент ви-

значення поточного функціонального стану студента, як елемента знань про нього, як самостійну складову системи навчання, поряд з його успішністю та інтелектуальними здібностями.

Контролююча система, заснована на зміні електрошкірних характеристик певних мікрозон на тілі людини під впливом навантаження [3]. Вона являє собою гаджет, що фіксується або на вусі, або на зап'ястку студента. Як і всі елементи системи дистанційного навчання, вона попередньо налаштовується під можливості, здібності і стан кожної особи що навчається. Дані про поточний функціональний стан студента дозволяють визначити виникнення, наростання відхилень в його стані, і повідомити про необхідність йому змінити рід діяльності, відпочити, зайнятися відновлюваною гімнастикою, тощо [4].

Таким чином, модель системи дистанційного навчання що побудована з урахуванням поточного функціонального стану студента охоплює, контролює і враховує всі основні чинники її успішної роботи.

Використані джерела:

1. Краснов В. В. Розробка системи інформаційного відображення процесів передачі знань в післядипломній медичній освіті : дис. ... д-ра мед. наук : 14.03.11 / Нац. мед. акад. післядиплом. освіти ім. П.Л. Шупика. Київ, 2011.
2. Кальниш В. В., Пишнов Г. Ю. Єдність змін функціонального стану організму працюючого при розвитку втоми. *Укр. журн. з проблем медицини праці.* 2012. № 1. С. 55-66.
3. Woo E. H., White P., Lai C. W. Musculoskeletal impact of the use of various types of electronic devices on university students in Hong Kong: An evaluation by means of self-reported questionnaire. Man Ther. 2016. Vol. 26. P. 47-53. doi: 10.1016/j.math.2016.07.004.
4. Евтихов О. В. Типы образовательных сред в современном образовании. Совр. исследования социальных проблем. 2014. № 4 (36). С. 34-43.

Клімушин П.С. - доцент кафедри інформаційних технологій та кібербезпеки Харківського національного університету внутрішніх справ**,** кандидат технічних наук, доцент; **Бєляєва Є. Г.** - курсант 4 курсу факультету № 4 Харківського національного університету внутрішніх справ.

ПРАКТИЧНІ РЕКОМЕНДАЦІЇ ЩОДО ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ГРОМАДЯНИ В МЕРЕЖІ ІНТЕРНЕТ

З появою інтернет-магазинів, соціальних мереж, додатків для смартфонів, питання про захист персональних даних стало одним з найбільш обговорюваних. Практично будь-який ресурс запитує наше ім'я, телефон або навіть адресу проживання, і тільки від того, як будуть використовувати персональні дані, залежить чи будете особа піддана можливості їх незаконного використання. В наш час захист таких даних є дуже актуальним.

Що ж можна віднести до персональних даних? До персональних даних можна віднести будь-які відомості, за якими ідентифікується або може бути ідентифікована фізична особа, зокрема: прізвище, ім’я, по батькові, адреса, телефони, паспортні дані, національність, освіта, сімейний стан, релігійні та світоглядні переконання, стан здоров’я, матеріальний стан, дата і місце народження, місце проживання та перебування тощо, дані про особисті майнові та немайнові відносини цієї особи з іншими особами, зокрема членами сім’ї, а також відомості про події та явища, що відбувалися або відбуваються у побутовому, інтимному, товариському, професійному, діловому та інших сферах життя особи (за винятком даних стосовно виконання повноважень особою, яка займає посаду, пов’язану із здійсненням функцій держави або органу місцевого самоврядування) тощо. Вказаний перелік не є вичерпним.

Суб'єкти, щодо яких здійснюється обробка персональних даних: громадяни; наймані працівники; посадові особи; платники податків і зборів; клієнти; покупці; споживачі; абоненти; пацієнти; пасажири, батьки; суб'єкти відносин у сфері страхування; суб'єкти фінансових відносин; суб'єкти відносин у сфері реклами (рекламодавці, рекламо-розробники, розповсюджувачі, споживачі); члени політичних партій / громадських / релігійних організацій; вихованці закладів освіти (учні, студенти, абітурієнти, курсанти, слухачі, стажисти, аспіранти, докторанти, випускники та ін.); інші фізичні особи, які надають власні персональні дані при реалізації своїх прав або обов'язків.

Які причини витоку персональних даних? За даними аналітичного дослідження, яке провела компанія Trend Micro, спираючись на інформацію з бази витоків даних Privacy Rights Clearinghouse, фахівці компанії були отримані наступні результати [1]:

1. 41% всіх витоків інформації викликані тим, що співробітник організації самостійно втратив робочий ноутбук, флешку, телефон або планшет, або пристрій вкрали;
2. зломи стали причиною лише 25% інцидентів за останні 10 років (2005-2015 рр.);
3. 17,4% склало ненавмисне розкриття інформації;
4. 12% витоків відповідальні інсайдери, які навмисно продавали інформацію;
5. 1,4% через шахрайство з платіжними картами.

Тобто, проаналізувавши дану статистику можна зробити висновок, що витік чи втрата персональних даних відбувається найчастіше, через необережність або не припущення імовірних наслідків особою, яка втрачає або розголошує свої персональні дані.

Крім поліції та інших державних органів доступ до персональних даних має величезна кількість людей: співробітники банку, співробітники пошти, співробітники компанії-оператора, співробітники страхової компанії, співробітники приватної клініки, працівники відділу кадрів на місці працевлаштування, персонал готелів, який реєструє проживання.

Досконале знання імені, прізвища, місця проживання, дати народження

та інших подібних відомостей допоможе зловмисникові видавати себе в Інтернеті за іншу особу. І чим більше такої інформації про захоплення, хобі та особисте життя є у шахрая, тим точніше буде схожість. А паспортні дані можуть і зовсім можуть допомогти зловмисникові взяти на чуже ім'я кредит або отримати доступ до банківських вкладів.

Рекомендації щодо захисту персональних даних:

1. При реєстрації в онлайн-магазині (а також в інших мережах), не обов'язково ділитися своїми реальними даними: ім'ям і прізвищем та ін..
2. Не публікуйте фотографії, з якої зловмисники зможуть отримати додаткову інформацію, яка їм буде корисна (про вас, ваше житло, плани на відпустку, квитки на літак або інші квитки зі штрих-кодом).
3. Намагайтеся не тримати у відкритому доступі (наприклад, в хмарному сховищі) скан-копії і ксерокопії особистих документів.
4. Встановіть пароль або інший спосіб ідентифікації на своєму смартфоні, ноутбуці (бажано на флеш-носії також).
5. Будьте уважні, не губіть носії інформації, такі як флеш-карти, мобільні телефони та ноутбуки.
6. Не залишайте папірці з паролями доступу біль свого робочого місця, бажано зробіть їх якомога складнішими, для попередження незаконного доступу до вашої системи.

Використані джерела:

1. Нефедова Марія. Скільки коштують особисті дані в Даркнеті. URL: https://xakep.ru/2015/09/24/leaks-statistics/

Кліницький І.І. - слухач магістратури юридичного факультету;
Косиченко О.О. - доцент кафедри економічної та інформаційної безпеки, кандидат технічних наук, доцент (Дніпропетровський державний університет внутрішніх справ)

ОСОБЛИВОСТІ ПРАВОВОГО РЕГУЛЮВАННЯ ПРАВОВИХ ВІДНОСИН З ВИКОРИСТАННЯМ КРИПТОВАЛЮТ

Поняття “Криптовалютний ринок” та “Криптовалюта” слід вважати порівняно новими, адже речі, котрі зазначені окреслюють, виникли тільки у 2009 році — тоді з’явилась перша піринґова платіжна система “Bitcoin”, розроблена анонімно. Зазначена децентралізована метода є практичною реалізацією моделі криптовалюти, що була розроблена у 1998 році вченим та комп’ютерним інженером Вей Дайєм (англ. Wei Dai) [1,2]/

Завдяки технологічним особливостям публічного регістру блокчейн та

криптографічним методам користувачі криптовалют, заснованих на даних підходах мають ринкові переваги:

1) анонімність, що дозволяє безперешкодно отримувати матеріальні і нематеріальні блага будь-якого типу в обмін на певну кількість електронної валюти.

2) відсутність єдиного фінансового регулятора (подібного до центральних банків у більшості держав) — що становить кардинально нове явище у сучасній торгівлі: у світі вже як півстоліття існує вільний ринок валюти, де ціна тієї чи іншої грошової одиниці залежить від попиту та пропозиції, але державне регулювання завжди надає змогу штучно зменшити або збільшити цінність валюти на ринку шляхом її емісії та ремісії — таким чином, прогнозувати майбутню ціну ще складніше; більшість криптовалютних інструментів влаштовані так, що випуск нової валюти заснований на алгоритмі, на котрому базується така грошова одиниця, що забезпечує значний рівень зацікавленості суспільства [2].

Проте, анонімність та висока цінність на ринку призвели до актуалізації проблеми правового вакууму стосовно децентралізованих грошових криптоодиниць не лише у світовому масштабі, а й на території України. Проблематика відсутності належного правового регулювання і розроблення концепції у контексті розроблення законодавчої регуляції були досліджені: Вахрушевим Д.С., Ломовцевим Д.О., Сузаковим І.Р., Фрідріхом фон Хайеком [3-7].

У світі не існує жодного регулятора для криптовалют, котрі засновані на принципі розподілених розрахунків (англ. “distributed ledger technology”). Тож приклад регулювання у США слід окреслити як “вільний обіг”: регулятор податкових операцій IRS у власному роз’ясненні “Notice 2014-21” не визначає жадних заходів у контексті обмеження криптовалютних операцій. У документі зазначено, що віртуальний валютний інструментарій, заснований на криптографічних методах, становить собою анонімний засіб міни і це може створювати ряд обмежень учасникам правовідносин. У певній мірі являють собою регуляцію роз’яснення зі сторони IRS у сфері процедур оподаткування угод з використанням криптовалюти. Зокрема, базовою є наявність прив’язки при здійсненні оподаткування операцій до курсу долара США на день проведення виплат. Регулятор приділив суттєвої уваги таким правовим відносинам як:

1) оподаткування заробітної платні, що сплачено у криптовалюті;

2) договір купівлі/продажу з розрахуванням у криптовалюті;

3) інвестиції у криптовалюті.

У межах юрисдикції України пунктом входження стосовно визначення правового статусу віртуальної валюти з використанням криптографічних засобів слугує правовий акт Національного Банку України під назвою “Роз’яснення щодо правомірності використання в Україні "віртуальної валюти/криптовалюти" Bitcoin від 10.11.2014 року” містить позицію фінансового регулятора стосовно криптовалютних операцій. У відповідності до зазначеного підзаконного нормативно-правового акту, має місце побоювання щодо

використання криптографічних валютних засобів. Роз'яснення не містить заборони щодо використання, проте наголошує на неможливості використання такого засобу у якості платіжного.

Виходячи з п'ятого абзацу роз'яснення, криптовалюта являється грошовим сурогатом. Відповідно до ст. 1 ЗУ "Про НБУ", грошовий сурогат — це будь-які документи у вигляді грошових знаків. Грошовими ж знаками є банкноти та монети (ЗУ "Про платіжні системи та переказ коштів в Україні" ст. 3 (п. 3.2)). Таким чином, виходячи з вище наведеного твердження та базуючись на тому, що криптовалюти не існують у формі банкнот та монет (адже мають ознаку віртуальності), дане роз'яснення не може бути застосовано у випадку такого виду валют.

Ураховуючи наведені факти, вакуум у регулюванні питання криптовалютних операцій збережено, хоч наведене роз'яснення можна вважати "*opinio iuris*" у сфері права, адже виражає ставлення регулятора валютного ринку до явища. Залишається невідомим порядок розглядання справ у рамках судової системи; наприклад, як реагувати Фіскальній службі України на факти несплати податків власниками LiteCoin чи Bitcoin.

На підставі преамбули до Конституції України значної уваги потребує фактичний стан речей у законодавстві Європейського Союзу, а також держав-членів, задля імплементації таких рішень у вітчизняне право. Європейський Центральний Банк, а також Європейський Парламент мають у більшій мірі ліберальний підхід: визнали зазначений засіб сплати як валюту, котра не підлягає централізованій регуляції і у певних ситуаціях може бути використана у якості грошей [8].

Досвід держав-учасниць ЄС також засновується на зазначеній позиції. До прикладу слід навести Відповідь на інтерпретацію № 6655, котра була видана Пьотром Новаком (Piotr Nowak), державним секретарем Міністерства фінансів Речі Посполитої Польської від 02 листопада 2016 року. Даний акт права містить у собі визначення ризиків використання криптовалюти, термінологію з відповідним посиланням на акти права видані згаданими вище інституціями ЄС. Суттєве значення такого документа виражено у тому, що третій абзац відсилає до нормативно-правових актів у сфері сплати податків. У Відповіді наголошено про відсутність потреби сплачувати ПДВ (VAT), на підставі закону Dz. U. z 2016 r. poz. 710 z późn. Zm, проте зазначена валюта підлягає оподаткуванню податком з доходів для осіб фізичних при конвертуванні у валюту державну (злотий) чи закордонну.

Продовження дослідження сучасної проблематики криптовалюти, відповідно до нинішнього українського законодавства, потребує аналізу фактичного стану речей. Слід виділити наступні ознаки для зазначеного виду платіжних засобів:

1) існують як такі (їх можна передати та зберігати);

2) мають визначену ринкову вартість.

З наведеного вище, кожна криптовалюта являє собою річ — відповідно до статті 179 (ч.1) Цивільного кодексу України, це предмет матеріального

світу, щодо якого можуть виникати цивільні права та обов'язки. Проблему становить ознака матеріальності, проте відповідно до позиції Хатунцева О. А.: матеріальність речі визначається у можливості до її оцінки. Так, до прикладу, ринкову цінність людської думки неможливо оцінити, але книга, як спосіб вираження думок, оцінці підлягає [9, с. 281]. Валюта у її сучасному розумінні повністю підлягає ринковій оцінці: валютний ресурс фактично коштує лише ті кошти, що були витрачені на його продукування, проте його ринкова вартість може бути значно вищою і керується попитом (ідеальний стан речей).

Виходячи зі ст. 715 Цивільного кодексу України, а також статусу криптовалюти на рівні матеріальної речі дозволяє трактувати операції з її використанням як бартер [10, с. 295].

На внутрішньодержавному ринку сторони угод фактично не обмежені у бартерних операціях. Хоч питання оподаткування криптовалют не визначається у жодному акті вітчизняного права, проте вартість таких також може бути доходом, у відповідності до статті 135 Податкового кодексу України, якщо виступають у ролі товару.

Обмеження щодо бартеру з використанням криптовалют мають місце. Постанова Кабінету Міністрів України №756 від 29.04.99 р. встановлює перелік обмежень зовнішньоекономічного бартеру. Зокрема, документ містить перелік товарів, після експорту яких ввезення імпорту має відбутися щонайбільше через 60, а не через 180 днів: пшениця, жито, ячмінь, ріпак, льон борошно, велика рогата худоба, вівці, кози, яловичина морожена, шкіра, аміак, карбамід, напівфабрикати із заліза та сталі, чавун, феромарганець.

Там само визначено перелік товарів, котрі в Україну заборонено ввозити за бартером, а також вивозити з країни (ювелірні вироби та їхні частини з коштовних металів, діаманти, бурштин), також товари, які за договором міни не можна вивозити з країни, але можна ввезти (алкоголь, сигарети, олія, соняшникове насіння, шкіра, гірничодобувне устаткування, вугілля і нафта; різні метали, брухт; коштовне каміння, також порошок із нього).

Стан вітчизняного правового поля у контексті криптовалютних засобів можна оцінювати як розроблений на недостатньому рівні, але у відповідності до наведеної правової бази України, існує можливість до аргументації такого типу операцій. Наявність можливості інтерпретації таких правовідносин при використанні сили цивільного законодавства і податкового створює передумови для легалізації доходів, отриманих через електронні валютні засоби, використання усього інструментарію з охорони прав. Критична позиція Національного Банку України вочевидь є негативною щодо довіри інвесторів, котрі диспонують криптовалютними платіжними засобами, адже передусім, може бути визнана як декларування плану дій.

Аналізуючи досвід на міжнародному рівні, можна зробити висновок, що держави-лідери світової економіки та наддержавні утворення хоч обережно відносяться до анонімних фінансових інструментів, проте роблять максимум можливостей для того, аби володільці гаманців з криптовалютою

отримували засоби до вільного та легального інвестування таких коштів, купівлі/продажу, захисту власних прав у судах і навіть сплати податків. Отже, такий економіко-правовий феномен як “криптовалюти” вже складно підвести до заборони чи значного обмеження у правах його власників, адже ринкові відносини у даній сфері з кожним днем збільшують своє значення у світовій економіці.

Використані джерела:

1. Сулейманов С. История биткоинов. TJOURNAL — издание о медиа, технологиях и трендах. / С. Сулейманов// [Електронний ресурс]: Режим доступу: http:// tjournal.ru/paper/bitcoin-history
2. Raszl I. The exponential growth of Bitcoin value explained. [Електронний ресурс]: Режим доступу: http://bitcoinowl.com/exponential-growth-bitcoin-value-explained
3. Notice 2014-21 by IRS – [Електронний ресурс]: Web-link: https://www.irs.gov/pub/irs-drop/n-14-21.pdf (date of excess: 26.05.2019).
4. Роз'яснення щодо правомірності використання в Україні "віртуальної валюти/криптовалюти" Bitcoin – Роз'яснення Національного банку України від 10.11.2014. – [Електронний ресурс]. Код доступу: http://zakon3.rada.gov.ua/laws/show/n0435500-14 (дата посилання: 26.05.2019).
5. U.S. Securities and exchange commission “Citizens of the USA with Maksim Zaslavskiy – [Електронний ресурс]: Web-link: https://www.sec.gov/news/press-release/2017-185-0 (date of excess: 26.11.2017).
6. Юшаева Р. С-Э., Медов И .Л. Криптовалюта - феномен XXI века // Теория и практика современной науки. Сборник научных трудов по материалам XX Международной научно-практической конференции. - М.: Издательство «Олимп», 2017 . С.250-252.
7. Ястребова А., Макогон Е. Как криптовалюта Bitcoin используется на практике в налоговом планировании [Електронний ресурс]: код доступу: http://www.nalogplan.ru/article/36 09-kak-kriptovalyuta-bitcoin-ispolzuetsya-napraktike-vnalogovom-planirovanii.
8. Marszałek Paweł Kryptowaluty – pojęcie, cechy, kontrowersje, 2019 Poznań, [Електронний ресурс]: http://orka.sejm.gov.pl/WydBAS.nsf/0/F8F4218303461D74C12583E10037EC68/$file/5.Marszalek.pdf>
9. Хатунцев О. А. Деление вещей на движимые и недвижимые // Бизнес в законе. 2008. №2. С.281-284

Лізунов С.І. - доцент кафедри захисту інформації Національного університету «Запорізька політехніка», кандидат технічних наук, доцент

ЗАХИСТ ВІД ВИТОКУ ІНФОРМАЦІЇ ПО КАНАЛАМ ВИСОКОЧАСТОТНИХ ВИПРОМІНЮВАНЬ

Сьогодні для зберігання, передачі і обробки режимної інформації широко застосовуються різні електронні пристрої, проте в ході їх роботи оброблювану інформацію можливо викрасти із-за випромінювання цими прилада-

ми високочастотних (ВЧ) випромінювань. Більше того, інформацію можна викрасти по радіоканалу за допомогою заносних радіозакладних пристроїв, а також за допомогою зовнішнього високочастотного нав'язування.

Проблеми таких уразливостей можна вирішувати активними і пасивними способами. Активний метод полягає в зашумленні випромінювань за допомогою генераторів шуму, а пасивний метод - в екрануванні джерел інформативного сигналу.

Проте використання активних засобів має певні недоліки:

- Тривале знаходження персоналу в кімнаті з генераторами шуму може негативно вплинути на їх здоров'я.

- При зміні розташування джерел інформативного сигналу (наприклад, перестановці ПК або додаванні нових), загальний рівень сигналу в приміщенні може зміниться таким чином, що сигнали можна буде виявити поза приміщенням, незважаючи на зашумлення.

- Необхідно зашумлювати сигнали в широкому діапазоні частот. Межі цього діапазону не завжди можна чітко визначити із-за биття декількох сигналів, а також можливого зовнішнього ВЧ впливу.

- Наявність пригнічуючих випромінювань демаскує об'єкт і може заважати роботі інших чужих пристроїв за межами контрольованої зони.

- Використання активних засобів передбачає постійні додаткові дії (наприклад, підготовка комплексу до роботи, включення, виключення, профілактика, постійна перевірка його працездатності і тому подібне).

- Необхідні додаткові джерела живлення. Іноді це приводить до обмеження працездатності генераторів шуму у часі.

Екранування має на увазі під собою обгороджування джерел випромінювання спеціальним екраном, який локалізує електромагнітну енергію в собі, не даючи їй вийти за його межі. Також екран заважає зовнішнім електромагнітним випромінюванням потрапляти всередину. Екранування має особливості, які можна з вигодою використати при захисті виділених приміщень або об'єктів :

- Будучи пасивним методом, після установки екрану з ним значно менше робіт по перевірці його працездатності.

- Екранування випромінюючих установок може понизити шкідливу дію електромагнітних випромінювань на людей.

- Екранування одночасно усуває загрози витоку інформації як по каналах побічних електромагнітних випромінювань та наведень (ПЕМВН), так і за допомогою радіозакладок, що знаходяться в приміщенні.

- Відсутні демаскуючі ВЧ випромінювання.

В якості матеріалів для ефективного екранування використовуються металеві листи і сітки [1]. Сталеві листи завтовшки 2-3 мм, зварені герметичним швом, забезпечують найбільший екрануючий ефект (до 100 дБ і більше). Товщина сталевого листа вибирається виходячи з міцності конструкції і можливості створення суцільного шва [2].

До недоліків листових металевих екранів можна віднести високу вар-

тість, велику вагу, великі габарити і складність монтажу. Цих недоліків позбавлені металеві сітки. Вони легше, простіше у виготовленні і розміщенні, дешевше. Основними параметрами сітки є її крок, рівний відстані між сусідніми центрами дроту, радіус дроту і питома провідність матеріалу сітки. До недоліків металевих сіток відносять, передусім, високий знос в порівнянні з листовими екранами.

Для екранування також застосовуються фольгові матеріали. До них відносяться електричне тонкі матеріали завтовшки 0,01- 0,05 мм. Фольгові матеріали в основному робляться з діамагнітних матеріалів - алюміній, латунь, цинк.

Перспективним напрямом в області екранування є застосування струмопровідних фарб і напилень [3], оскільки вони дешеві, не вимагають робіт по монтажу, прості в застосуванні. Струмопровідні фарби створюються на основі діелектричного плівкотвірного матеріалу з додаванням в нього складових, що проводять струм, пластифікатора і отверджувача. В якості струмопровідних пігментів використовують колоїдне срібло, графіт, сажу, оксиди металів, порошкову мідь, алюміній [4].

Особливу увагу треба приділяти екрануванню вікон, дверей та систем вентиляції. Для цього, крім вище згаданого, використовують спеціальні тканини [5].

Слід врахувати, що для правильної роботи екран має бути заземлений, інакше він може навіть виступати випромінювачем небезпечного сигналу. Також екран має бути цілісним і не мати проміжків більше ніж одна десята довжини хвилі небезпечного сигналу. У зв’язку з цим в місцях входу в екроване приміщення різних комунікацій необхідно встановлювати спеціальні фільтри, що перешкоджають виходу небезпечних сигналів за межі контрольованої зони.

За певних умов, елементи вищезгаданих конструкцій можуть виконувати роль звукопроводів, що потребує особливої уваги та додаткових заходів при їх монтажі та експлуатації з метою захисту мовної інформації.

Використані джерела:

1. Виды экранирующих материалов. Применение и экранирование. [Електронний ресурс]: – Режим доступу: https://electrosam.ru/glavnaja/jelektrotehnika/ekraniruiushchikh-materialov/
2. Инженерно-техническая защита информации: учеб. пособие для студентов, обучающихся по специальностям в обл. информ. безопасности / А. А. Торокин. — М.: Гелиос АРВ, 2005. — 960 с.: ил. — ISBN 5-85438-140-0.
3. А. Борисов, А. Мачулянский, М. Родионов. Применение тонких металлических пленок для электромагнитного экранирования. – Національний технічний університет України «КПІ»: Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні, вип. 3, 2001 р., с. 187-196.
4. НОУ ИНТУИТ | Лекция | Методы защиты информации от утечки через ПЭМИН. [Електронний ресурс]: – Режим доступу: http://www.intuit.ru/studies/courses/2291/591/lecture/12704
5. Тканини для захисту від ЕМВ. [Електронний ресурс]: – Режим доступу: https://nanomarket.com.ua/g49937063-tkanini?gclid=CjwKCAjw-ZvlBRBbEiwANw9UWlzcDyRTm9TY3pG_rUjy0fxiy7xZ1smpl7lb7zGPfN9WtkjsIFzkORoCgpgQAvD_BwE

Лізунов С.І. - доцент кафедри захисту інформації Національного університету «Запорізька політехніка», кандидат технічних наук, доцент

СИСТЕМИ АКТИВНОГО ПРИГНІЧЕННЯ АКУСТИЧНОЇ ІНФОРМАЦІЇ

Зазвичай, для усунення просочування інформації по акустичному каналу, застосовують або звукоізоляцію, або генератори корельованих акустичних перешкод.

У першому випадку (пасивний метод) потрібні значні витрати часу на проведення робіт по звукоізоляції. Крім того, залишаються проблемні ділянки приміщення (вікна, двері, повітропроводи і тому подібне) і віброакустичні канали витоку (системи опалювання, водопостачання, каналізації і так далі).

У другому випадку (активний метод) наявність генераторів шуму створює дискомфорт при проведенні переговорів. Саме випромінювання є демаскуючою ознакою, що полегшує зловмисникам визначити час і місце переговорів.

Недоліки обох перелічених вище методів можуть бути зменшені при застосуванні систем активного пригнічення акустичних шумів (Active Noise Control, Active Noise Cancellation, ANC, Active Noise Reduction, ANR).

Системи активного шумозаглушування ґрунтуються на процесі інтерференції хвиль. Іншими словами, якщо створити дзеркальне відображення звукової хвилі (інвертувати її), і накласти її на початкову, то звукові хвилі погасять одна одну.

Для захоплення навколишнього звуку, система активного шумозаглушування (САШ) оснащена одним, або декількома мікрофонами, які слухають навколишні звуки. Потім, ці звуки передаються в електронний блок, в якому і відбувається аналіз і їх інвертування. Потім отриману дзеркальну хвилю (з перевернутою фазою) подають на випромінювач. Ці звукові хвилі в процесі інтерференції змішуються в нову хвилю і пригнічують одна одну.

Найефективніше такі системи справляються з шумом від 100 Гц до 1 кГц.

Попри те, що сам по собі метод дозволяє ефективно пригнічувати навколишні звуки, реальні пристрої не завжди справляються з цим завданням, особливо з акустичними коливаннями з частотою більше тисячі Герц.

Річ у тому, що на реєстрацію звуку і обчислення протилежної хвилі у мікроконтролера йде деякий час. Через це звук, що випускається ним, вже не повністю протилежний до звуку, що входить, а відстає від нього по фазі.

Цей недолік можна зменшити, якщо сигнал, який потрібно подавити, подавати на вхід такого пристрою по електричному або електромагнітному каналу.

Завдяки тому, що електричний сигнал поширюється швидше за звук, прилад починає обробляти сигнал ще до його приходу у вигляді акустичної хвилі. Завдяки цьому мікроконтролер устигає підібрати "протилежний" звук, співпадаючий по фазі з оригінальним, з меншим запізнюванням. Шумозаглушування таких систем працює для звуків з частотою до 4 кГц, що є досить прийнятним для спектру мовної інформації.

Таким чином, на межах контрольованої зони можна знизити рівень акустичних хвиль від джерел режимної інформації до безпечної (прийнятної) величини.

Завдання хорошої чутності співрозмовниками один одного можна вирішити за допомогою правильного розташування і налаштувань системи, а також спеціальних гарнітур у вигляді масок.

Такі системи можна також з успіхом використовувати в режимних приміщеннях, де циркуляція акустичної (мовної) інформації заборонена взагалі.

Максимова М.К. – слухачка магістратури юридичного факультету;
Косиченко О.О. – доцент кафедри економічної та інформаційної безпеки, кандидат технічних наук (Дніпропетровський державний університет внутрішніх справ)

ОСОБЛИВОСТІ ЗАХИСТУ ТА ПОПЕРЕДЖЕННЯ ФАЛЬСИФІКАЦІЇ ДОКУМЕНТІВ, ЩО ПОСВІДЧУЮТЬ ОСОБУ ПРИ ПЕРЕТИНІ ДЕРЖАВНОГО КОРДОНУ УКРАЇНИ

Одним з основних напрямків державної політики з питань національної безпеки та євроінтеграції України є запобігання транснаціональній організованій злочинності під час процедури перетину державного кордону України. Використання підроблених паспортних документів – це достатньо поширений засіб, який сприяє реалізації загроз різних видів організованої транснаціональної злочинності, особливо торгівлі людьми, терористичній діяльності, нелегальній міграції.

Важливим елементом боротьби з таким явищем як фальсифікація паспортних документів є забезпечення ефективної судово-експертної діяльності відповідних підрозділів Державної прикордонної служби України (далі – ДПСУ). Для проведення якісної судово-технічної експертизи паспортних документів необхідно ретельно аналізувати інформацію про сучасні способи підробки документів.

Потреба в постійному дослідженні ознак і методів підробок зумовлені стрімким розвитком поліграфічних засобів. Такий аналіз сприяє покращенню системи захисту документів, що подають право на перетин державного кор-

дону України [1, с. 58-64].

Відповідно до статистичних даних Головного експертно-криміналістичного центру ДПСУ за 2016-2018 роки, найбільша частина нелегальних мігрантів, що потрапляє в Україну шляхом використання підроблених паспортних документів є вихідцями з країн Близького Сходу, Африки, Азії; СНД. Правопорушники в більшості випадків застосовують часткове підроблення документів, а саме: заміну сторінки персональних даних, заміну фотокарток, унесення змін у реквізити документів, перепрошивку бланка.

Органи охорони державного кордону України стверджують, що багато випадків частково підроблення паспортів України трапляється у східних регіонах – на тимчасово окупованій території Автономної Республіки Крим та в деяких районах Донецької та Луганської області [2].

Основними способами часткової підробки документів є механічне підчищення його знебарвлення; дописування та виправлення як в рукописному; так і машинописному текстах; заміна аркушів та фотозображень.

Науковці визначають такі засоби захисту від підроблення як технологічний, що полягає у внесені до реквізитів документа певних ознак за допомогою спеціальних технологічних процесів (спеціальний папір, захисні волокна та водяні знаки).; поліграфічний захист, що здійснюється за допомогою різних видів і способів поліграфічного друку (графічні елементи, мікродрук і приховані зображення, фонові сітки); фізико-хімічний захист, який виражається у використані в складі матеріалів документу спеціальних речовин, наявність яких визначається такими методами як флуоресцентні та інфрачервоні фарби, якими наносяться зображення, тексти та номери в документах, що посвідчують особу.

На жаль, не всі документи, що посвідчують особу є достатньо захищеними, наприклад сторінки посвідчення особи на повернення в Україну та посвідчення члену екіпажа не наділені водяними знаками. Також можна помітити відсутність захисник волокон у таких документах. У багатьох вітчизняних паспортних документах відсутня синтетична захисна нитка, така ознака захисту наявна у паспортах США, Франції, Туреччини та інших держав. Потрібно зазначити, що посвідчення члена екіпажа та посвідчення особи на повернення в Україну відрізняється від інших документів, що посвідчують особу відсутністю обкладинки. Це створює додаткові ризики для підробки таких документів [3, с. 30-37].

На думку членів міжнародної асоціації ІКАО (ICAO — International Civil Aviation Organization), для покращення якості українських документів, що посвідчують особу, треба розширити перелік способів додаткового захисту, а саме: на обкладинку та на всі сторінки документів наносити невидимі зображення та захисну стрічку з позитивним і негативним мікротекстом назви країни, що буде люмінесціювати при ультрафіолетовому випромінюванні; дублювати зображення фотопортрета додатково ще на 2, 3 чи 4 сторінках документу; серійний номер наносити способом високого друку не лише на одній сторінці; використовувати металографський друк [4, с. 530-533].

Огляд документів законодавчо регламентується ст.237 Кримінального процесуального кодексу України (далі – КПК України), однак огляд документів, що посвідчують особу має певні специфічні особливості, оскільки це документи сурового обліку та звітності. Важливість такого огляду полягає у виявленні ознак підробки документів, що має значення для попередження правопорушень як на державному та міжнародному рівнях [5, с. 295].

Система та етапи перевірки документів, що посвідчують особу визначені в «Інструкції з організації і здійснення перевірки документів громадян України, іноземців та осіб без громадянства , які перетинають державний кордон». Існують такі рівні перевірки зазначених документів: стандартна перевірка, яка буває спрощеною та повторною; поглиблена перевірка; експертне дослідження [6].

В Україні гострою проблемою залишається технічне забезпечення експертних підрозділів, яке більшою є застарілим, але це не перешкоджає виконанню основних завдань.

Отже можна зробити висновок, що сучасні засоби захисту документів, що посвідчують особу в цілому виконують функцію захисту таких документів від фальсифікації, проте відбувається постійне вдосконалення механізмів захисту шляхом упровадження новітніх технологічній та запозичення міжнародного досвіду для покращення якості українських документів. Правоохоронним органом України потрібно модернізувати технічні засоби відповідно до сучасних реалій та завдань експертного дослідження документів.

Використані джерела:

1. Ананьїн О.В., Чередніченко Д.К. Елементи захисту сучасних паспортних документів, що надають право іноземцям на перетинання державного кордону України, та характерні способи їх фальсифікації /О.В.Ананьїн, Д.К.Чередніченко//Криміналістичний вісник.-2018.-вип.29.-с.58-64.

2. Інфографіка на сайті Державної прикордонної служби України. [Електронний ресурс]. – [Електронний ресурс]. - Режим доступу: www.dpsn.gov.ua

3. Кобилянський О.Л. Спеціальні засоби захисту документів від підробки: криміналістична характеристика/ О.Л.Кобилянський // Криміналістичний вісник.-2016.-вип.26.-с.30-37.

4. Чорноус Ю.М. Міжнародне співробітництво у розслідуванні злочинів/Ю.М.Чорноус//Юридичні науки.-2014.-вип.2-с.530-533

5. Тихонова В.І. Дослідження документів, виготовлених за новітніми технологіями/В.І.Тихонова//Теорія та практика судової експертизи і криміналістики.-2016. - Вип.10 - с.295.

6. Про затвердження Інструкції з організації і здійснення перевірки документів громадян України, іноземців та осіб без громадянства, які перетинають державний кордон: затв. Наказом Адміністрації Державної прикордонної служби України від 05.06.2012 р. [Електронний ресурс].- Режим доступу: www.rada.gov.ua

7. Тальянчук Л.С. Криміналістичне дослідження документів, що посвідчують особу при перетині державного кордону України /Л.С.Тальянчук// Науковий вісник Національної академії внутрішніх справ.-2016.-вип.5. - с.172-178

Мирошниченко В.О. - професор кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ, кандидат технічних наук, доцент

ВІДЕОСПОСТЕРЕЖЕННЯ: МОЖЛИВОСТІ ТА ПЕРСПЕКТИВИ

Сьогодні відеоспостереження міцно увійшло в наше повсякденне життя і є невід'ємним інструментом у багатьох сферах діяльності, в тому числі і правоохоронної. Грамотно побудована система відеоспостереження дозволяє вирішувати широкий і різноманітний спектр завдань: від контролю за складними і динамічними процесами до аналізу і своєчасного реагування на різні позаштатні ситуації.

Звичайно ж, основними завданнями, які вирішують системи відеоспостереження, є питання, пов'язані із забезпеченням безпеки, а також питання контролю і управління, які, як правило, постійно розвиваються і стають все більш високотехнологічними.

У зв'язку з цим використання інтелектуальних систем відеоспостереження з метою забезпечення безпеки (в широкому сенсі цього слова) сьогодні представляється вкрай актуальним. Використовувані в даний час системи відеоспостереження дозволяють:

• здійснювати відеофіксацію подій зі створенням відеоархівів;
• здійснювати розпізнавання об'єктів (люди, авто, предмети) які представляють інтерес або небезпеку;
• виконувати охоронні функції стратегічних об'єктів, охороняти територію від незаконного проникнення підозрілих і сторонніх осіб;
• підвищити безпеку транспортної інфраструктури;
• автоматизувати допуск осіб на певні об'єкти і контролювати територію в'їзду і виїзду автотранспорту.

Таким чином, використання відеотехнологій значно спрощує контроль за безпекою на різних об'єктах і сприяє ефективній роботі правоохоронних органів в цілому.

Залежно від поставленої задачі, системи відеоспостереження можуть використовуватися на різних об'єктах. Найбільш "популярними" місцями є місця скупчення людей, транспортна структура, а також КПП і охороньовані території [1].

Сьогодні професійне застосування відеоспостереження відкриває ряд широких і часто просто унікальних можливостей. Це стало реальним завдяки розвитку інтелектуальних функцій систем відеоспостереження, а саме - відеоаналітики. Сучасні системи стають все "розумнішими", надаючи тим самим нові можливості для їх використання.

Інтелектуальні детектори, вбудовані в систему відеоспостереження і

працюючі в автоматичному режимі, дозволяють не просто спостерігати за подіями, що відбуваються і збирати їх в архівах, але також сповіщати оператора про різні події та інциденти. Так, важливою функцією відеоаналітики є можливість аналізу зображення з застосуванням логічних алгоритмів. У звичайних охоронних системах відеоспостереження застосовуються різні детектори, наприклад, руху або перетину периметра. Деякі виробники пропонують такі детектори вже вбудовані в камери. Проте, для систем інтелектуального відеоспостереження цього недостатньо. Необхідні відеосистеми, які будуть реалізовувати будь-які послідовності дій відповідно до аналізу відеозображення, що надходить з камер.

Відзначимо, що для забезпечення безпеки успішно застосовуються не тільки класичні системи відеоспостереження, а й такі просунуті технології, як системи розпізнавання осіб і розпізнавання автомобільних номерів, які є важливим елементом інтелектуальних систем відеоаналітики [2].

Принцип роботи системи розпізнавання осіб заснований на автоматичному виділенні камерою відеоспостереження осіб, які перебувають в полі зору камери. Відеоспостереження полягає в наступному: система в автоматичному режимі виділяє, фотографує і зберігає особи, що потрапили в поле зору камери, при цьому система може розпізнати обличчя і оповістити оператора про те, що та чи інша особа перебуває на конкретному об'єкті або в конкретній зоні [3]. Застосування подібних систем можливо не тільки і не стільки з метою забезпечення безпеки та / або контролю доступу, можливості таких технологій дозволять вирішувати більш складні завдання.

Варто сказати кілька слів про типи камер, які можуть використовуватися в системах відеоспостереження на різних об'єктах. Для ефективної роботи відеосистем, необхідно підбирати камери з урахуванням конкретних особливостей кожного окремого об'єкта. Важливу роль в цьому питанні відіграють такі характеристики, як площа приміщення, температурні умови, особливості освітлення і т.д.

В рамках даної роботи коротко торкнемося питання застосування такої інноваційної технології, як машинний зір. Сам термін "машинний зір" має на увазі комп'ютерну обробку відеоінформації, отриманої з камер спостереження. Система, яка функціонує на основі алгоритмів машинного зору, перш за все, включає детектор захоплення зображень і детектор аналізу і обробки зображень, що надає можливість вирішувати вкрай широкий спектр завдань. При цьому на сьогодні застосовуються як системи двовимірного, так і об'ємного машинного зору.

На закінчення кілька слів про інноваційні розробки в сфері інтелектуального відеоспостереження і відеонаналізу, пов'язані з фізіогномікою і розпізнаванням емоцій людини, які по праву можуть вважатися технологіями майбутнього і, безумовно, знайдуть ефективне застосування, в тому числі і в правоохоронній сфері. На сьогоднішній день дослідження в області фізіогноміки і розпізнавання людських емоцій знаходиться в стадії активного розвитку. Відзначимо, що "розумні" системи вже навчилися розпізнавати пос-

мішку на обличчі людини або ж відсутність такої. Прикладом успішної роботи в даному напрямку може служити французький автоконцерн PSA, інженери якого розробили систему розпізнавання емоцій людини, призначену для установки в автомобілях. Передбачається, що дана технологія також буде використовуватися і в інших областях. Мета розробників подібних систем - створити програмне забезпечення, яке могло б розпізнавати базові людські емоції: здивування, радість, смуток і ін., проводити аналіз емоційного стану людини і прогнозувати подальшу поведінку людини.

Таким чином, використання інтелектуального відеоспостереження є одним з напрямків для ефективного вирішення низки складних соціальних і технічних завдань, що дозволяють усувати позаштатні ситуації.

Використані джерела:

1. В.О. Мирошниченко, О.С. Гавриш. Відеоспостереження як інструмент забезпечення безпеки на транспорті. Науковий вісник Дніпропетровського державного університету внутрішніх справ: Зб. наук. праць. –2018. –№2.
2. Мирошниченко В.О. Біометрічна ідентифікація клієнтів в банківській сфері. Міжнародна та національна безпека: теоретичні і прикладні аспекти. Матер III Міжнар. наук-практ. конф. (м. Дніпро, 15 бер.2019 р.) Дніпро: Дніпроп. держ. ун-т внутр. справ, 2019, с. 263 – 265.
3. В.О. Мирошниченко, І.В. Краснобрижий, А.М. Гребенюк. Ефективність біометричних технологій та особливості їх використання в системах контролю доступу. Науковий вісник Дніпропетровського державного університету внутрішніх справ: Зб. наук. праць. –2019. –№3.

Мурзіна О.А. - асистент кафедри медичної і фармацевтичної інформатики та новітніх технологій, кандидат педагогічних наук; **Каблуков А. О**. - доцент кафедри медичної і фармацевтичної інформатики та новітніх технологій, кандидат технічних наук, доцент (Запорізький державний медичний університет)

ОПТИМІЗАЦІЯ НАВЧАЛЬНОГО ПРОЦЕСУ ЧЕРЕЗ СТВОРЕННЯ ІНФОРМАЦІЙНО-ОСВІТНЬОГО СЕРЕДОВИЩА

Підвищення ефективності професійної підготовки майбутніх юристів потребує удосконалення існуючих та пошуку нових форм та методів організації навчального процесу з відповідним врахуванням використання комплексів технічних і дидактичних засобів, які забезпечують взаємозв’язок аудиторної та позааудиторної форм занять.

На думку Л. Петухової та О. Співаковського, використання інформаційно-комунікаційних технологій засвідчило переваги їх над традиційними методами навчання в контексті здійснення особистісно-орієнтованого підхо-

ду, оскільки більшою мірою сприяють реалізації принципів індивідуалізації й диференціації навчального процесу, розширенню його змісту, підвищенню інтенсифікації і результативності навчання в цілому [11, с. 7].

Перспективним шляхом організації процесу навчання на основі широкого використання ІКТ у ВНЗ є поєднання технологій традиційного та дистанційного навчання. Процес, за якого традиційні технології поєднуються з інноваційними технологіями електронного, дистанційного та мобільного навчання, називають «змішаним навчанням». Змішане навчання як інструмент модернізації сучасної освіти на практиці представляється в створенні нових педагогічних методик, що основані на інтеграції традиційних підходів організації навчального процесу, де здійснюється передача знань, та технології електронного навчання [2, с. 19].

Ю. Триус стверджує, шо використання традиційних, інноваційних педагогічних технологій та інформаційно-комунікаційних технологій навчання за принципами взаємного доповнення підвищує якість освіти [3, с. 304].

Ми пропонуємо створення такого середовища навчання, де майбутні юристи і викладачі можуть в зручних для себе обставинах та зручний час здійснювати процес навчання; викладач тезісно пояснює навчальний матеріал і зупиняється на важких моментах на занятті в аудиторії, інше студенти вивчають самостійно; проводяться як очні, так і online консультації; студенти в аудиторії приділяють більше часу відпрацюванню практичних навичок тощо. Така організація навчання дозволяє студентам самостійно отримувати нові знання за допомогою електронних ресурсів у зручний для себе час, а на заняттях у спілкуванні з викладачем та одногрупниками практикуватися в нових уміннях. Формує у майбутніх юристів відповідальне ставлення до навчання, планування часу, обирання темпу засвоєння навчального матеріалу та дозволяє організувати спільну роботу над проектами, проведення дискусій, семінарів, організованих у вигляді електронних телеконференцій, форумів, відбувається процес розвитку навичок онлайн-спілкування. Під час такого навчання відбувається процес організації самостійної когнітивної діяльності майбутніх юристів та дозволяє врівноважити базові та їх супутні знання за рахунок самостійного вивчення теоретичних матеріалів та виконання додаткових завдань. Використання сучасних програмних і технічних засобів, робить навчання більш ефективним.

Навчальний процес, організований за такою технологією, спрямований на формування всебічно розвиненої особистості, тому реалізує освітню, розвиваючу та виховну функції.

Результатом такого навчання є формування особистості майбутнього юриста з необхідним набором ключових компетентностей, здатного вирішувати різноманітні професійні задачі. Процес навчання за такою моделлю спрямований на розвиток у майбутніх юритсів навичок самоконтролю. На нашу думку, таке навчання сприяє підвищенню ефективності навчання, оскільки відбувається не тільки аудиторна навчальна діяльність студента, а й постійна та регулярна самостійна робота з використанням сучасних програмних

та технічних засобів, що веде до неперервності навчального процесу. Таке навчання активізує аналітичні здібності майбутніх юристів та розвиває критичне мислення за рахунок того, що вони отримують навчальний матеріал не тільки від викладача на лекції, але й самостійно повинні шукати, обирати та обробляти необхідний матеріал. Застосування у навчанні новітніх технологій, методів, інструментів та засобів дозволяє більш ґрунтовно використовувати потенціал навчального контенту.

Компетентнісний підхід, який спрямований на формування і розвиток у студентів ключових компетентностей (ціннісно-смислова, загальнокультурна, навчально-пізнавальна, інформаційна, комунікативна, соціально-трудова, компетентність особистісного самовдосконалення) становить загальнонаукову та конкретно-наукову методологію такого навчання.

Отже, ми пропонуємо створення інформаційно-освітнього середовища, яке в межах дистанційної форми освіти суттєво доповнює аудиторну взаємодію педагогів та студентів через інтерактивні форми спілкування з використанням Skype-конференцій, вебінарів, круглих столів, дебатів, дискусій.

Використані джерела:

1. Петухова Л. Є., Співаковський О. В. Актуальні питання формування інформатичних компетентностей майбутніх учителів початкових класів / Л. Є. Петухова, О. В. Співаковський // Комп'ютер у школі та сім'ї. – 2011. - №1. – с. 7-11.
2. Кривонос О.М., Коротун О.В. Змішане навчання як основа формування ІКТ-компетентності вчителя / О.М. Кривонос, О.В. Коротун // Наукові записки. – Випуск 8. – Серія: Проблеми методики фізико-математичної і технологічної освіти. Частина 2. – Кіровоград: РВВ КДПУ ім. В. Винниченка, 2015 – 180 с.
3. Триус Ю. В. Комбіноване навчання як інноваційна освітня технологія у вищій школі / Ю. В. Триус, І. В. Герасименко // Теорія та методика електронного навчання : збірник наукових праць. Випуск ІІІ. – Кривий Ріг, 2012. – 299-308 с.

Нестерович В.Ф. - доктор юридичних наук, доцент, завідувач кафедри державно-правових дисциплін Луганського державного університету внутрішніх справ імені Е.О. Дідоренка

РОЛЬ ЕЛЕКТРОННИХ ІНСТРУМЕНТІВ У ПІДВИЩЕННІ ВЗАЄМОДІЇ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ ТА ГРОМАДСЬКОСТІ В УКРАЇНІ

У сучасному інформаційному, відкритому та демократичному суспільстві важлива роль у підвищенні взаємодії Національної поліції та громадськості в Україні безумовно належить різного роду електронним інструментам. Ведення керівництвом Національної поліції своїх сторінок у соціальній мережі «Facebook», оперативне інформування Національною поліцією громад-

ськості про ті чи інші події через месенджери, розміщення Національною поліцією актуального відео в YouTube, запуск Національною поліцією спеціальних Інтернет-порталів та електронних реєстрів – усе це є невід'ємною складовою сучасної діяльності Національної поліції України.

Цікаво, що наукове обґрунтування використання електронних інструментів у підвищенні взаємодії влади та громадськості відбулося задовго до практичного впровадження засад електронного урядування. Зокрема, на думку родоначальника комп'ютерної демократії, німецького вченого Г. Крауха, теорія електронної взаємодії громадськості та влади дозволяє вирішити проблеми сучасного урядування на більш високому рівні ніж інші теорії. Головним аргументом цьому є те, що однаковий доступ людей до інформаційно-комунікаційних технологій створює необмежені можливості для розвитку сучасної демократії [1, с. 222]. У зв'язку з цим, звертає увагу російський вчений В. Руденко, що «у сучасних концепціях демократії велике значення надається становленню нового суб'єкта прямого народовладдя – так званої діджітальної (цифрової) публіки. Нові технологічні досягнення роблять можливим не тільки участь окремих, і найчастіше відчужених один від одного громадян у голосуванні, а й створюють основу для їх самоорганізації, що не вимагає безпосереднього спілкування» [2, с. 22].

Зважаючи на наведені наукові позиції, набувають нового сенсу й фундаментальні права людини, які лежать в основі підвищенні електронної взаємодії громадськості та Національної поліції в Україні. Зокрема, право людини шукати, отримувати і розповсюджувати інформацію та свої погляди будь-якими засобами та незалежно від державних кордонів, яке визначено у статті 19 Загальної декларації прав людини 1948 р., $^{1}/_{3}$ населення планети, за даними ООН, реалізує завдяки доступу до світової мережі Інтернет [3, с. 123]. Колосальний та нині ще не до кінця вичерпаний потенціал Інтернету щодо отримання, вивчення та поширення необхідної інформації у текстуальних та аудіовізуальних формах суттєво розширюють спектри впливу громадськості на прийняття нормативно-правових актів. Можливість спілкуватися через комп'ютерні мережі дозволяє досить швидко згуртувати та об'єднати зусилля розрізнених громадян перетворюючи їх у потужну і впливову громадську силу, яка здатна консолідовано підходити до вирішення тієї чи іншої суспільної проблеми.

Більше того, у Доповіді Спеціального доповідача ООН з питань захисту права на свободу думок та їх вільне вираження Франка Ла Ру, проголошеній 3 червня 2011 р. на 17-й сесії Ради ООН з прав людини, наголошується на необхідності визнання права вільного доступу до Інтернету базовим правом людини, – так само, як і права на життя, свободу віросповідання, вільне пересування тощо. Схожу тональність можна простежити і у Спільному посланні Генерального секретаря ООН, Верховного комісара ООН з прав людини, Генерального директора ЮНЕСКО до всіх країн і народів, де сформульовано стратегічне завдання ООН: «Перетворення Інтернету у глобальний суспільний ресурс, який дає змогу почути голос кожної людини». А 27 травня 2011 р. відбулася зустріч

«Групи восьми», в ході якої було прийнято Довільську декларацію «Незмінна відданість свободі і демократії», якою Інтернет проголошено інструментом просування прав людини і демократії у всьому світі [3, с. 123-124].

Отже, дослідження співвідношення розвитку Інтернету та підвищення взаємодії Національної поліції та громадськості в Україні дозволяє зробити висновок, що комп'ютерні мережі є потужним інструментом зміцнення й подальшого вдосконалення сучасної демократії. Сутнісною рисою інформаційного суспільства є те, що нові інформаційно-комунікаційні технології дозволяють суттєво розширити права громадян шляхом надання їм більшого доступу до різного роду інформації. Крім того, комп'ютерні мережі дозволяють значно посилити ступінь впливу громадськості на прийняття нормативно-правових актів та здійснення контролю за їх виконанням, активно використовуючи при цьому інформацію з метою захисту своїх прав, свобод та законних інтересів, а не тільки пасивно її споживаючи. Тому цілком закономірно, що провідні країни західної демократії починають переглядати чинне конституційне законодавство з метою посилення конституційно-правових засад впливу громадськості на прийняття нормативно-правових актів.

Зокрема, у США суттєво переглянуто засади взаємодії органів публічної влади та громадськості з метою їх вдосконалення. Уряд, вказується у Меморандумі Президента США для глав виконавчих департаментів і агентств «Прозорість і відкритий уряд» від 21 січня 2009 року, має бути учасницьким. Залучення громадськості підвищує ефективність уряду і покращує якість його рішень. Знання широко розійшлися в суспільстві, і посадові особи отримати вигоду з наявності доступу до цих дисперсних знань. Виконавчі департаменти та агентства повинні надати американцям більш широкі можливості для участі в розробці політики та забезпечити їх уряд перевагами колективного громадського досвіду та інформації, а також запитати громадську думку про те, як можна розширити та покращити можливості для участі громадськості в управлінні державою. Виконавчі департаменти та агентства повинні використовувати інноваційні інструменти, методи і системи для взаємодії на всіх рівнях влади з некомерційними організаціями, підприємствами та окремими особами в приватному секторі. Потрібен зворотній зв'язок з громадськістю, щоб оцінити та підвищити рівень співпраці і визначити нові можливості для її поглиблення [4]. Слідом за цим у 2011 р. було запроваджено спеціальну громадську Інтернет-платформу «We the People», яка надає можливість кожному створити петицію на сайті Білого дому з того чи іншого питання державної політики США [5].

Суттєвий прорив у використанні електронних інструментів зроблено і в Україні в рамках підвищення взаємодії Національної поліції та громадськості, унаслідок чого діяльність поліції стає більш відкритою, а електронні ресурси, розпорядником яких є Національна поліція та МВС України більш доступними для громадськості. Найбільшими викликами у використанні електронних інструментів у рамках підвищення взаємодії Національної поліції та громадськості є унеможливлення протиправного втручання в особисте і сі-

мейне життя людини, а також недопущення різного роду маніпуляцій з інформацією у результаті роботи з електронними ресурсами Національної поліції.

Використані джерела:

1. Скакун О.Ф. Теория государства и права: Учебник / О.Ф. Скакун. Х.: Консум; Ун-т внутр. дел, 2000. 704 с.
2. Руденко В. Н. Конституционно-правовые проблемы прямой демократии в современном обществе: Автореферат дис. … доктора юридических наук: 12.00.02 – конституционное право; муниципальное право / В. Н. Руденко; Уральская государственная юридическая академия. Екатеринбург, 2003. 46 с.
3. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан дотримання та захисту прав і свобод людини в Україні / Омбудсман України. Київ, 2011. 370 с.
4. Memorandum for the Heads of Executive Departments and Agencies of January 21, 2009 «Transparency and Open Government». *Federal Register*. 2009. Vol. 74. № 15. January 26. P. 4685-4686.
5. We the People is Two Years Old. *Web-site of the We the People*. URL: https://www.whitehouse.gov/.

Пекарський С.П. - доцент кафедри спеціальних дисциплін та професійної підготовки факультету № 2 Донецького юридичного інституту МВС України, кандидат юридичних наук

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКА ПРИ ВИКОРИСТАННІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ОСВІТНЬОМУ ПРОЦЕСІ

Розвиток правоохоронних органів характерний упровадженням інформаційних технологій у діяльність підрозділів Національної поліції України і закладів вищої освіти в яких здійснюється підготовка майбутніх поліцейських. Це відкриває широкі перспективи для використання інформаційних технологій в освітньому процесі закладів вищої освіти зі специфічними умовами навчання, які входять до сфери управління МВС України. Своєю чергою статтею 3 Закону України «Про інформацію» визначені основні напрями державної інформаційної політики, одним із яких є забезпечення інформаційної безпеки України [1]. Саме тому дане положення необхідно враховувати в процесі освітньої підготовки поліцейських, зокрема під час вивчення спеціальних дисциплін де розглядаються питання, пов’язані з державною таємницею [2].

Безперечно практика протидії злочинності охоплює окремі відомості, що становлять державну таємницю. Звідом відомостей, що становлять державну таємницю, який затверджений наказом СБУ від 12.08.2015 № 440 (зі змінами і доповненнями на 17.09.2019) [3], та є єдиною формою реєстрації відомостей

що становлять державну таємницю в Україні, визначені також і відомості, які відносяться до сфери державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці і тому такі відомості підлягають охороні державою. Саме тому Законом України «Про державну таємницю» та іншими виданими відповідно до нього нормативно-правовими актами встановлено єдиний порядок забезпечення охорони державної таємниці, під яким розуміється режим секретності [2]. Своєю чергою правові відносини щодо забезпечення дотримання режиму секретності та охорони державної таємниці вивчаються навчальною дисципліною «Режим секретності». Тому приходимо до висновку, що метою викладання навчальної дисципліни «Режим секретності» є набуття здобувачами освіти основних знань та виробки умінь та навичок щодо:

- правових основ, сутності та особливостей єдиного порядку забезпечення охорони державної таємниці в державі;
- визначення заходів щодо забезпечення режиму секретності;
- методики віднесення інформації до державної таємниці;
- здійснення дієвого контролю за забезпеченням охорони державної таємниці;
- формування вмінь та навичок щодо порядку організації секретних робіт;
- допуску та доступу осіб до секретних робіт та документів, роботи з матеріалами обмеженого грифу користування, дотримання вимог перебування у режимних приміщеннях;
- обов'язків та обмежень прав громадян, яким надано допуск і доступ до державної таємниці, забезпечення умов їх роботи;
- відповідальності працівників органів, установ, підприємств, підрозділів, які допущені до державної таємниці тощо.

На нашу думку даний аспект необхідно враховувати у процесі підготовки навчальної літератури для дисциплін, які вивчають питання, пов'язані зі збереженням державної таємниці та дотримання режиму секретності в практичній діяльності підрозділів Національної поліції України. Саме тому, на виконання вимог наказу МВС України від 14.02.2008 № 62 «Про затвердження положення про вищі навчальні заклади МВС» [4], з метою підвищення якості навчання зі спеціальних дисциплін, рівня підготовки фахівців для підрозділів Національної поліції України необхідно створювати, розвивати та впроваджувати навчально-методичне забезпечення, навчальні посібники, підручники у освітній процес (дотримуючись при цьому вимог, що висуваються до збереження державної таємниці) й розповсюджувати передові інформаційні технології та результати наукових досліджень серед практичних підрозділів як Національної поліції України так і МВС у цілому.

Також протягом навчання здобувачі вищої освіти - майбутні працівники поліції, особливо підрозділів кримінальної поліції та органів досудового розслідування вивчають спеціальну літературу, відповідні нормативні акти які

не підлягає широкому розповсюдженню. Ця інформація стосується окремих форм, методів, прийомів і результатів діяльності поліції, щодо розв'язання завдань протидії злочинності, зміцнення правопорядку і відноситься законодавством до категорії державної таємниці. Розголошення, втрата такого роду інформації, а також відомостей про заходи, які плануються і здійснюються поліцією щодо забезпечення особистої та публічної безпеки і боротьби зі злочинністю, порушують її нормальну діяльність, що значно знижує її ефективність.

Також організація освітнього процесу у закладах вищої освіти зі специфічним умовами навчання, які входять до сфери управління МВС України вимагає впровадження наукових розробок, які можуть бути доступними для здобувачів вищої освіти (курсантів, слухачів) та сприятимуть поліпшенню результатів самостійної роботи курсантів чи слухачів під час вивчення спеціальних навчальних дисциплін. Тому приходимо до висновку про необхідність дотримуватися вимог законів України, нормативних актів, які регламентують порядок роботи з інформацією, що має обмежений гриф доступу під час наукових досліджень, підготовки навчальних посібників, підручників з питань охорони державної таємниці. Це знайшло відображення в наказі МОН України від 23.09.2019 № 1220 «Про опублікування результатів дисертацій на здобуття наукових ступенів доктора і кандидата наук», яким затверджені: «Вимоги до опублікування результатів дисертацій на здобуття наукових ступенів доктора і кандидата наук» та «Вимоги до опублікування монографії що подається на здобуття наукових ступенів доктора і кандидата наук» [5]. Відповідно до наведеного, Міністерством освіти та науки України визначено, що основні наукові результати дисертації на здобуття наукових ступенів доктора і кандидата наук, яка містить державну таємницю, висвітлюються у наукових публікаціях, у тому числі призначених для опублікування матеріалів, що містять державну таємницю, відповідно до законодавства [5, п. 3]. Саме тому приходимо до висновку, про необхідність суворого дотримання вимог законодавства України при проведенні наукових досліджень до об'єкту яких відносяться суспільні відносини, які регламентують режим секретності та охорону державної таємниці.

Підводячи підсумок зазначаємо, що в даному дослідженні нами визначені загальні питання забезпечення інформаційної безпека при використанні інформаційних технологій в освітньому процесі.

Використані джерела:

1. Про інформацію : Закон України від 2 жовтня 1992 р. № 2657-XII [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/ 2657-12;
2. Про державну таємницю : Закон України від 21 січня 1994 р. № 3855-XII [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/ 3855-12#n38;
3. Про затвердження Зводу відомостей, що становлять державну таємницю: наказ СБУ від 12.08.2015 № 440 (зі змінами і доповненнями на 17.09.2019) [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/ laws/show/z0902-05;
4. Про затвердження положення про вищі навчальні заклади МВС: наказ МВС України

від 14 лютого 2008 р. № 62 [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/z0193-08;
5. Про опублікування результатів дисертацій на здобуття наукових ступенів доктора і кандидата наук: наказ Міністерства освіти та науки України від 23.09.2019 № 1220 [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/z1086-19

Прокопов С.О. - старший викладач кафедри економічної та інформаційної безпеки (Дніпропетровський державний університет внутрішніх справ)

УДОСКОНАЛЕННЯ ІНФОРМАЦІЙНО-ТЕХНІЧНОЇ ПЛАТФОРМИ ПРОФЕСІЙНО-ДІЛОВОЇ ГРИ «ЛІНІЯ 102»

Більше трьох років пройшло з впровадження в навчальний процес Дніпропетровського державного університету внутрішніх справ професійно-ділової гри «Лінія -102» [1]. За цей період розробка фахівців ДДУВС набула всеукраїнських масштабів, вона запрацювала у всіх навчальних закладах системи Міністерства внутрішніх справ. З метою покращення опанування можливостями інформаційно-технічної платформи професійно-ділової гри «Лінія 102» фахівцями та курсантами поліцейських навчальних закладів викладачами кафедри економічної та інформаційної безпеки були розроблені «Інтерактивні методичні рекомендації інформаційно-технічної платформи професійно-ділової гри «Лінія 102» [2]. Детальному ознайомленню з інтерактивними методичними матеріалами присвячена ця доповідь.

Інтерактивні методичні рекомендації інформаційно-технічної платформи професійно-ділової гри «Лінія 102» розміщені на веб-вузлі 102.dduvs.in.ua (рис. 1), доступ до якого мають всі поліцейські навчальні заклади.

Рис. 1.

Для входження до загальної сторінки Інтерактивні методичні рекомендації інформаційно-технічної платформи професійно-ділової гри «Лінія 102» необхідно натиснути виділену на рис. 1 кнопку у вигляді навушників. Ми попадаємо у загальне меню інтерактивних методичних рекомендацій (рис. 2):

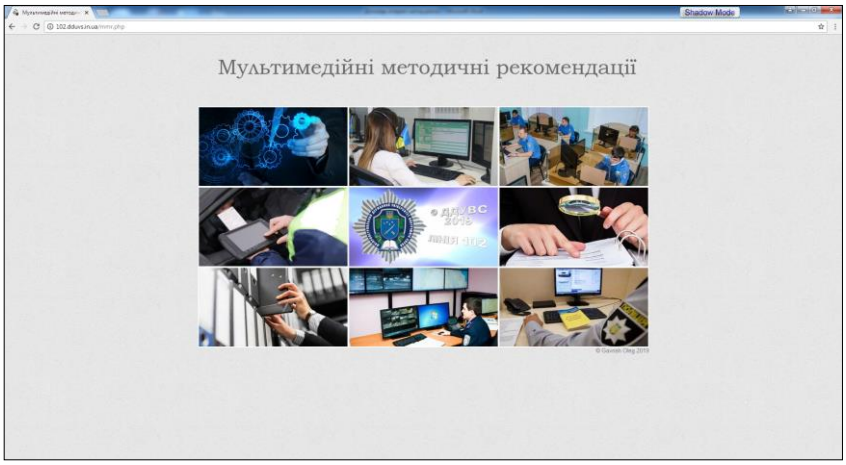


Рис. 2.

На загальному меню розміщені вісім активних іконок. Для ознайомлення з загальними можливостями інформаційно-технічної платформи професійно-ділової гри «Лінія 102» необхідно натиснути крайню ліву іконку (рис. 3):

Рис. 3.

Меню загальні положення має наступний вигляд (рис. 4):

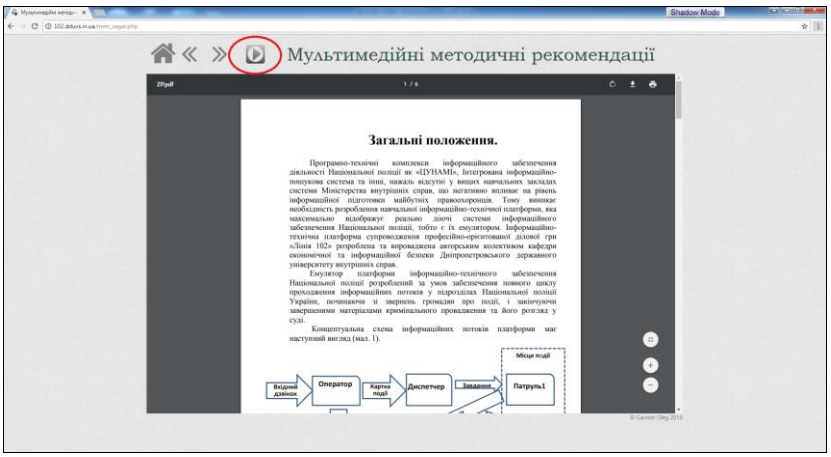


Рис. 4.

В автоматичному вигляді випадає текстова інформація про загальну побудову інформаційно-технічної платформи професійно-ділової гри «Лінія 102», але якщо натиснуту виділену на рисунку кнопку «плей», запуститься навчальний відеоролик з закадровими роз'ясненнями роботи інформаційної системи (рис 5):

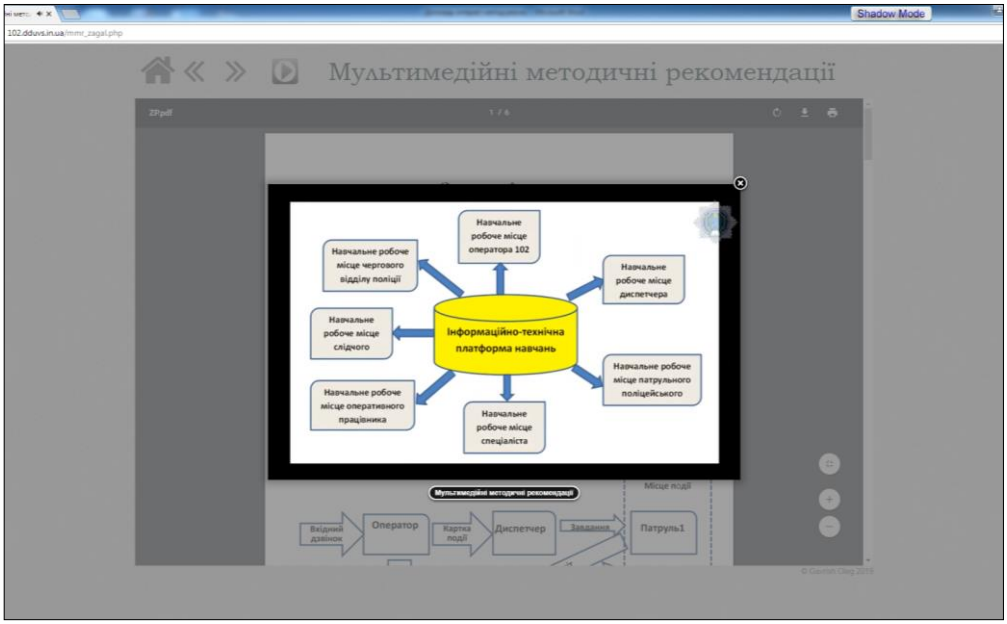


Рис. 5.

Аналогічно працюють інші 7 іконок активації інтерактивних методичних матеріалів навчальних робочих місць оператора 102, диспетчера, патрульного поліцейського, чергового відділу поліції, оперативного працівника, слідчого, спеціаліста-криміналіста.

Розміщення на сайті інформаційно-технічної платформи професійно-ділової гри «Лінія 102» інтерактивних методичних матеріалів дозволить швидше та більш ефективніше використовувати можливості навчальних робочих місць при проведенні тренінгів з використанням квест-технологій.

Використані джерела:
1. Гавриш О.С., Махницький О.В., Прокопов С.О. Інформаційно-технічна платформа інтерактивного комплексу з підготовки здобувачів вищої освіти та практичних працівників Національної поліції в ДДУВС/ Наукова стаття. Науковий журнал Право і суспільство. – 2017. – № 1-1. – С. 128–141.
2. Гавриш О.С., Махницький О.В., Прокопов С.О., Рижков Е.В. Інтерактивні методичні рекомендації. ДДУВС- 2019. [Електронний ресурс] – Режим доступу http://102.dduvs.in.ua/mmr.php.

Рижков Е.В. – завідувач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ, кандидат юридичних наук, доцент

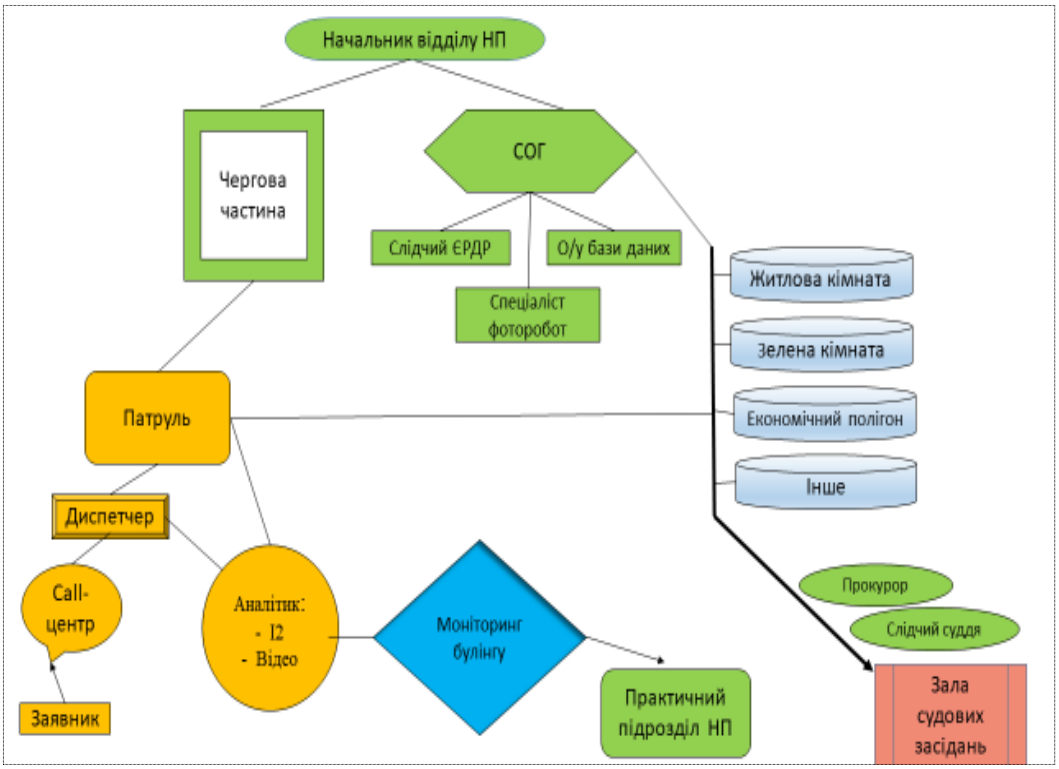
ПЕРСПЕКТИВИ РЕАЛІЗАЦІЇ МОНІТОРИНГОВИХ ФУНКЦІЙ У ПРОЕКТІ «ЛІНІЇ-102» ІНСТРУМЕНТАМИ КРИМІНАЛЬНОГО АНАЛІЗУ

Пошук сучасних методик навчання у спеціалізованих закладах МВС формує нову тенденцію щодо залучення здобувачів до виконання практичних завдань. З урахуванням спеціалізації ВНЗ, технічних та інших можливостей педагогічні колективи намагаються збільшити практичну складову навчального процесу, як у основний час – через внесення змін до робочих програм навчальних дисциплін так і поза навчальний час – у факультативній формі.

Така робота, наприклад, проводиться у Харківському національному університеті внутрішніх справ та Одеському державному університеті внутрішніх справ, де курсантів залучають до моніторингових функцій у соціальних мережах та використовують чат-боти щодо виявлення протиправних дій, пов’язаних із незаконним збутом наркотичних речовин. Враховуючи певний проміжок часу педагогічні колективи досягли в цьому питанні певних успіхів. Має свій певний досвід і Дніпропетровський державний університет внутрішніх справ. Так у 2017-2018 навчальному році за власною ініціативою кафедри економічної та інформаційної безпеки було започатковано кіберфакультатив, мета кого полягала у підвищенні комп’ютерної обізнаності здобувачів. У 2018-2019 році кафедрою оперативно-розшукової діяльності було започатковано факультатив з кримінального аналізу, який проводився за активної участі практичних працівників відповідного відділу ГУНП.

Слід зазначити, що в умовах дефіциту навчального часу такі форми поза навчального здобутку знань та навичок є реальним джерелом підвищення фаховості майбутніх випускників. Проте за умов відсутності належної організаційної форми такі новаторські підходи до співпраці зі здобувачами мають

короткотривалий позитивний ефект. З метою закладання довготривалого фундаменту у розвиток педагогічних новацій бажано створення міждисциплінарних та міжкафедральних утворень. Позитивним прикладом такої форми є Лінія-102, яка розроблена та функціонує в університеті з 2016 року і яка за рішенням керівництва відповідного Департаменту МВС з 2018 року є обов'язковою для використання в навчальному процесі всіх інших навчальних закладів зі специфічними умовами навчання. Вона дозволяє використання свого потенціалу як в повному обсязі (див. схему) так і сегментарно (за окремими темами, окремими навчальними дисциплінами, окремими кафедрами).



Маючи необмежений потенціал до подальшого вдосконалення Лінія-102 дозволяє доповнювати базовий комплект функцій окремими модулями з урахуванням спеціалізації кожного з навчальних закладів. Реалізацію таких додатковий модулів та додаткового функціоналу платформи, на нашу думку, повинна відбуватись в процесі вирішення здобувачами нових навчальних фабул максимально наближених до реальних, в тому числі методом поліцейського квесту. Більш того, з огляду на останні тенденції та набутий педагогічними колективами досвід та потенційні можливості, які надають інформаційні інструменти, в тому числі інструменти кримінального аналізу, можна стверджувати, що маємо поступовий перехід від суто навчальних фабул до відпрацювання реальних ситуацій.

Суть такої роботи полягає в першу чергу у моніторингу відкритих джерел за конкретно визначеним сегментом суспільних відносин (явищами, суб'єктами та інш.), пошук первинної інформації щодо відповідної групи про-

типравних діянь, їх правова ідентифікація (кваліфікація), первинна перевірка і доповнення у законний спосіб без перебільшення допустимого статусу здобувачами та подальше направлення набутих відомостей до відповідних практичних підрозділів Національної поліції. Важливим аспектом правової безпеки при цьому недопущення здобувачами дій провокаційного характеру та виконання функцій суб'єктів слідчої чи оперативно-розшукової діяльності.

Конкретними засобами організації вказаної діяльності можуть виступати авторські програмні розробки (за прикладом навчального ЄРДР від ХНУВС, Лінія-102 (ЦУНАМІ) від ДДУВС), автоматизовані робочі місця (наприклад, АРМ «Ювенал»), спеціалізовані чат-боти (наприклад, @get_kontakt_bot, @smart_searchbot, @OpenDataUABot, @HowToFind_bot, @storebot, @mailsearchbot, @whoisdombot, @UAFind_bot, @tavk_bot, @temp_mail_bot), інше спеціалізоване програмне забезпечення кримінального аналізу (наприклад, IBM i2 Analyst's Notebook, IBM i2 iBase та IBM i2 iBridge), а також такі форми навчання як факультативи, тренінги, змагання та позанавчальна практика.

Сучасна інформаційна реальність суспільного життя, характер скоєння протиправних діянь, тотальна діджиталізація та перехід розвинутих держав до інформативно-аналітичного підходу протидії злочинності в повній мірі обумовлює перехід навчального процесу підготовки правоохоронців на таку саму модель, де є місце для педагогічної творчості, партнерських взаємовідносин зі здобувачами вищої освіти та працівниками практичних підрозділів у справі формування дієвого резерву майбутніх фахівців у цій сфері.

Рижкова С.А. - інспектор сектору превенції Шевченківського ВП Дніпровського ВП ГУНП в Дніпропетровській області

ВИКОРИСТАННЯ ЧАТ-БОТІВ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ ЯК ІНСТРУМЕНТ ПОБУДОВИ ПАРТНЕРСЬКИХ ВІДНОСИН З НАСЕЛЕННЯМ

Відповідно до ст. 11 Закону України «Про Національну поліцію», діяльність поліції здійснюється в тісній співпраці та взаємодії з населенням, територіальними громадами та громадськими об'єднаннями на засадах партнерства і спрямована на задоволення їхніх потреб. Важливим в цьому аспекті є побудова партнерських відносин на рівні довіри між населенням та поліцією в цілому, де сторони зацікавлені в безпечному середовищі [1].

Слід зазначити, важливим в цьому напрямку відіграє конструктивний комунікативний аспект взаємодії між громадянами та поліцією, який досягається різними методами, це і проведення профілактичної, роз'яснювальної

роботи серед населення щодо неприпустимості протиправної поведінки; спільна діяльність громадян (громадських формувань) та поліції, яке має на меті – забезпечення публічного порядку та публічної безпеки; інформування громадянами правоохоронні органи про відомі їм факти скоєння правопорушень, тощо. Тобто комунікативний аспект (обмін інформацією, яка представляє в тому числі оперативний інтерес) між населенням та поліцією є досить вагомим фактором, який є запорукою ефективної роботи органів та підрозділів Національної поліції в цілому.

Проте слід зазначити, з розвитком інформаційних технологій, збільшенням користувачів мережі Інтернет, створення соціальних мереж, окрім «традиційних» комунікативних засобів діалогу між представниками громадськості та поліції, поступово формується нова філософія діалогу та взаємодії між населенням та поліцією, яка трансформується в інформаційно-комунікаційну площину, мова йде про використання чат-ботів, як платформу нових можливостей створення умов для комунікації та співпраці громадян та поліції.

Чат-бот **(**англ. chatbot) − комп'ютерна програма, розроблена на основі нейромереж та технологій машинного навчання, яка веде розмову за допомогою слухових або текстових методів [2]. Термін «ChatterBot» вперше вжив Майкл Маулдін (творець першого Вербота, Julia) у 1994 році, щоб описати ці розмовні програми. З ростом популярності месенджерів в 2010-х чат-боти знайшли нове життя. Більшість працює на платформах популярних месенджерів: Facebook Messenger, Telegram, Viber, ВКонтакті, Skype, Slack. Сьогодні чат-боти є частиною віртуальних помічників, і доступні через програми багатьох організацій, веб-сайти та платформи обміну миттєвими повідомленнями. Боти можуть працювати в вигляді додатків або бути вбудованими в функціонал пошукових систем. Чат-бот використовують для досягнення якої-небудь мети (наприклад, надання потрібної інформації). Чат-боти – це програмні продукти, які симулюють людське спілкування в месенджерах, тобто коректно зроблений віртуальний помічник, заточений під конкретну мету, вміє вирішувати буквально будь-які завдання, доступні людині [3].

Одним із перших і найбільш відомим юридичним ботом лишається сервіс DoNotPay. Сервіс, розроблений 18-річним Джошуа Браудером, допомагає підготувати заяву про апеляцію на штраф за порушення паркування в Лондоні. Складаючи заяву за лічені хвилини, бот виявився поза конкуренцією у порівнянні з дорогими англійськими юристами і за перші півроку допоміг оскаржити понад 160 тисяч штрафів. Сьогодні бот, окрім Великої Британії, працює також у семи великих містах США.

На сьогодні прикладів використання юридичних чат-ботів багато. Їх функціонал дуже широкий – пошук інформації в державних реєстрах, надання юридичних консультацій, підготовка юридичних документів, оплата штрафів і зборів та багато іншого. На світовому юридичному ринку працюють і більш просунуті автоматичні системи, які шукають юридичні ризики в контрактах (LawGeex, ThoughtRiver, Legal Robot), роблять юридичний аналіз

контракту (Seal, Luminance, Kira Systems), роблять інтелектуальний пошук по судовій практиці і законодавству (Judicata, Casetext, ROSS Intelligence) або допомагають з реєстрації інтелектуальної власності (TrademarkNow, PatentBot) [4].

Отже, зупинимось саме на використанні чат-ботів в діяльності Національної поліції та чат-можливостей, які допомагають в роботі.

Фахівці Харківського національного університету внутрішніх справ створили чат-бота, за допомогою якого користувачі соціальної мережі «Telegram» зможуть блокувати інтернет-магазини, які продають наркотики [5].

Працівники Національної поліції в Сумах запустили Telegram-чат «Безпечне місто Суми». Користувачами чату є вже понад п'ять тисяч людей, серед яких і працівники патрульної поліції, і надзвичайних служб, і голови ОСББ, і просто містяни.. До речі, такий Telegram-чат «Безпечне місто» є у м. Кропівницькому. Подібні чати також існують в Ужгороді, Рівному, Мукачевому та Вінниці. Зазначимо, що в цьому випадку був створений не Telegram-бот, а саме Telegram-чат, основним аргументом на користь такої форми є те, що на думку розробників кожен випадок індивідуальний і дуже важко зробити бота, який би відповідав усім запитам. На користь запровадження саме чату, є той факт, що всю інформацію, яка надходить, обробляє людина-адміністратор, вивчає зміст повідомлень цілодобово та відпрацьовує матеріал. Ще однією превагою у такій комунікації є можливість залишити інформацію анонімно, тобто змінити ім'я та налаштувати функцію приватності. Вдень у чаті працює адміністратор, а вночі його моніторить працівник чергової частини. Працівник поліції (чергової частини) ознайомлюється з інформацією у чаті, та робить первинну кваліфікацію, з'ясовуючи при цьому - чи належить подія до компетенції поліції чи до компетенції іншої структури. І якщо питання не підвідомче Національній поліції, повідомлення передається до відповідної служби. У чаті 100% усього складу патрульної поліції і коли наряд їде на виклик, вони вже мають певну поінформованість завдяки фотографіям та іншим відомостям, мають відповідне орієнтування щодо пошуку маршруту та певних осіб, або мають можливість зателефонувати особі (заявнику) через Telegram. Якщо людина налаштована на розмову з представниками поліції, є можливість встановити деталі події. Після створення зазначеного чату, патрульні поліцейські Сум, констатують збільшення звернень до поліції, в тому числі реагування на адміністративні правопорушення у сфері безпеки дорожнього руху, порушення правил паркування транспортних засобів, порушення правил тиші у нічній час, а також надання допомоги особам, які потребують поліцейського піклування [6].

Досить цікавим є той факт, що не тільки створення чат-ботів є ініціативою Національної поліції, слід зазначити, що й громадяни виступають ініціаторами такої діяльності, що в тій чи іншій мірі допомагає роботі поліції. Досвід роботи Олександра Харченко, який раніше працював у патрульній поліції, надихнув його на створення Telegram-бота «БамперБот», метою якого є

алгоритм дій для водіїв, які потрапили у ДТП. В залежності від ситуації, в якій опинився водій, бот допоможе скласти європротокол, надасть поради, як спілкуватися з поліцією. Таким чином, Telegram-бот «БамперБот» підвищує рівень правової обізнаності громадян та допомогає в роботі патрульній поліції [7].

Ще приклад ініціативи громадського активіста з Івано-Франківщини Богдана Пашковського, в створенні телеграм-платформи #ifpolice у мережі Телеграм створено @ifpolice_bot - це Бот Головного Управління Національної поліції в Івано-Франківській області. Ботова сторінка прикріплена до чату «Франківськ 112», де часто з тими чи іншими проблемами звертаються прикарпатці або ж повідомляють про проблеми на дорогах області та інші правопорушення. Відтак: 1) поліція реагує на важливі повідомлення через Бота; 2) надсилає важливу інформацію у «Франківськ 112» від імені Бота; 3) кожен можете зв'язатися з поліцією у Телеграмі, написавши Боту приватне повідомлення. При цьому завжди пріоритетною залишається «Лінія 102» [8].

Таким чином, в контексті взаємодії поліції з населенням, суб'єктами ініціативи створення чат-ботів належить як працівникам Національної поліції так і громадянам. За метою призначення чат–боти можуть використовуватись для:

1. підвищення рівня правової свідомості громадян, у взаємодії з поліцією;
2. протидії, моніторингу в соціальних мережах фактів кібербулінгу, торгівлі наркотичними засобами, поширення інформації сексуального характеру, тощо;
3. оперативного реагування на заяви та повідомлення громадян органами та підрозділами Національної поліції (можливість мати доступ до відео, фото фіксації тієї чи іншої події);
4. надання юридичних консультацій, підготовка юридичних документів, оплата штрафів і зборів, тощо.

Використані джерела:

1. Про Національну поліцію: Закон України від від 02.07.2015 № 580-VIII. Відомості Верховної Ради. 2015 № 40-41. Ст.379. URL: https://zakon.rada.gov.ua/laws/show/580-19.
2. Чат-боты. Что это и зачем нужно бизнесу? URL:https://shcherbakovs.com/chat-bots-whatisit-and-whyyouneedit/.
3. Дрокіна Н.І. Роль чат-ботів в месенджерах для забезпечення ефективності маркетингових комунікацій: Актуальні питання економічних наук: міжнародна науково-практична конференція, м. Київ, 28-29 вересня 2018 р.: Херсон, 2018.С.99- с.102
4. Legal Tech. Боти vs юристи. URL:https:// evris.law/uk/stattja-legal-tech-boti-vs-juristi/
5. В Харькове создали чат-бот для блокировки интернет-ресурсов по продаже наркотиков. URL:https://www.city.kharkov.ua/ru/news/u-kharkovi-stvorili-chat-bot-dlya-blokuvannya-internet-resursi
6. Сумська поліція створила Telegram-чат: як він працює і що туди пишуть. URL:https://cukr.city/city/2019/telegram-chat-police-sumy
7. Киевский экс-полицейский запустил Telegram-бота с подсказками, что делать при ДТП. URL:https://ain.ua/2017/08/30/telegram-bot-na-sluchaj-dtp/
8. Поліція відзначила активіста за допомогу в створенні телеграм-платформи #ifpolice URL: https://galychyna.if.ua/2019/01/15/politsiya-vidznachila-aktivista-za-dopomogu-v-stv

Рудий Т.В. – доцент кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів Львівського державного університету внутрішніх справ, кандидат технічних наук, доцент;
Зачек О.І. – доцент кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів Львівського державного університету внутрішніх справ, кандидат технічних наук, доцент

СУЧАСНИЙ ПІДХІД ДО ВИКОРИСТАННЯ ТЕХНОЛОГІЙ КРИМІНАЛЬНОГО АНАЛІЗУ У ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Сучасні виклики і загрози, перш за все гібридні, які обумовлені впливом комплексу політичних, економічних, правових, технологічних чинників вимагають системного реагування, адекватної трансформації як усього сектору безпеки, так і інформаційної та кібербезпеки зокрема, а також включення цієї системи у сферу політичних пріоритетів держави. Під впливом глобалізаційних процесів, розвитку інформаційних технологій (ІТ), телекомунікаційних сервісів, цифрової економіки інформаційна та кібербезпека набувають самостійного, трансдержавного характеру.

Розвиток та безпека інформаційного і кіберпростору, запровадження цифровізації процесів урядування, гарантування безпеки й сталого функціонування інформаційно-комунікаційних систем, державних інформаційних ресурсів мають бути складовими державної політики у сфері розвитку інформаційного простору та становлення інформаційного суспільства в Україні.

Проте, ціла низка проблем, які стосуються організації, взаємодії і координування роботи правоохоронних органів, розроблення сучасних систем інформаційно-аналітичного забезпечення, автоматизованих інструментальних засобів кримінального аналізу, які працюють у режимі реального часу ще потребують глибокого вивчення [1].

Актуальною і першочерговою для розв’язання залишається проблема недосконалості національного законодавства і відсутності єдиної правової бази правоохоронних органів у протидії кіберзлочинності. Законодавство України у безпековій сфері не визначає загальні фреймові (рамкові) підходи та визначення, а деталізує часткові, покрокові рішення, що пояснюється низьким рівнем знань у галузі ІТ, теорії інформаційної та кібернетичної безпеки як керівництва держави, політичних діячів, так і конкретних виконавців, а найголовніше – відсутність дієвого, ефективного загальнодержавного підходу до протидії кіберзлочинності [2, 3].

Законодавча база – важлива складова, але уже настав час перейти від слів до дій з огляду на те, що основним недоліком чинного законодавства у

безпековій сфері є його пасивний характер – декларується лише необхідність забезпечення кібербезпеки та протидії кіберзлочинності на рівні доктрин, указів, рішень тощо. Зокрема, на організаційно-правовому рівні необхідно чітко ідентифікувати проблему протидії кіберзлочинності, визначити основні загрози в сфері кібербезпеки.

З огляду на викладене виникла нагальна необхідність у реорганізації та вдосконаленні методів протидії кіберзлочинності. Одним із засадничих підходів стосовно застосування сучасних технологій у сфері протидії кіберзлочинності на якісно новому рівні є кримінальний аналіз.

Даючи кримінологічну характеристику кіберзлочинів треба визнати, що більшість виявлених кіберзлочинів розпорошені у звітності різних підрозділів Національної поліції України (НПУ) і це не дає можливості провести комплексний аналіз та характеристику кіберзлочинності.

Тому, власне, одним із головних завдань кримінального аналізу, на рівні взаємодії з іншими силовими структурами держави, які забезпечують протидію кіберзлочинності, є перехід від процесу ситуативних відносин до чіткої та зрозумілої системи їх взаємодії на основі консолідації усіх розрізнених джерел оперативної інформації з подальшим глибоким аналізом для прийняття обґрунтованих управлінських рішень на усіх керівних рівнях.

Застосування технологій інформаційно-аналітичної діяльності (ІАД) та відповідних інформаційно-аналітичних систем (ІАС) дозволить структурувати наявні інформаційні ресурси і використовувати їх як моделі консолідованої інформації. Головним аспектом функціонування ІАС є переорієнтація з версій різних систем управління базами даних на вищий якісний рівень, який дозволяє виконувати аналітичні експертні дії.

У цьому зв'язку кожна ІАС створюється і розробляється з урахуванням наступних вимог: одержання розрізнених даних з багатьох джерел одночасно; акумулювання даних і створення масивів баз даних, використання технологій пошуку та індексації; для кожного з користувачів у режимі реального часу організовано надання необхідної інформації для прийняття рішень, виконання конкретних заходів, здійснення певних дій; підготовка регулярної та планової оцінки різних станів об'єктів управління на основі використання інструментів інтелектуального і оперативного аналізу; подання усієї інформації і результатів її аналізу у строго впорядкованій формі для ефективного сприйняття даних користувачами усіх рівнів.

Аналітична інформація повинна відповідати наступним якісним характеристикам: цінність (корисність); точність; достовірність; повнота; оперативність; коректність.

Базовими елементами та засобами реалізації ІАД виступають ІАС – системи зв'язку та трансмісії даних, інформаційно-телекомунікаційна інфраструктура, бази даних правової інформації, технічні, програмні, лінгвістичні, правові, організаційні засоби. Згадані аспекти відтворені у статтях 25, 26, 27 Закону України ″Про Національну поліцію″ [4]. У сою чергу технологічна платформа ІАС дозволяє здійснювати інтегрування та координування дій між рі-

зними підрозділами НПУ. У практиці кримінального аналізу розрізняють наступні типи аналітичних продуктів [5]:

1. Аналітичний звіт: сепарована інформація з внутрішніх і зовнішніх джерел; висновки; рекомендації, прогнози, настанови; додаткові матеріали (графіки, схеми, дані геолокації).
2. Профіль (досьє) особи, об'єкта: максимальний обсяг інформації на об'єкт аналізу у відповідності до запиту ініціатора.
3. Інформаційне зведення: оброблені табличні дані шляхом вибірки з баз даних за критеріями ініціатора.
4. Витяг інформації: вибірка інформації з баз даних за критеріями ініціатора.

Отже, від того, якою мірою підрозділи кримінального аналізу НПУ спроможні якісно аналізувати наявну інформацію і, як результат, надавати аналітичні продукти, які є підтримкою для прийняття адекватних кіберзагрозам управлінських рішень, залежить успіх виконання поставлених завдань.

На останок, як висновок, на думку авторів успішне реалізування та впровадження технологій кримінального аналізу дасть можливість активно використовувати ІАД, що сприятиме підвищенню ефективності протидії кіберзлочинності.

Використані джерела:

1. Стратегія розвитку системи Міністерства внутрішніх справ України до 2020 року. Електронний ресурс. Шлях доступу: https://www.cyberpolice.gov.ua/strategy-2020/.
2. Рудий Т. В. Організаційно-правовий супровід захисту інформаційних систем підрозділів національної поліції України на основі міжнародних стандартів / Т.В. Рудий, О. В. Захарова, В. В. Сеник, С. В. Сеник, М. І. Ізьо // Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична / головний редактор Р. І. Благута. – Львів: ЛьвДУВС, 2017. – Вип. 2. – С. 213-225.
3. Проблеми чинної вітчизняної нормативно-правової бази у сфері боротьби з кіберзлочинністю: основні напрями реформування. Аналітична записка. Національний інститут стратегічних досліджень. Електронний ресурс. Шлях доступу: http://www.niss.gov.ua/articles/454/.
4. Закон України ″Про Національну поліцію″ / Відомості Верховної Ради України, 2015, №40-41. – С. 379 // Електронний ресурс. Шлях доступу: http://zakon3.rada.gov.ua/laws/show/580-19.
5. Кримінальний аналіз у діяльності НПУ / Концепції впровадження в Національній поліції України моделі поліцейської діяльності, керованої аналітикою ″Intelligence Led Policing″ // Електронний ресурс. Шлях доступу: www.slideshare.net/NationalPolice/ss-75925350.

Саркісян В. М. - аспірант кафедри державно-правових дисциплін Луганського державного університету внутрішніх страв ім. Е. О. Дідоренка

ВИКОРИСТАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У РАМКАХ ЗДІЙСНЕННЯ ГРОМАДСЬКОГО КОНТРОЛЮ ЗА НАЦІОНАЛЬНОЮ ПОЛІЦІЄЮ ПІД ЧАС ПРОВЕДЕННЯ ВИБОРІВ В УКРАЇНІ

Сучасне демократичне урядування важко уявити без використання під час його здійснення різного роду інформаційних технологій, які серед іншого все помітніше проникають у практику підготовки та проведення виборів в Україні, на що вже неодноразово зверталася увага в науковій та навчальній літературі [1-6]. Соціальні мережі, месенджери, електронні петиції, електронні опитування, розміщення та поширення політичної реклами на відеохостингах, проведення виборчої кампанії кандидатами та політичними партіями в мережі «Інтернет» все це є неодмінною ознакою сучасних демократичних та конкурентних виборів. Відтак вкрай важливим аспектом у цьому питанні є використання сучасних інформаційних технологій у рамках здійснення громадського контролю за Національною поліцією під час проведення виборів в Україні.

Основною метою використання сучасних інформаційних технологій у рамках здійснення громадського контролю за Національною поліцією під час проведення виборів в Україні є забезпечення політичної нейтральності діяльності Національної поліції за рахунок упередження її втягнення у виборчу боротьбу на боці певного кандидата або політичної партії, які приймають участь у виборах, а також сприяння поінформованості Національної поліції про виявлені громадськістю факти порушень виборчого законодавства України та більш активного і об'єктивного реагування поліції на ці порушення.

Одним з ключових моментів у проведенні реформи поліції в Україні є посилення ролі громадського контролю в діяльності поліції. Наочним підтвердженням цьому є суттєве приділення уваги взаємодії поліції та громадськості в Законі України «Про Національну поліцію» від 2 липня 2015 року № 580-VIII. Зокрема, у цьому Законі серед іншого встановлюються наступні засади громадського контролю в діяльності поліції: 1) поліція здійснює свою діяльність на засадах відкритості та прозорості в межах, визначених Конституцією та законами України (ч. 1 ст. 9); 2) поліція забезпечує постійне інформування органів державної влади та органів місцевого самоврядування, а також громадськості про свою діяльність у сфері охорони та захисту прав і свобод людини, протидії злочинності, забезпечення публічної безпеки і по-

рядку (ч. 2 ст. 9); 3) з метою інформування громадськості про діяльність поліції керівник поліції та керівники територіальних органів поліції раз на рік готують та опубліковують на офіційних веб-порталах органів поліції звіт про діяльність поліції (ч. 1 ст. 86) [7].

Водночас у Законі України «Про Національну поліцію» наводяться загальні засади здійснення громадського контролю за Національною поліцією, тоді коли використання сучасних інформаційних технологій у рамках здійснення громадського контролю за Національною поліцією під час проведення виборів в Україні має свій особливий характер, що у першу чергу обумовлено конституційно-правовою специфікою здійснення виборчого процесу на виборах в Україні [8-10]. Суттєво полегшує використання сучасних інформаційних технологій у рамках здійснення громадського контролю за Національною поліцією під час проведення виборів в Україні відкритість та прозорість діяльності поліції, а також доступність для громадськості різного роду реєстрів та інформаційних ресурсів, розпорядником яких є Національна поліція та Міністерство внутрішніх справ України.

У якості позитивного прикладу підвищення прозорості діяльності Національної поліції під час проведення виборів в Україні слід назвати введення у дію на передодні чергових виборів Президента України 2019 року інформаційно-аналітичної системи «Вибори-2019». Зазначена система є геоінформаційним аналітичним порталом МВС України, який призначений для моніторингу здійснення правопорушень для відображення публічної інформації про стан громадської безпеки. Портал МВС дає можливість: 1. На базі геоінформаційної системи вести моніторинг в режимі реального часу здійснених правопорушень виборчого процесу: Адміністративних правопорушення виборчого законодавства; Кримінальних правопорушення виборчого законодавства; Некласифікованих порушення виборчого законодавства; Інших подій, що порушують виборчий процес. 2. Оприлюднення та візуалізації деперсоніфікованих подій [11].

При здійсненні громадського контролю за Національною поліцією під час проведення виборів в Україні громадськість найбільше цікавлять наступні питання: 1) стан готовності Національної поліції щодо забезпечення публічної безпеки і порядку під час проведення виборів в Україні; 2) загальний стан криміногенної обстановки під час проведення виборів в Україні; 3) кількість звернень, які надійшли до органів Національної поліції щодо порушень виборчого законодавства України та результати їхнього розгляду; 4) кількість та характер порушень виборчого законодавства України, які були виявлені співробітниками Національної поліції; 5) заходи, які вже вжиті або будуть здійсненні щодо недопущення порушень виборчого законодавства України; 5) стан реагування керівництва Національної поліції щодо скарг на протиправні дії або бездіяльність поліцейських під час проведення виборів в Україні.

Таким чином, використання сучасних інформаційних технологій у рамках здійснення громадського контролю за Національною поліцією під час

проведення виборів в Україні є важливою та затребуваною конституційно-правовою формою участі громадськості у вирішенні державних та суспільних справ. До числа основних електронних ресурсів та інструментів, які використовуються у рамках здійснення громадського контролю за Національною поліцією під час проведення виборів в Україні слід віднести соціальні мережі, месенджери, відеохостинги, веб-потрати та сайти, Інтернет-видання тощо.

Використані джерела:

1. Електронна демократія: навч. посіб. / Н. В. Грицяк, С. Г. Соловйов; за заг. ред. д-ра наук з держ. упр., проф. Н. В. Грицяк. К. : НАДУ, 2015 66 с.
2. Електронне урядування: навч. посіб. / Семенченко, Андрій Іванович; Жиляєв, Ігор Борисович; Дзюба, Сергій Вікторович; Рубан, Ігор Анатолійович; Усаченко, Лариса Михайлівна; Руденко, Ольга Мстиславівна; [за ред. А. І. Семенченка], Навч.-наук. ін-т післядиплом. освіти. Херсон : Грінь Д. С., 2014. 391 с.
3. Впровадження електронного голосування: основні аспекти. Програмний документ Грудень 2011 р. [Українською мовою] / Міжнародний інститут демократії і сприяння виборам. Стокгольм, 2011. 43 с.
4. Нестерович В.Ф. Вплив громадськості на прийняття нормативно-правових актів з використанням комп'ютерних мереж. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2011. № 2. С. 73-81.
5. Нестерович В.Ф. Інституційне утвердження електронних петицій в Україні у контексті зарубіжного досвіду. *Віче*. 2015. № 22. С. 18-23.
6. Нестерович В.Ф. Постмодерні нормативні підходи конституційно-правових засад впливу громадськості на прийняття нормативно-правових актів. *Право і суспільство*. 2016. № 1. С. 24-29.
7. Про Національну поліцію: Закон України від 2 липня 2015 року № 580-VIII. *Відомості Верховної Ради України*. 2015. № 40-41. Ст. 379.
8. Про вибори Президента України: Закон України від 5 березня 1999 року № 474-XIV. *Відомості Верховної Ради України*. 1999. № 14. Ст. 81.
9. Про вибори народних депутатів України: Закон України від 17 листопада 2011 року № 4061-VI. Відомості Верховної Ради України. 2012. № 10. Ст. 73.
10. Про місцеві вибори: Закон України від 14 липня 2015 року № 595-VIII. *Відомості Верховної Ради України*. 2015. № 37-38. Ст. 366.
11. Інформаційно-аналітична система «Вибори-2019». URL: https://mvs.gov.ua/ua/pages/5496_Informaciyno_analitichna_sistema_Vibori_2019.htm

Світличний В.А. - доцент кафедри інформаційних технологій та кібербезпеки Харківського національного університету внутрішніх справ, кандидат технічних наук, доцент;
Головня А.І. - курсант навчальної групи Ф4-102 Харківського національного університету внутрішніх справ

КРІПТОВАЛЮТА. ЕЛЕКТРОННІ ГАМАНЦІ, ПЛЮСИ ТА МІНУСИ

Як відомо, нині широку популярність набуває віртуальна валюта. Користувачі віртуальних гаманців все частіше та частіше роблять вклади у криптовалюту. Та наскільки це безпечно? І чи досить розвинуті сучасні технології, щоб так широко використовувати цю валюту?

Кріптовалюта — вид цифрової валюти, емісія та облік якої засновані на асиметричному шифруванні і застосуванні різних криптографічних методів захисту, таких як Proof-of-work та/або Proof-of-stake. Функціонування системи відбувається децентралізовано в розподіленій комп'ютерній мережі. Кількість кіберзлочинів росте з неймовірною швидкістю. Практично кожен місяць ми чуємо з новин про яку-небудь велику атаку, а уявіть, скільки дрібніших відбувається щодня. Олії в цю ситуацію однозначно додає активний розвиток інноваційних фінтех-індустрій. Адже утримувачі кріптовалюти куди "зручніші" жертви ніж уряди або великі корпорації. За повідомленнями Coinbase (найбільша кріптовалютная біржа США), кожен місяць кількість атак на криптовалюти збільшується на 100%. Також багато хакерських атак так і залишаються в таємниці, так як біржі і клієнти не хочуть ставити під сумнів свою репутацію з боку користувачів.

Незважаючи на те, що 14% всіх коштів залучених через ICO проектів на платформі Ethereum (а це $ 1,6 млрд) були вкрадені, тобто приблизно кожен десятий проект зазнав успішну атаку. Наприклад, проект Zerocoin. Один зайвий символ у вихідному коді проекту дозволив хакерам викрасти більше $ 500 тис. «Умільці» просто генерували додаткову кріптовалюту в рамках транзакції до тих пір, поки не були помічені. Або ситуація з сервісом Parity Ethereum, коли хакери скористалися уразливістю системи і вкрали з гаманців користувачів $32 млн. Однак, такі помилки приносять набагато менших збитків ніж фішингові атаки. На жаль, від них не врятує ні антивірус, ні найефективніші системи захисту. Так кіберзлочинцям вдалося викрасти $8 млн під час проведення ICO блокчейн-стартапу CoinDash, зламавши сайт і замінивши адресу для відправки коштів користувачами. Також через фішингову атаку хакери зламали біржу Bithumb. У той день "пощастило" не тільки південнокорейській біржі, а й гаманцю Classic Ether Wallet. Хакери заволоділи доменом гаманця і зникли з $300 тис.

Спільно з фішинговими атаками хакери люблять використовувати шкідливе ПО, яке дозволяє досить швидко красти величезна кількість коштів. У минулому році на сайті Reddit з'явився пост про криптовалюту, де розташовувалася посилання на сайт CryptoChartiq. При кліці на посилання на пристрій користувача завантажувалося програмне забезпечення, яке просто дочиста списувала кошти з online-гаманців. Ще однією гучною історією стало розміщення шкідливого посилання в пошуковому топі Google, яка обіцяла відвідувачам навчити їх поводитися з кріптовалютою і даркнетом. Далі майданчик перенаправляла відвідувачів на фішингові сайти, крадучи при цьому кріптокошти. Ця хакерська атака була організована власниками ресурсу Darknetmarkets.org. Також останнім часом популярність набирають скріпти для майнінга, боротьбою з якими вже зайнялися розробники Google Chrome. Сподіваємося, що і інші браузери теж підтягнуться. Поки для боротьби з цим видом злочинної діяльності можна боротися установкою спеціальних розширень на зразок AntiMiner, No Coin і minerBlock.

Власник кріптовалют часто зберігає її в електронному гаманці. У вас як у власника повинні бути два ключа - публічний (його ви вказуєте для перерахування вам монет) і приватний (його ви використовуєте для підтвердження транзакцій). На даний момент існують два види гаманців - "гарячі" і "холодні". В "гарячих" гаманцях обидва ключі зберігаються в інтернеті у вашого провайдера, а в "холодних" гаманцях приватний ключ зберігається у вас на пристрої. При цьому не можна сказати, що "холодні" гаманці захистять вас повністю. Використовуйте двухфакторную аутентифікацію для додаткової безпеки, хоча і це не 100%. Тут скоріше грає роль системний підхід і загальна обережність. Зберігайте невеликі суми для витрат на "гарячих" гаманцях, заощадження тримайте на "холодних", не тримайте гроші на біржах, встановіть двухфакторну аутентифікацію, не клацайте по сумнівними посиланнями та використовуйте захищену операційну систему iOS.

Майнери, що використовують обчислювальні потужності користувачів - процесори і відеокарти, потихеньку відходять на задній план, так як це стає нерентабельно. Однак, особливо працьовиті майнери досі можуть на цьому заробляти дуже непогані гроші. Найбільш відомими є ботнети DevilRobber і CoinMiner. При цьому останнім часом набирають популярність скріпти для майнінга, які розміщуються в вихідному коді сайтів.

Як показує практика, основні жертви хакерів - це прості люди, власники кріптовалют. Тобто організовуючи масштабну атаку, хакери сподіваються, що у більшої частини користувачів рівень захисту буде залишати бажати кращого. І досить часто вони виявляються праві. Тому необхідно частіше доводити до користувачів інформацію про те, як захистити себе від хакерських атак.

Сеник В. В. – завідувач кафедри, кандидат технічних наук, доцент;
Кулешник Я. Ф. – доцент кафедри, кандидат технічних наук, доцент;
Магеровська Т. В. – доцент кафедри, кандидат фізико-математичних наук, доцент (кафедра інформаційного та аналітичного забезпечення діяльності правоохоронних органів Львівського державного університету внутрішніх справ)

ПРОБЛЕМИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Лавиноподібний розвиток інформаційних технологій набув глобального характеру в теперішньому світі. Сучасні телекомунікаційні системи надають найширші можливості доступу до інформаційних ресурсів та переміщення їх на значні відстані не залежно від міждержавних кордонів. У сучасних умовах інформація стала ринковим товаром із своїми споживчими властивостями та характеристиками. І, безперечно, основним таким товаром є інформація з обмеженим доступом. Нині чинне законодавство України до такої інформації відносить таємну інформацію, інформацію для службового користування та конфіденційну [1, 2, 3]. Для забезпечення захисту перших двох категорій інформаційних ресурсів на нормативно-правовому рівні передбачено створення комплексних систем захисту інформації [4, 5]. Разом з цим, стосовно третьої категорії – конфіденційної інформації, то тут як на нормативно-правовому, так і на організаційно-технічному рівні існує чимало проблем. Це, зокрема, не до кінця законодавча урегульованість поняття «конфіденційна інформація», відсутність її чіткої класифікації, недосконаліть організаційно-технічного забезпечення її обігу в інформаційно-телекомунікаційних системах, низький рівень забезпечення внутрішньої безпеки інформаційних систем, у тому числі і питання неконтрольованого поширення даних [6], нерозуміння управлінськими апаратами державних та недержавних установ у забезпеченні захисту та передаванні такої інформації, необачні дії власників (тримачів) конфіденційної інформації щодо її розголошення та розповсюдження.

Серед різних законодавчо визначених та невизначених категорій конфіденційної інформації, яка найчастіше набуває неконтрольованого поширення в інформаційно-телекомунікаційних системах, є персональні дані. Їх втрати через низьку організованість систем безпеки у різних базах даних, інформаційних підсистемах призводить не лише до завдання моральних збитків особі, а й створює підґрунтя для вчинення різних правопорушень та зловживань (наприклад, шахрайства, крадіжки коштів з банківських карток то-

що). Стабільно зростаюча кількість фактів витоку конфіденційної інформації в усіх державах світу показує, що від 70 до 90% даних, які втрачаються, це персональні дані.

Такий стан речей призвів до того, що на проблеми захисту персональних даних нині звертають увагу оператори інформаційно-телекомунікаційних систем, бізнес-аналітики, спеціалісти у галузі інформаційних технологій. Про наявність цих проблем говориться практично у всіх аналітичних матеріалах з питань інформаційної безпеки чи безпеки бізнесу. Зокрема, дослідження показують, що лише половина фахівців з інформаційної безпеки вважають своє підприємство, компанію чи установу такою, що готова протистояти сучасним інформаційним загрозам, зокрема і таким, що можуть призвести до неконтрольованого поширення інформації за межі інформаційних систем, у яких вона обробляється.

В окремих випадках ми бачимо безпосереднє ігнорування законодавчих вимог як самими державними чи комерційними установами, власниками інформаційно-телекомунікаційних систем, так і власниками персональних даних (користувачами соціальних мереж, інших прикладних он-лайн програм тощо).

Звичайно, нині існує багато способів захистити персональні дані в інформаційно-телекомунікаційних системах і без побудови комплексної системи захисту інформації (до речі, яка є доволі застарілим підходом до захисту інформаційних ресурсів і у розвинених країнах не застосовується [7]). Це і застосування різноманітних апаратно-програмних засобів, і організаційно-технічних методів захисту інформації тощо. Однак, у даному випадку нами пропонується упроваджувати та удосконалювати системи, які виявляють та попереджають витік інформації, пов’язаної з персональними даними. Такі системи мають проводити аналіз потоків інформації, що передаються інформаційно-телекомунікаційними каналами за межі інформаційної системи, виявляти у них персональні дані та передавати відповідну інформацію на сервер управління для прийняття подальших рішень. Для вдосконалення роботи таких систем необхідно активізувати розроблення алгоритмів щодо виявлення та відповідного реагування на спроби передачі персональних даних. Також слід проводити відповідні заходи щодо формування та підтримання баз даних, які дозволятимуть проводити аналіз та реалізацію алгоритмів виявлення та реагування несанкціонованої передачі інформації.

Використані джерела:

1. Про інформацію : Закон України 02 жовтня 1992 р. № 2657-XII. *База даних «Законодавство України» / ВР України*. URL : http://zakon2.rada.gov.ua/laws/show/2657-12/
2. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05 липня 1994 р. № 80/94-ВР. *База даних «Законодавство України» / ВР України*. URL : http://zakon2.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80/
3. Про захист персональних даних : Закон України від 01 червня 2010 р. № 2297-VI. *База даних «Законодавство України» / ВР України*. URL : http://zakon2.rada.gov.ua/laws/show/2297-17/

4. НД ТЗІ 1.1-005-07. Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення / Затверджено наказом Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 12.12.2007 р. № 232. Київ, 2007.
5. НД ТЗІ 1.6-003-04. Створення комплексів технічного захисту інформації на об’єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації / затв. наказом ДСТСЗІ СБ України від 10.03.2004 р. № 04. Київ, 2004.
6. INFOBEZ-EXPO / международная выставка-конференция [Электронный ресурс]. 2013. URL: \www/ URL: http://infobez-expo.ru/
7. Середа В. В., Живко З. Б., Рудий Т. В. Нормативно-правові аспекти застосування міжнародних стандартів в системі управління безпекою підприємств. *Сучасні проблеми інформатики в управлінні, економіці, освіті та подоланні наслідків Чорнобильської катастрофи* : матеріали XVI міжнародного наукового семінару / за наук. ред. д-ра екон. наук, проф. М. М. Єрмошенка, д-ра екон. наук, доц. І. Ю. Штулер. Київ: Національна академія управління, 2017. С. 69–73.

Строітєлєва Н.І. - доцент кафедри медичної та фармацевтичної інформатики, кандидат фізико-математичних наук, доцент (Запорізький державний медичний університет);
Кісельов Є.М. – доцент кафедри електронних систем, кандидат технічних наук, доцент (Запорізький національний університет)

МЕТОДИКА ПІДГОТОВКИ ФАХІВЦІВ З ДИСЦИПЛІНИ «ОСНОВИ ІНФОРМАЦІЙНИХ СИСТЕМ»

Сучасні інформаційні технології змінюють оточуючий світ дуже швидко і відіграють велику роль в організації навчання в українських вишах з використанням новітніх приладів та сервісів. Особлива увага приділяється підвищенню рівня викладацької майстерності з використанням передових освітніх методик і засобів. Актуальність обраної теми обумовлена тим, що у сучасних умовах зростає інтерес викладачів до використання нових інформаційних технологій, удосконалення форм і методів організації навчального процесу та забезпечення самоосвіти і саморозвитку всіх учасників навчального процесу.

Метою викладання дисципліни «Основи інформаційних систем» є надання студентам чітких уявлень про математичні, фізичні та логічні основи будування та функціонування персонального комп'ютера, комп’ютерних мереж, операційних систем та алгоритмічних основ програмування. Головні завдання дисципліни - надати студентам теоретичні та практичні відомості щодо навиків роботи на персональному комп’ютері в різних операційних системах з основним програмним забезпеченням, а також отримання навиків щодо

створення структурованих програм для вирішення як обчислювальних завдань, так і завдань, пов'язаних з обробкою складних структур даних.

При проведенні лекцій з дисципліни використовується поєднання таких наочних і словесних методів навчання як ілюстрація, розповідь, пояснення, демонстрація. Під час лабораторного практикуму використовуються методи роботи у групах, виконання тренувальних, стендових та розрахункових робіт.

Для проведення лабораторних занять з дисципліни «Основи інформаційних систем» був розроблений лабораторний стенд на основі апаратної платформи Arduino. Платформа Arduino отримала широке визнання у розробників нових електронних пристроїв, викладачів і студентів інженерних напрямів підготовки. Використання Arduino спрощує процес роботи з мікроконтролерами. По технічному оснащенню вона ідеально підходить для освітнього процесу по проектуванню різних електронних систем і роботів, завдяки зрозумілому середовищу програмування і можливості спостереження фізичних процесів в реальному часі, а також завдяки зрозумілому середовищу програмування і ряду інших переваг. Вона може використовуватися як засіб навчання і дослідження в цифровій обробці сигналів, електроніці, схемотехніці, робототехніці, автоматиці та ін. Потужніші плати Arduino застосовні для вирішення складних технічних завдань, пов'язаних з розробкою великих проектів і їх комплексною автоматизацією.

Центральне місце в розробленому стенді займає апаратна платформа Arduino Mega 2560 – це електронний конструктор і зручна платформа з відкритим вихідним кодом, створена для швидкої і легкої розробки різноманітних електронних пристроїв, зокрема для налагодження алгоритмів систем контролю і автоматизації [1]. Програмна частина платформи представляє собою програмну оболонку, що включає в себе текстовий редактор, адаптований для написання програмного коду на мові Сі, компілятор і набір засобів для програмування апаратури.

Функціональна блок-схема розробленого приладу включає блоки індикації, регулювання, контролювання та маніпуляцій, а також блок розширення для підключення різноманітних пристроїв (світлодіодів, двигунів, звукових індикаторів тощо). Конструкція стенду дозволяє корегувати індивідуальні завдання лабораторних робіт для покращення вивчення матеріалу студентами. Існує також конструктивна можливість розширення можливостей стенду завдяки підключення до нього деяких інших елементів та приладів.

Завдяки повнофункціональній платформі Arduino стає можливим просте та ефективне моделювання приладів контролю та управління. Проста мова програмування та зрозумілі функції виводів платформи роблять Arduino найбільш зручним інструментом для початківців та професіоналів. На базі платформи можна побудувати велику кількість корисних приладів. Починаючи від простого змінювання яскравості світлодіоду до впливу на системи, які можуть керувати клімат-контролем та системою безпеки цілого будинку.

Під час вивчення навчальної дисципліни студенти навчаються використовувати ПК як інструмент для оптимізації та інтенсифікації інформаційних

процесів, вирішувати логічні задачі; тестувати комп'ютерну систему будь-якої конфігурації; складати програмні коди для контролера Arduino. У результаті вивчення навчальної дисципліни студент повинен знати основи теорії систем, двійкової системи числення, алгебри логіки; загальну структуру комп'ютера та його компонентів; принципи побудови комп'ютерних мереж.

Оцінювання навчальних успіхів студентів реалізується шляхом проведення поточного та підсумкового контролю успішності. Поточний контроль здійснюється за тестовою методикою з отриманням бальних оцінок, які характеризують рівень засвоєння студентами теоретичного матеріалу, та бальною оцінкою якості виконання лабораторних робіт.

Таким чином, у сучасному виші викладання «Основ інформаційних систем» відбувається із використанням різноманітних засобів та методів передових інформаційних технологій. Для повноцінного подання дисципліни викладач залучає до процесу сучасні технічні та інформаційні засоби спілкування з аудиторією.

Використані джерела:

1. Arduino [Електронний ресурс] – 2019 – Режим доступу: [Електронний ресурс] – статті 2019 – Режим доступу: https://www.arduino.cc/en/Guide/HomePage - Дата доступу: листоп. 2019. – Назва з екрану.

Федчак І.А. - доцент кафедри оперативно-розшукової діяльності факультету № 2 Інституту з підготовки фахівців для підрозділів Національної поліції Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент

ВИКОРИСТАННЯ ПІД ЧАС ПРОВЕДЕННЯ КРИМІНАЛЬНОГО АНАЛІЗУ СПЕЦІАЛІЗОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ IBM I2

Аналіз діяльності правоохоронних органів у сфері протидії злочинності свідчить про її недостатню ефективність. Зважаючи на ту обставину, що сучасний злочинний світ надзвичайно активний, адаптивний, динамічний, високотехнологічний та організований можна стверджувати, що побудова діяльності оперативних підрозділів поліції щодо протидії поширенню його впливу не може мати успішних результатів без змін у нормативно-правовому та організаційно-тактичному виразі їх діяльності. У зв'язку з цим у правоохоронних органів постає нагальна необхідність у реорганізації та вдоскона-

ленні сталих методів їх діяльності. Вивчення досвіду практики зарубіжних правоохоронних органів дозволяє виокремити дієвий напрям діяльності органів та підрозділів поліції у забезпеченні протидії усім проявам злочинності – кримінальний аналіз, який можна застосовувати на етапах ведення оперативно-розшукової діяльності, досудового розслідування та розгляду кримінальних проваджень у суді.

Окремі аспекти використання кримінального аналізу в діяльності правоохоронних органів розглядали у своїх наукових працях Дж. Картер, С. Філіпс, К. Вестфал, О. В. Власюк, О. Є. Користін, О. М. Заєць, К. Ю. Ісмайлов, В. В. Єрофеєв, А. В. Махнюк, В. І. Мельник, В. А. Некрасов та інші.

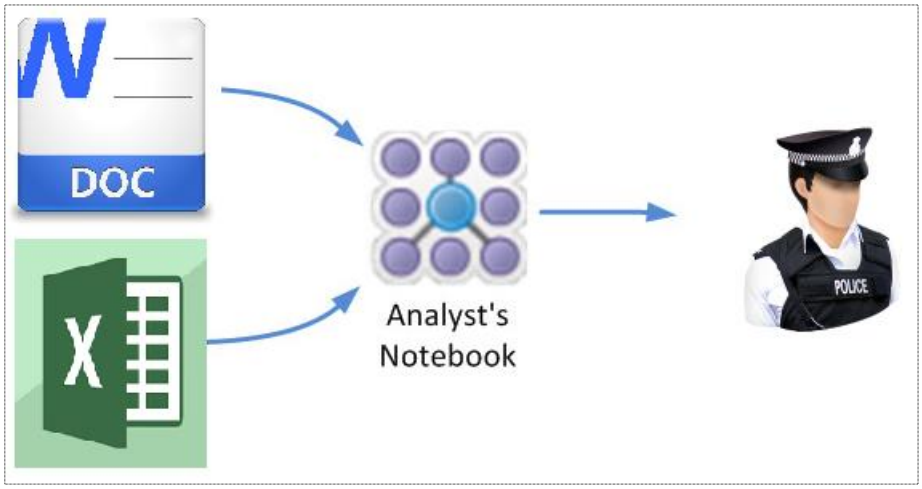
Кримінальний аналіз – специфічний вид інформаційно-аналітичної діяльності, спрямований на встановлення та передбачення взаємозв'язків між даними про злочинну діяльність та іншими даними, потенційно з ними пов'язаними, їх оцінювання, інтерпретація та прогнозування розвитку досліджуваних подій з метою їх використання під час досудового розслідування та здійснення оперативно-розшукової діяльності, а також для розроблення тактичних та стратегічних заходів із протидії злочинності [1].

Кримінальний аналіз – це оперативно-слідча дія, яка полягає у методичному пошуку і визначенні зв'язків: з одного боку – між самими даними, які стосуються правопорушення, а з іншого боку – між ними та іншими відомостями, які можна вирізнити. Це ідентифікація та визначення внутрішніх взаємозв'язків між інформаціями (відомостями), які стосуються правопорушення та будь-якими іншими даними, отриманими з різних джерел. Кримінальний аналіз ставить за мету підготовку висновків і пропозицій подальших дій. Він є інструментом, який супроводжує процеси прийняття рішень [2]. Основою такої діяльності – є аналіз процесів та явищ, які відбуваються в кримінальному середовищі, та результатів їхньої злочинної діяльності з метою виявлення злочинних зв'язків, закономірностей та тенденцій.

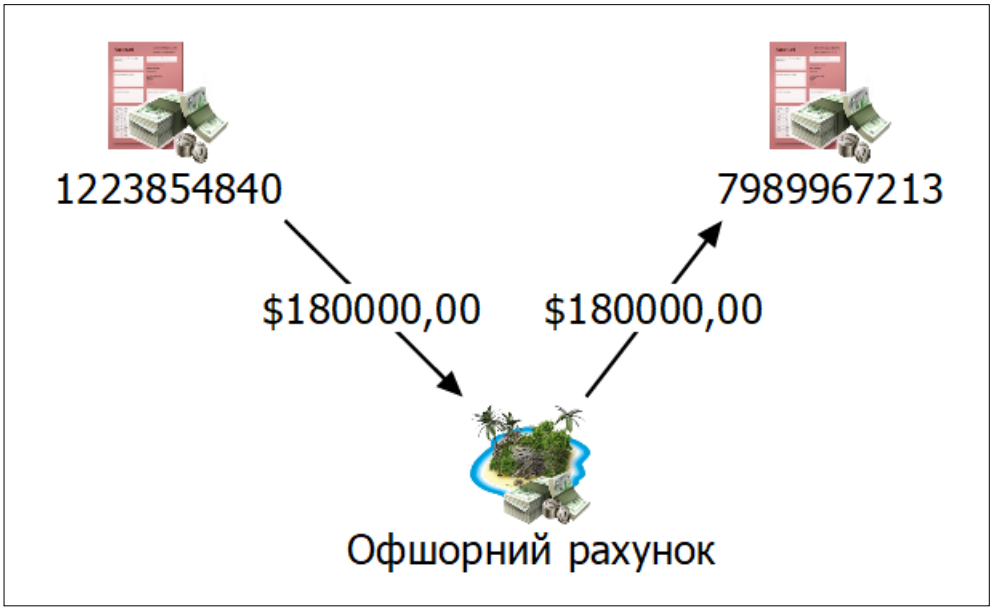
У рамках наданих повноважень працівники поліції здобувають значні за обсягом масиви даних, що містять інформацію про злочинну діяльність як окремих суб'єктів, так і організованих злочинних груп. У зв'язку з чим надважливим на сьогодні є застосування аналітичних інструментів, які б надали можливість оперативно опрацьовувати високооб'ємні дані, а також виконувати автоматизовані аналітичні функції. Одним із таких інструментів у кримінальному аналізі є використання комплексного спеціалізованого комп'ютерного програмного забезпечення IBM i2 Analyst's Notebook, IBM i2 iBase та IBM i2 iBridge.

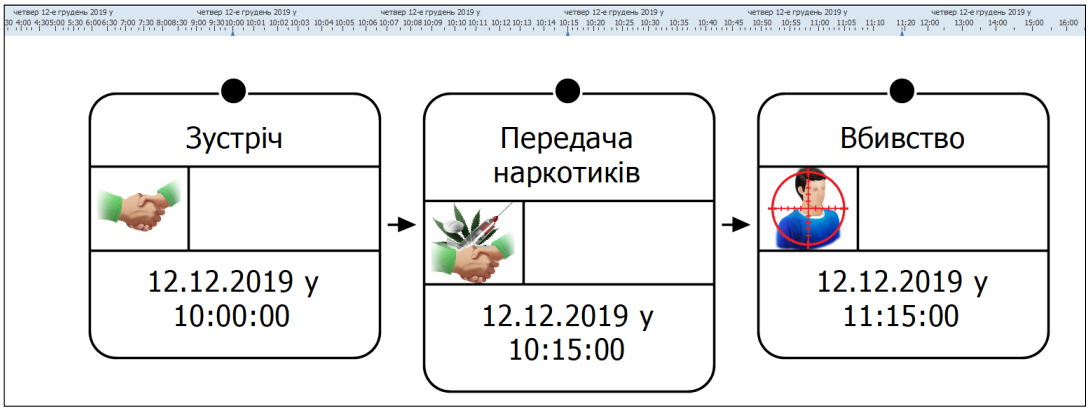
IBM i2 Analyst Notebook – візуальне аналітичне середовище, яке дозволяє максимально ефективно використовувати надвеликі обсяги інформації, які сформовані у масивах даних до прикладу у Національної поліції. Програма характеризується інтуїтивно зрозумілим інтерфейсом та з урахуванням контексту дозволяє аналітикам швидко зіставляти, аналізувати та наочно представляти дані з різних джерел, скорочуючи час на пошук важливої інформації в сукупності розрізнених даних. IBM i2 Analyst's Notebook надає акту-

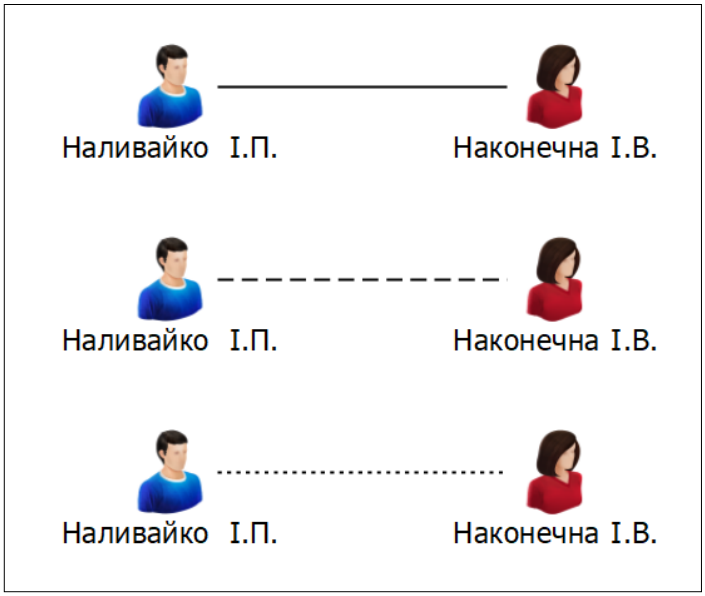
альні та дієві аналітичні засоби, які допомагають виявляти, передбачати, попереджувати та припиняти злочинну діяльність.

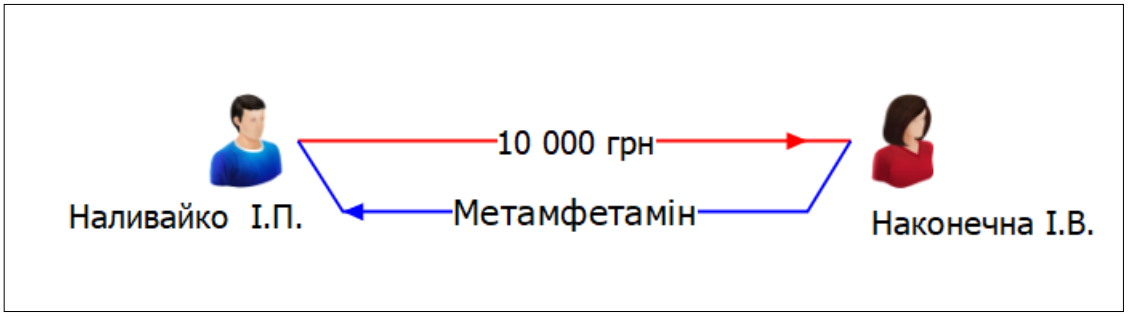


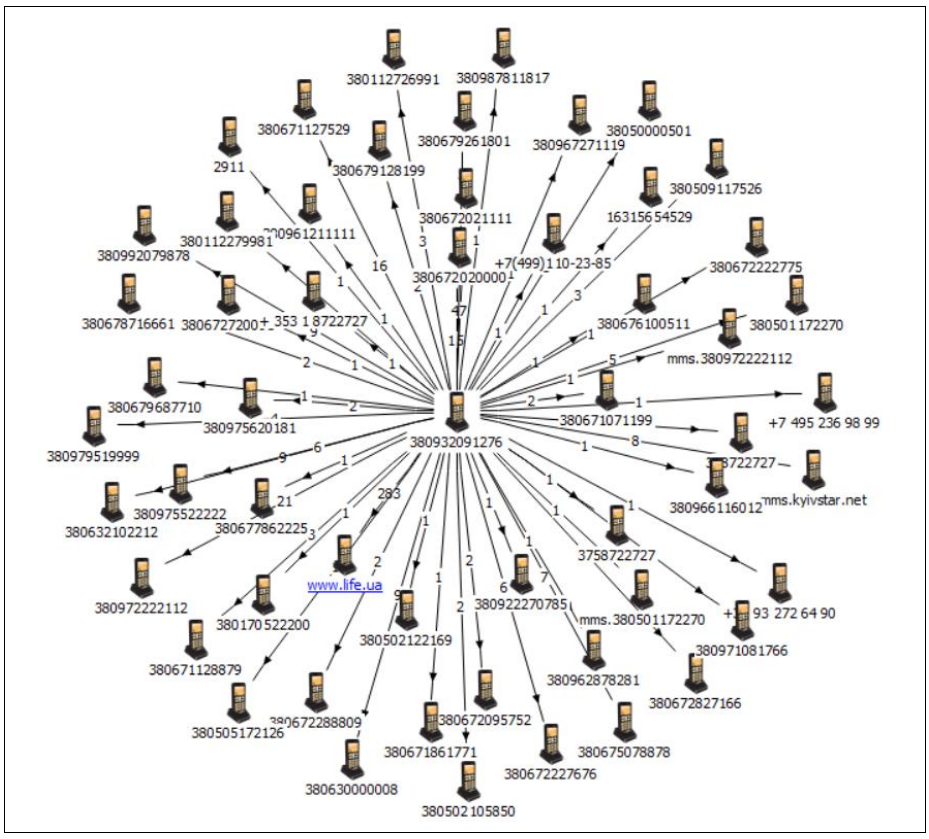
Щоб побудувати повну картину для дослідження Analyst’s Notebook може звертатись до даних цілого ряду джерел. В Analyst’s Notebook дані відображаються у вигляді об’єктів, зв’язків та властивостей. Об’єкти в Analyst’s Notebook відображають явища реального світу, такі як банківські рахунки та телефони, або події, наприклад, зустрічі.

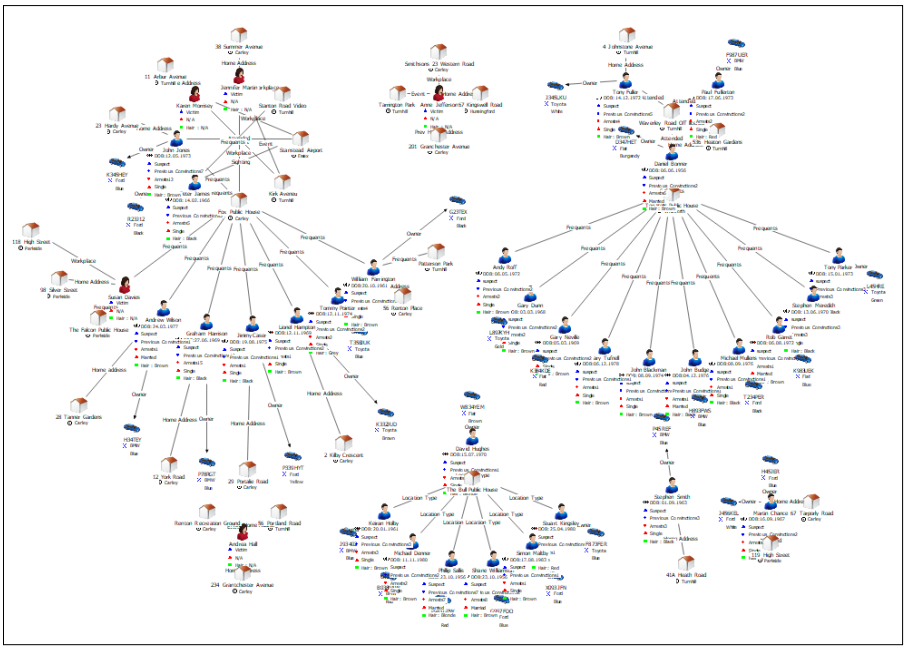


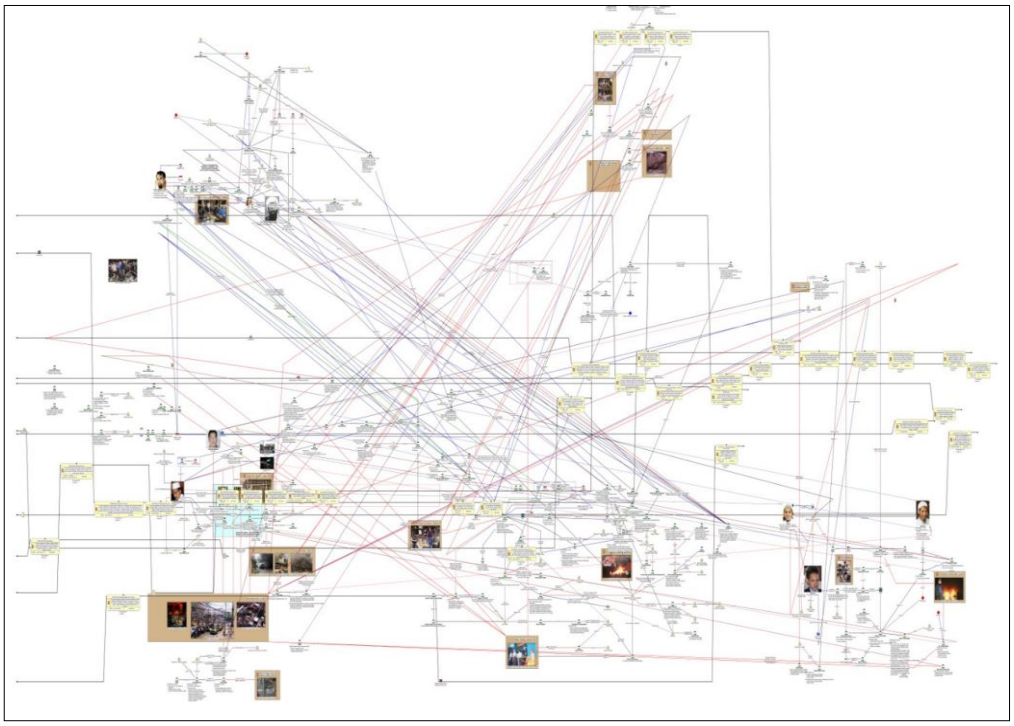

Зустріч
12.12.2019 у
10:00:00
Передача
наркотиків
12.12.2019 у
10:15:00
Вбивство
12.12.2019 у
11:15:00


Наливайко І.П.
Наконечна І.В.
Наливайко І.П.
Наконечна І.В.
Наливайко І.П.
Наконечна І.В.


10 000 грн
Метамфетамін
Наливайко І.П.
Наконечна І.В.

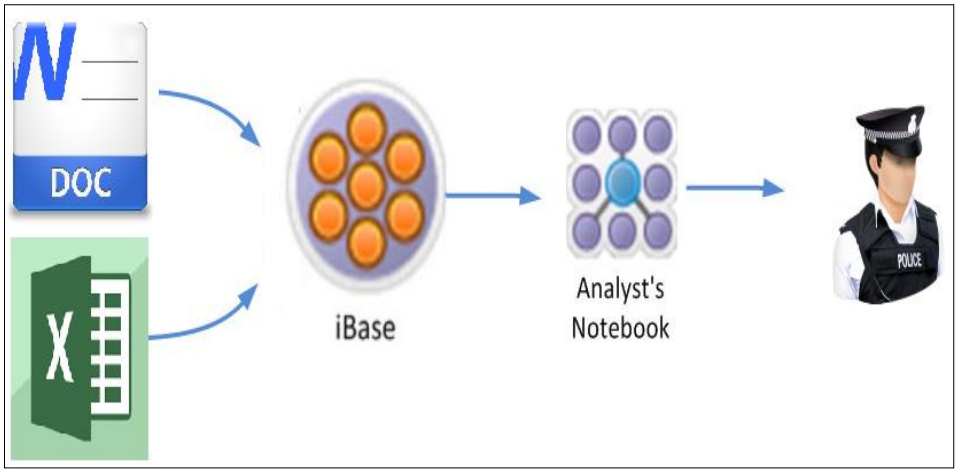

380112726991
380987811817
380671127529
380679261801
380967271119
38050000501
2911
380679128199
380509117526
380672021111
380961211111
380112279981
380992079878
+7(499)110-23-85
380672222775
380678716661
380672020000
380672727200
+_353 1 8722727
380676100511
380501172270
mms.380972222112
380679687710
380975620181
380671071199
+7 495 236 98 99
380979519999
380932091276
380966116012
mms.kyivstar.net
380975522222
380677862225
380632102212
3758722727
380972222112
www.life.ua
380922270785
mms.380501172270
+ 93 272 64 90
380170522200
380502122169
380971081766
380671128879
380962878281
380672827166
380672288809
380672095752
380505172126
380671861771
380675078878
380672227676
380630000008
380502105850



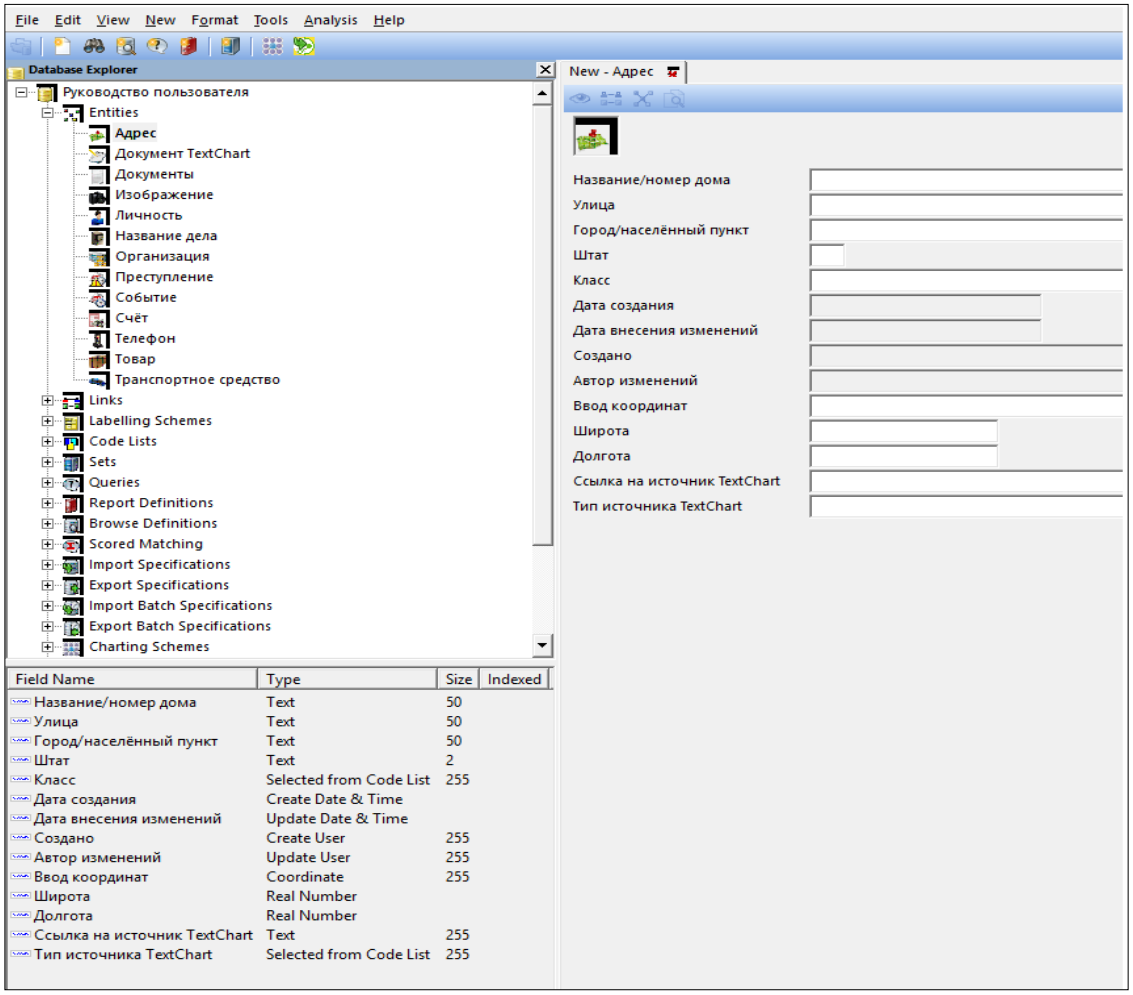


Властивості використовуються, щоб зберігати інформацію, яка відома про елемент, (наявність у людини судимості або дата та час зустрічі). Важливо наперед вирішувати, де розмістити ті чи інші відомості. Такі рішення впливають на доступні після цього типи аналізу і на висвітлення інформації.

Збирати, контролювати та аналізувати дані з декількох джерел в захищених робочих групах дозволяє програма IBM **i2 iBase** – інтуїтивно зрозумілий аналітичний додаток баз даних, що дозволяє колективам аналітиків, які спільно працюють збирати, контролювати і аналізувати дані з декількох джерел в захищених середовищах робочих груп.



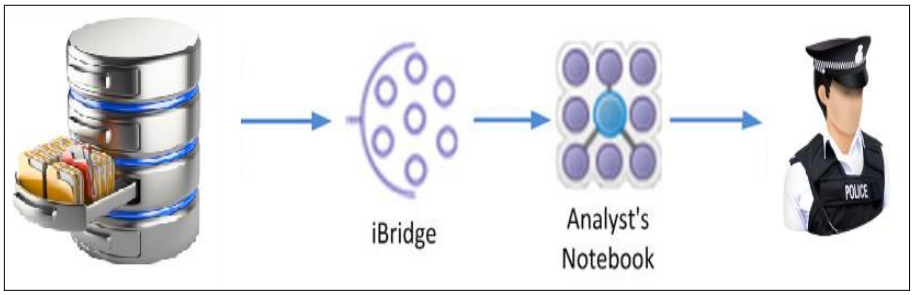
Цей продукт дозволяє вирішити повсякденну проблему аналітиків, яка полягає у виявленні і розкритті особливостей взаємозв'язків, шаблонів і тенденцій в сучасних умовах, що характеризуються стрімким зростанням обсягів складних структурованих і неструктурованих даних. I2 iBase надає багатьом користувачам середовище обміну даними, в якому велика кількість функцій аналізу і візуалізації поєднуються з інструментами поширення.



i2 iBase містить наступні компоненти:

- гнучке набуття даних та управління ними, візуалізація інформації та її аналіз;
- автоматизований аналіз на основі завдань для прискорення розкриття прихованих зв'язків, який допомагає аналітикам своєчасно надавати практично застосовні результати;
- підтримка керованої спільної роботи і потоків операцій, яка спрощує колективну роботу;
- керований та готовий до використання додоток, який забезпечує гнучке та економічно вигідне упровадження.

IBM i2 iBridge – це розширене рішення для зв’язку та аналітичного пошуку, яке під’єднає користувачів IBM i2 Analyst’s Notebook в реальному часі безпосередньо з базами даних, які функціонують, до прикладу, у Національній поліції для забезпечення негайного початку аналітичного дослідження. Ефективні інструменти пошуку та виконання запитів повертають результати у вигляді готових до аналізу даних з візуалізацією зв’язків між записами для прискорення створення аналітичних даних.



Як висновок слід зазначити, що для того, щоб адекватно відповідати вимогам часу та сучасним викликам злочинного світу працівникам поліції слід якомога швидше опановувати сучасні інструменти опрацювання значних та великих обсягів інформації, запроваджувати їх у свою щоденну практичну діяльність.

Використані джерела:

1. Методичні рекомендації щодо організації та проведення кримінального аналізу підрозділами Національної поліції України. – Національна поліція України. – Київ, 2019 р.
2. Мірослав Яніцкі. Оперативний кримінальний аналіз. - Проект міжнародної організації з міграції "Розвиток систем аналізу ризику та кримінального аналізу для Державної прикордонної служби України відповідно до європейських стандартів (АРКА)”. – 2009 рік.

КУРСАНТИ ТА СТУДЕНТИ ПІД НАУКОВИМ КЕРІВНИЦТВОМ

Бондаренко О.С. - курсант 3 курсу Дніпропетровського державного університету внутрішніх справ;
Бублик Н. С. – науковий керівник**,** викладач кафедри кримінального процесу Дніпропетровського державного університету внутрішніх справ.

ДЕЯКІ ПРОЦЕДУРНІ АСПЕКТИ ВИРІШЕННЯ ПИТАННЯ ЩОДО ВНЕСЕННЯ ВІДОМОСТЕЙ ДО ЄРДР ЗА КПК УКРАЇНИ 2012 РОКУ

Актуальність теми зумовлена потребою у здійсненні аналізу особливостей нормативного регулювання використання Єдиного реєстру досудових розслідувань (далі – ЄРДР), зокрема, під час вирішення слідчим або прокурором питання щодо внесення відомостей до ЄРДР, оскільки аналіз судової практики дає підстави стверджувати про відсутність єдиного розуміння у суб'єктів правозастосування окремих процедурних аспектів вирішення питання щодо внесення відомостей про кримінальне правопорушення до ЄРДР.

Так, відповідно до ч.1 ст. 214 Кримінального процесуального кодексу України (далі – КПК України) слідчий, прокурор невідкладно, але не пізніше 24 годин після подання заяви, повідомлення про вчинене кримінальне правопорушення або після самостійного виявлення ним з будь-якого джерела обставин, що можуть свідчити про вчинення кримінального правопорушення, зобов'язаний внести відповідні відомості до Єдиного реєстру досудових розслідувань, розпочати розслідування та через 24 години з моменту внесення таких відомостей надати заявнику витяг з Єдиного реєстру досудових розслідувань [1].

Така будова кримінального процесуального закону дозволила деяким дослідникам вважати, що першою стадією кримінального процесу України з 2012 року є стадія досудового розслідування, з якої починається досудове провадження, а стадії, аналогічної порушення кримінальної справи, взагалі немає [2].

Аналіз конструкції наведеної норми приходить до припущення, що за будь-якою заявою чи повідомленням, що надійшли до слідчого чи прокурора має бути «відкрито» кримінальне провадження і розпочато досудове розслідування, оскільки ч. 2 ст. 214 КПК визначає, що досудове розслідування розпочинається з моменту внесення відомостей до Єдиного реєстру досудових

розслідувань.

Крім того, перевірка заяв і повідомлень про кримінальні правопорушення ні цією статтею, ні наступними статтями КПК України прямо не передбачена. Показово, що особлива частина КПК України, тобто сама процедура кримінального провадження, починається з розділу третього, який має назву «Досудове розслідування».

Розглядаючи дане питання, можна дійти до наступного, перша глава цього розділу - глава 19 - носить назву «Загальні положення досудового розслідування». Таким чином, ні про які стадії, що передують стадії досудового розслідування, в розділі третьому КПК країни, мова не йде.

Крім того, ст. 3 КПК України, що роз'яснює термінологію Кримінального процесуального кодексу, вказує, що стадією кримінального процесу є досудове розслідування (п. 5 ч. 1 ст. 3), яке починається з моменту внесення відомостей про кримінальне правопорушення до Єдиного реєстру досудових розслідувань і закінчується припиненням кримінального провадження або направленням до суду обвинувального акту, клопотання про застосування примусових заходів медичного або виховного характеру, клопотання про звільнення особи від кримінальної відповідальності. Ні про яку більш ранню стадію, ніж стадія досудового розслідування, в ст. 3 КПК не йдеться.

На відміну від чинного КПК України, частинами першою-другою ст. 97 КПК УРСР 1960 року передбачалось, що прокурор, слідчий, орган дізнання або суддя зобов'язані приймати заяви і повідомлення про вчинені або підготовлювані злочини, в тому числі і в справах, які не підлягають їх віданню. По заяві або повідомленню про злочин прокурор, слідчий, орган дізнання або суддя зобов'язані були не пізніше триденного строку прийняти одне з таких рішень:

1) порушити кримінальну справу;

2) відмовити в порушенні кримінальної справи;

3) направити заяву або повідомлення за належністю [36].

З огляду на все вищезазначене сьогодні можна констатувати наявність в практичній площині ситуації, за якої заявники та особи, що звертаються із певною інформацією до слідчого або прокурора з посиланням на ст. 214 КПК наполягають на внесенні відповідних відомостей до ЄРДР з одного боку, навіть якщо такі заяви чи повідомлення очевидно не містять інформації про вчинення кримінального правопорушення, а з іншого боку нормативна відсутність інституту досудової перевірки, на думку уповноважених посадових осіб правоохоронних органів, «зв’язує їм руки» і не дозволяє легально відмовити у реєстрації відповідних заяв та повідомлень, як заяв та повідомлень про вчинення кримінального правопорушення, що призводить до надмірної кількості зареєстрованих кримінальних проваджень або до появи неформальних практик «напівлегальної відмови» у відкритті кримінального провадження.

Суб’єктний склад вирішення питання щодо реєстрації відомостей, що містяться у заяві чи повідомленні про кримінальні правопорушення до ЄРДР на практиці та в теоретичній моделі здійснення такої реєстрації відрізняється.

В практичній (нормативній моделі) можливість підготовки рішення у формі постанови про відмову у реєстрації чи реєстрацію прямо не визначена у КПК України (однак, ми наполягаємо на наявності такої можливості), натомість, як вбачається з Положення про порядок ведення Єдиного реєстру досудових розслідувань [4], на підзаконному рівні пропонується інший спосіб опрацювання інформації та вирішення заяв та повідомлень:

1. сортування уповноваженою на здійснення розгляду особою заяви чи повідомлення про кримінальне правопорушення до однієї з трьох категорій: такі, відомості, що містяться в яких підлягають внесенню до ЄРДР, такі, що підлягають розгляду за Законом України «Про звернення громадян»[5] і такі, що підлягають розгляду в порядку КУпАПу [6];
2. підготовка відповіді:

- у разі віднесення заяви чи повідомлення до категорії таких, що підлягають розгляду в порядку Закону України «Про звернення громадян» - письмової відповіді у строки, передбачені ст. 20 Закону;
- у разі віднесення заяви чи повідомлення до категорії таких, що підлягають розгляду в порядку КУпАПу – складання протоколу про адміністративне правопорушення;
- у разі віднесення заяви чи повідомлення до категорії таких, відомості, що містяться в яких підлягають внесенню до ЄРДР – (а) складання уповноваженою службовою особою органу (підрозділу) поліції рапорту на ім'я керівника органу (підрозділу) поліції або особи, яка виконує його обов'язки, (б) керівник органу (підрозділу) поліції або особа, яка виконує його обов'язки, доручає уповноваженій службовій особі невідкладно зареєструвати рапорт працівника поліції в ІТС ІПНП (журналі ЄО) та (в) не пізніше 24 годин з моменту реєстрації надіслати зазначені матеріали до органу досудового розслідування органу (підрозділу) поліції для внесення відповідних відомостей до ЄРДР.

Таким чином, суб'єктний склад під час здійснення вирішення питання щодо реєстрації відомостей, що містяться у заяві чи повідомленні про кримінальні правопорушення до ЄРДР в практичній моделі представлений поліцейським органу (підрозділу) поліції (іншою посадовою особою іншого органу досудового розслідування), якому доручено розгляд заяви або повідомлення, керівником органу чи особою, яка виконує його обов'язки та уповноваженою службовою особою - працівником чергової служби, у разі відсутності в структурі органу (підрозділу) поліції відповідної чергової служби - інший визначений керівництвом органу (підрозділу) поліції працівник, якого уповноважено на прийняття та реєстрацію заяв і повідомлень про кримінальні правопорушення та інші події, а також слідчим, який вноситиме відомості про вчинення кримінального правопорушення до ЄРДР.

В теоретичній моделі ми пропонуємо в якості дієвих осіб початкового етапу підготовчого провадження наступних суб'єктів: заявника, уповноважену службову особу, слідчого чи прокурора, який видаватиме постанову про внесення чи відмову у внесенні відомостей за заявою чи повідомленням про

кримінальне правопорушення заявника.

Вказане в повній мірі надає можливість дійти до висновку, що різниця суб'єктивного складу ідеальної і практичної моделі полягає у:

а) відсутності проміжної ланки – керівника органу досудового розслідування, повноваження якого, передбачені ч. 2 ст. 39 КПК, не охоплюють дії із заявою чи повідомленням про кримінальне правопорушення до його реєстрації до ЄРДР;

б) позиціонування особи, що аналізує та сортує заяву чи повідомлення про кримінальне правопорушення не просто як уповноваженої службової особи органу досудового розслідування, а як суб'єкта із спеціальним процесуальним статусом, що зумовлює специфічні права та обов'язки, - слідчого або прокурора.

Використані джерела:

1. Кримінальний процесуальний кодекс України: Закон України № 4651-VI від 13.04.2012. URL: https://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення 12.11.2019).
2. Филин Д.В. Начало досудебного производства в уголовном процессе Украины URL: http://www.iuaj.net/node/1462 (дата звернення 12.11.2019)
3. Кримінально-процесуальний кодекс України: Закон Української радянської Соціалістичної Республіки №1002-05 від 28.12.1960 (втратив чинність). URL: https://zakon.rada.gov.ua/laws/show/1001-05 (дата звернення 10.11.2019)
4. Положення про порядок ведення Єдиного реєстру досудових розслідувань, затверджене Наказом Генеральної прокуратури України від 06.-4.2016 №139 URL: https://zakon.rada.gov.ua/laws/show/z0680-16 (дата звернення 04.11.2019)
5. Про звернення громадян: Закон України № 393/96-ВР від 02.10.1996. URL: https://zakon2.rada.gov.ua/laws/show/393/96-вр (дата звернення 11.11.2019)
6. Кодекс України про адміністративні правопорушення: Закон України № 8073-X від 07.12.1984. URL: https://zakon.rada.gov.ua/laws/show/80731-10 (дата звернення 14.11.2019)

Воробець Х. О. - курсант факультету економіко-правової безпеки;
Тютченко С.М. – науковий керівник, старший викладач кафедри економічної та інформаційної безпеки
(Дніпропетровський державний університет внутрішніх справ)

ЕКОНОМІЧНА ЗЛОЧИННІСТЬ В УКРАЇНІ ТА ЇЇ НЕГАТИВНИЙ ВПЛИВ НА РОЗВИТОК ДЕРЖАВИ

На сьогоднішній день питання економічної злочинності в Україні залишається дуже актуальним. За оцінками, які дають фахівці з різних куточків світу, в Україні фактично склались дві економіки: легальна, яка є контрольо-

вана державою та нелегальна, тобто тіньова. Криміналізація економіки України гальмує розвиток підприємництва, становлення реального ринкового середовища [1].

Економіка є фундаментом в існуванні та стабільному розвитку будь-якої сучасної держави. Саме тому, формування ефективної системи економічних відносин, стійкої до негативних зовнішніх впливів та водночас інтегрованої до міжнародного економічного простору, є одним із найважливіших завдань національної політики держави. Стратегія національної безпеки України, затверджена Указом Президента України від 26 травня 2015 р. № 287/2015, визнала забезпечення економічної безпеки одним з основних напрямів державної політики України [2].

Ефективність протидії злочинності безпосередньо залежить від отримання повної та достовірної інформації щодо кількісних і якісних показників певного виду злочинів та визначення тенденцій розвитку досліджуваного феномену. Однією з проблем протидії економічній злочинності в Україні є труднощі у визначенні її кількісних та якісних показників. З одного боку, це пов'язано зі внесенням значних змін до Кримінального кодексу України (далі – КК України) щодо відповідальності за економічні злочини, з іншого – з відсутністю єдиної статистичної звітності щодо вчинених економічних злочинів.

Фахівці зазначають, що зменшення кількості зареєстрованих злочинів у сфері господарської діяльності свідчить про значне зниження активності правоохоронців у виявленні економічних злочинів. Що стосується географії поширення економічної злочинності по регіонах України, то спостерігається тенденція її розповсюдження переважно в найбільш економічно розвинутих областях, а саме в Дніпропетровській, Одеській, Харківській, Запорізькій, Львівській та Вінницькій областях і в м. Києві.

Серед економічних факторів аналізованого виду злочинності найбільш вагоме місце посідає низький рівень доходів населення в країні, що безпосередньо впливає на формування корисливої мотивації. За оцінками ООН на 2017 р 80% населення України живе за межею бідності. Крім того фактичний прожитковий мінімум більше ніж удвічі перевищує офіційний.

Суттєвим чинником економічної злочинності в Україні залишається й високий рівень безробіття населення. За даними Державної служби зайнятості рівень безробіття у 2016 р. становив 9,1 %, у 2017 р. – 9,9 %, а у 2018 р. – вже 10,1 % [3]. Через тривалий спад виробництва, що відбувається в багатьох галузях, постійно зростає кількість людей, які лише числяться на виробництві, а на практиці перебувають у неоплачуваних відпустках. Останні є фактично «тимчасовими» безробітними – резервом безробіття реального.

Аналіз поточних кількісних і якісних показників економічної злочинності та порівняння з відповідними даними за попередні роки загалом засвідчують наявність низки негативних тенденцій у поширенні економічних злочинів в Україні. Хоча відповідно до офіційної статистики частка економічних злочинів у структурі злочинності в нашій державі становить лише 6 %, прямі

та непрямі збитки від них становлять мільярди гривень щорічно. Значні прогалини в регулюванні економічних відносин, неефективність контролю за сферою державних закупівель, лобіювання інтересів конкретних виробників, низька ефективність ужитих державою антикорупційних заходів і відсутність комплексної нормативно-правової бази протидії економічній злочинності призводять до неефективності спорадичних антикриміногенних заходів у вказаній сфері. Окрім того, негативні тенденції економічної злочинності в України значно посилюються завдяки впливу низки економічних, соціальних і політичних детермінант, безпосередньо пов'язаних із наявністю збройного конфлікту на сході України. Убачається, що встановлені тенденції економічної злочинності мають бути враховані під час розробки комплексної стратегії протидії цьому виду злочинності як важливого інструменту забезпечення економічної безпеки держави та поліпшення добробуту її громадян.

Використані джерела:

1. Конституція України/ Відомості Верховної Ради України// , 1996, № 30, ст. 141- [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua /laws.
2. Кримінальний кодекс України // Відомості Верховної Ради України, 2001,- № 25-26, ст.131 [Електронний ресурс]. – [Електронний ресурс]. − Режим доступу: http://zakon.rada.gov.ua/laws.
3. Глущенко В. В. Економічна злочинність , прийоми приховування і методи ii виявлення. / В.В. Глущенко // Вісті Кримінологічної асоціації України .-2004.-Вип 1.- Х: В-цтво Харк. нац. ун-ту внутр. Справ.- с.173- 175

Гавриш Б.О. - курсант 1 курсу факультету підготовки фахівців для органів досудового розслідування;

Мирошниченко В.О. – науковий керівник, професор кафедри економічної та інформаційної безпеки, кандидат технічних наук, доцент

КРИПТОГРАФІЯ ТА СТЕГАНОГРАФІЯ В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

На сьогоднішній день в нашому суспільстві постала велика проблема із захистом інформації, мережева безпека стала важливою частиною сучасної системи зв'язку.

Захист інформації (Data protection) — сукупність методів і засобів, що забезпечують конфіденційність, цілісність і доступність інформації за умов впливу на неї загроз природного або штучного характеру, реалізація яких може призвести до завдання шкоди власникам і користувачам інформації.

На сьогоднішній день існують декілька видів захисту інформації, при

чому кожен вид захисту інформації забезпечує окремі аспекти інформаційної безпеки:

• технічний — забезпечує обмеження доступу до носія повідомлення апаратно-технічними або програмними засобами (антивіруси, фаєрволи, маршрутизатори, токіни, смарт-карти тощо), що забезпечує попередження витоку по технічним каналам та попередження блокування;

• інженерний — попереджує руйнування носія внаслідок навмисних дій або природного впливу інженерно-технічними засобами (сюди відносять обмежуючі конструкції, охоронно-пожежна сигналізацію);

• криптографічний — попереджує доступ за допомогою математичних перетворень, який забезпечує несанкціоновану модифікацію та розголошення інформації;

• організаційний — попередження доступу на об'єкт інформаційної діяльності сторонніх осіб за допомогою організаційних заходів (правила розмежування доступу).

На сьогоднішній день в інформаційній безпеці широке застосування отримали такі інструменти захисту інформації як криптографія та стеганографія. Стеганографія приховує сліди спілкування, тоді як криптографія використовує шифрування, щоб зробити повідомлення незрозумілим. Стеганографія не передбачає змін у структурі повідомлення. З іншого боку, криптографія змінює стандартну структуру секретного повідомлення при передачі по мережі.

Отже, стеганографія - це техніка приховування спілкування, приховуючи таємне повідомлення у фальшиве повідомлення. Термін стеганографія має грецький вплив, що означає «таємне письмо». Основна ідея стеганографії - запобігти підозрі щодо існування інформації. Раніше це було невидиме чорнило, відбитки олівців на рукописних символах, невеликі проколи шпильками - це методи, які використовувалися для приховування повідомлення. Найпростіша техніка приховування повідомлення - це створення повідомлення, в якому секретне повідомлення містить лише кілька значущих символів. Техніка стеганографії включає в себе носій обкладинки, секретне повідомлення, ключ шифрування та носій шифрування. Текст, аудіо, зображення та відео поводяться як носії обкладинки, які містять приховану інформацію, закладену в ньому. Носій шифрування генерується за допомогою носія обкладинки та вбудованого повідомлення. Ключ шифрування також використовується як додаткова таємна інформація, як пароль, що використовується одержувачем для отримання повідомлення. Як було сказано вище, текст, аудіо, зображення та відео використовуються в якості носіїв прикриття, тому стеганографія надходить у різних формах. Використовуючи текст, щоб приховати повідомлення, слово чи рядок можна змістити, можна використовувати пробіли, навіть кількість та положення голосних використовуються для приховування таємного повідомлення.

Перспективними на сьогодні є аудіо та відео стеганографія. Аудіо стеганографія дозволяє приховати таємне повідомлення в аудіофайлі за допомо-

гою його цифрового зображення. Це може бути досягнуто легко, оскільки типовий 16-бітний файл має 216 рівнів звуку, а різницю кількох рівнів неможливо виявити людським вухом. Зображення є найбільш вживаною формою стеганографії, причина цього в тому, що вона викликає найменшу підозру. Відеостеганографія дає більше можливостей маскування великого обсягу даних, оскільки це поєднання зображення та звуку. Тому методи відео- та ауді-остеганографії також можуть бути використані на відео.

Основним недоліком використання стеганографії є значна кількість накладних витрат, які вона створює для приховування невеликої кількості інформації. Крім того, не слід виявляти систему захисту, інакше вона марна.

Криптографія забезпечує кілька схем кодування для досягнення безпеки під час спілкування в загальнодоступній мережі. Слово криптографія походить від грецького слова, яке означає "таємне написання". Криптографію можна зрозуміти на прикладі, коли відправник посилає повідомлення, яке спочатку існує в простому тексті. Перед передачею повідомлення по мережі воно шифрується та перетворюється в шифротекст. Коли це повідомлення надійде до одержувача, воно знову розшифровується назад у простий текст.

На сьогоднішній день існує два типи криптографії: симетричний та асиметричний [1]. Симетрична криптографія використовує ключ для шифрування та розшифрування відповідно простого тексту та тексту шифру. Єдиною умовою тут є те, що він має один і той же ключ для шифрування та дешифрування, а також вимагає менше часу на виконання. Криптографія асиметричного ключа використовує два ключі, названі як приватний ключ і відкритий ключ. Відкритий ключ надається одержувачем відправника для шифрування повідомлення, тоді як приватний ключ застосовується самим одержувачем для розшифрування повідомлення. Ключі можна повторно використовувати з іншими об'єктами.

Таким чином, стеганографія - це наука, яка займається тим, як комунікацію можна замаскувати, тоді як криптографія - це наука про перетворення змісту комунікації на неясність. Це також передбачає різницю між порушенням системи захисту: стеганографія зазнає поразки, якщо виявлено наявність стеганографії, тоді як у криптографії зловмисник не повинен вміти прочитати секретне повідомлення, інакше система буде порушена. Захищеність стеганографії залежить від секретності системи кодування даних. Технічні характеристики сучасних обчислювальних систем є дуже потужними, що дозволяє при використанні таких інструментів захисту інформації як криптографія та стеганографія застосовувати складні математичні алгоритми.

Використані джерела:

1. Мухачев В.А., Хорошко В.А. Методы практической криптографии. – К.: ООО «Полиграф Консалтинг», 2005. – 215 с.

Дембицька Т.П. - курсант факультету економіко-правової безпеки;
Тютченко С.М. – науковий керівник, старший викладач кафедри економічної та інформаційної безпеки (Дніпропетровський державний університет внутрішніх справ)

ВАЖЛИВІСТЬ ПОВНОВАЖЕНЬ ДЕПАРТАМЕНТУ ЗАХИСТУ ЕКОНОМІКИ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ В БОРОТЬБІ З ЕКОНОМІЧНИМИ ЗЛОЧИНАМИ

В сучасних умовах стрімкого технологічного та інформаційного розвитку національних економік високих обертів набирає економічна злочинність, яка на сьогодні характеризується загрозливими розмірами. Вчинення злочинів в сфері економіки становлять реальну небезпеку країни в цілому та окремих громадян. Постановою Кабінету Міністрів України від 13 жовтня 2015 р. було створено юридичну особу публічного права – Департамент захисту економіки Національної поліції України (ДЗЕ НПУ) як міжрегіональний територіальний орган Національної поліції з вертикальним підпорядкуванням, на який покладено функції протидії злочинності у сфері економіки [1,с. 3].

Відправною точкою кримінологічного дослідження протиправних дій у сфері економіки в нашій державі вважається перехід від адміністративно-командної до ринкової економіки, тобто в перехідний період соціально-економічного розвитку. Але економічні злочини також були широко поширені і в тоталітарну епоху. Головним засобом усереднення матеріальних потреб в радянську епоху була ліквідація і заборона приватної власності. Це породило нескінченні розтрати, розкрадання, підкупи, чорний ринок, таємний розпродаж казенного майна.

Злочини у бюджетній сфері, зокрема у сфері державних закупівель, є одним із найбільш відомих злочинів, який несе значну шкоду суспільству та державі в цілому. Так, протидії в даній сфері спрямовані на незаконне заволодіння державними коштами, а тому злочинцями в даних правопорушеннях виступають державні службовці - розпорядники бюджетних коштів.

Економічні злочини мають надзвичайно складний механізм здійснення, а отже і складний механізм їх виявлення та розслідування. Механізм злочину являє собою систему процесів взаємодії всіх учасників злочину між собою і навколишнім середовищем, що приводить до утворення криміналістично значущої інформації про злочин, його учасників та результати. Механізм злочину містить відомості про те, яким чином здійснено той чи інший злочин у сфері економіки. Особливість вчинення економічного злочину полягає в тому, що предметом такого протиправного діяння виступає майно як капітал,

а тому має місце підвищена організованість та використання специфічних способів поведінки. [2, с. 36]

Для ефективної протидії вищенаведеним правопорушенням на підрозділи захисту економіки покладено наступні завдання:

- участь у формуванні та забезпеченні реалізації державної політики у сфері боротьби зі злочинністю, захисту економіки та об'єктів права власності;
- виявлення, запобігання та припинення злочинів у сфері економіки, зокрема вчинених суспільно небезпечними організованими групами та злочинними організаціями, які впливають на соціально-економічну й криміногенну ситуацію в окремих регіонах та в державі загалом;
- боротьба з корупцією й хабарництвом у сферах, які мають стратегічне значення для економіки держави, а також серед посадових осіб органів державної влади та самоврядування;
- протидія корупційним правопорушенням;
- установлення причин та умов учинення правопорушень у сфері економіки, а також ужиття заходів щодо їх усунення [3, с.42].

Фактором, який приваблює злочинців до здійснення економічного злочину виступає розвиток кризових ситуацій в економіці, боротьба за економічну владу. Це дає можливість розширення застосування кримінальних способів заволодіння владою та здійснення протиправних порушень у сфері економіки.

Отже, економічним злочинам властива модернізація та пролонгована дія факторів, що означає певну часову затримку між фактором та дією. Це є причиною, яка ускладнює моніторинг та прогноз економічної злочинності, але не знімає необхідності стратегічних, стратегічних економічних, правових, управлінських та інших рішень. Департамент захисту економіки Національної поліції України має відповідні повноваження, які протистоять вчиненню економічних злочинів.

Використані джерела:

1. Кравчук С. Й. Економічна злочинність в Україні / С. Й. Кравчук. − [Електронний ресурс]. − Режим доступу: http://westudents.com.ua/knigi/116-ekonomchna-zlochinnst-v-ukran-kravchuk-sy.html
2. Меденцев А. М. Характеристика предмета та умов вчинення злочинів у сфері державних закупівель / А. М. Меденцев. − [Електронний ресурс]. − Режим доступу: http://www.vestnik-pravo.mgu.od.ua/archive/juspradenc8/65.pdf
3. Степанюк Р. Л. Типові технології злочинної діяльності в бюджетній сфері України / Р. Л. Степанюк // Форум права. − 2011. − № 1. − С. 977−981.

Жук А. - студент 1 курсу юридичного факультету;
Гавриш О.С. - науковий керівник, старший викладач кафедри економічної та інформаційної безпеки (Дніпропетровський державний університет внутрішніх справ)

БУЛІНГ, АБО ШКІЛЬНЕ ЦЬКУВАННЯ

Проблема булінгу на сьогоднішній день є актуальною і для українських шкіл. Зокрема, лише за останній рік десятки випадків булінгу в Україні та його наслідків активно висвітлювалися ЗМІ: починаючи від жорстокого побиття школярок однолітками у Чернігові, закінчуючи смертю школяра внаслідок завдання тяжких тілесних ушкоджень у школі на Одещині. І це лише найгучніші епізоди, яким, як правило, передують роки попереднього насильства, що часто замовчується навіть самими жертвами цькування.

Булінг (від англійського bullying) – цькування, залякування, агресивне переслідування одного з членів колективу з боку інших представників колективу. [1] На сьогодні ми маємо жахливу статистику. Як прилад, 48% дітей ніколи не розповідали дорослим про те, що однолітки застосовують до них психологічне, чи фізичне насильство. Ще 40% розповідали комусь з дорослих. Інші 22% вважають це нормальним явищем.

Вагомим фактором на булінг є реакція батьків. Якщо дитина сказала, що не хоче йти до школи, то це точно не характеризує її як ледачу. Є дуже велика вірогідність того, що вона не хоче йти до школи саме через булінг. [2]

Безумовно дитина проводить більшість часу у закладах освіти, будь то дитячий садочок, школа, коледж, чи університет. І саме працівники цих закладів зобов’язані першими реагувати на випадки булінгу. І діяти не шляхом наказу припинити свої діяння, а допомогти як агресору, так і постраждалому. Можливо комусь з них потрібна допомога психолога, чи батьків.

Причин булінгу дуже багато. Починаючи від зросту, та кольору волосся, закінчуючи сексуальною орієнтацією, чи кольором шкіри. Молодші школярі мають неодмінно звертатися по допомогу до дорослих — учителів і батьків. Допомога дорослих дуже потрібна і в будь-якому іншому віці, особливо якщо дії кривдників можуть завдати серйозної шкоди фізичному та психічному здоров'ю. Старші діти, підлітки можуть спробувати самостійно впоратись із деякими ситуаціями. Психологами було розроблено кілька порад для них. Як варіант можна ігнорувати кривдника, обов’язково стримувати гнів, та злість. Ні в якому разі не вступати в бійку. [3] Але краще не залишати це без відома дорослих. Про те, що тебе хтось ображає ніколи не соромно говорити. У кожному закладі освіти є психолог, який скоріш за все може тобі допомогти.

Зараз найпоширенішим видом булінгу є так званий “живий” булінг, власне коли цькують безпосередньо в лице. Якщо взяти до уваги відсотки, то це близько 80%. Менш поширений булінг у соціальних мережах, близько 19%. І

близько одного відсотку припадає на телефонні дзвінки, та месенджери.

Щодо санкцій за вчинення насильства. Відтепер за вчинення таких дій-янь стосовно неповнолітньої, або малолітньої особи на винуватцю буде необхідно сплатити штраф від 850 до 1700 гривень. Знущання, вчинені повторно упродовж року, або групою осіб каратимуться штрафом у розмірі від 1700 до 3400 грн, чи громадськими роботами на строк від 40 до 60 годин. У разі цькування неповнолітніми особами, віком від 14 до 16 років, відповідальність будуть нести батьки, або особи, що які замінюють. До них буде застосоване покарання у вигляді штрафу від 850 до 1700 грн або громадські роботи на строк від 20 до 40 годин. Також відповідальність передбачена за приховування фактів булінгу. Якщо керівник закладу освіти не повідомить поліцію про відомі йому випадки цькування серед учнів, його оштрафують на суму від 850 до 1700 грн або призначать виправні роботи на строк до одного місяця з відрахуванням до 20 % заробітку. [4]

Аби викорінити таке явище в Україні, та в цілому світі необхідно не лише говорити про це, а й навчати вчителів, проводити усілякі тренінги, ввести зміни у законодавство. Обов'язково проводити тренінги з дітьми, де їх будуть навчати як можна протидіяти булінгу, як не стати жертвою, та що треба робити якщо тобі довелося бути жертвою знущань.

Використані джерела:

1. Булінг в Україні та світі . [Електронний ресурс]. – Режим доступу: // https://www.radiosvoboda.org
2. Булінг – тиша яку ми маємо почути . [Електронний ресурс]. – Режим доступу: // https://glavcom.ua/
3. Протидія булінгу . [Електронний ресурс]. – Режим доступу: //http://llt.multycourse.com.ua/
4. Штрафи за булінг . [Електронний ресурс]. – Режим доступу: //. life.pravda.com.ua

Загоровська І.О. - курсант 3-го курсу факультету підготовки фахівців для органів досудового розслідування;

Прокопов С.О. – науковий керівник, старший викладач кафедри економічної та інформаційної безпеки (Дніпропетровський державний університет внутрішніх справ)

ПЕРСПЕКТИВИ РОЗВИТКУ ІНФОРМАЦІЙНОЇ ПІДСИСТЕМИ «ГАРПУН»

Живучи сьогоднішнім днем можна сказати, що людство вступає до нової ери, де одним із найвищих цінностей визнається інформація і знання тобто найбільш зростаючим ресурсом є розвиток інформаційних та комунікаційних технологій у всіх сферах економічного та суспільного життя.

На сьогодні підвищення рівня протидії злочинності є однією з найважливіших умов широкого використання сучасних досягнень науково-технічного прогресу, які останніми роками зробили прорив у сфері інформаційних технологій. Ефективність розслідування злочину полягає в отриманні інформації про криміналістичне значущі об'єкти, які можуть бути отримані із будь яких джерел. Серед джерел можуть бути сукупність інформаційно-пошукових систем, які створенні та функціонують у правоохоронних органів із метаю забезпечення процесу розслідування злочинів певною інформацією.[1 ст.326]

Інформаційні підсистеми «Гарпун» була створена відповідно до наказу МВС України № 497 від 13 червня 2018 року та застосовувалася збирання, накопичення, зберігання, а також для обробки відомостей про транспортні засоби усіх типів (автомобілі, автобуси, мотоцикли всіх типів, марок і моделей, самохідні машини, та інших) та номерні знаки ТЗ, які розшукуються у рамках кримінального, виконавчого проваджень, проваджень у справах про адміністративні правопорушення, оперативно-розшукової діяльності, а також за ухвалою слідчого судді, суду.

Однією з перших областей України у яких почала працювати інформаційна підсистема «Гарпун» була Дніпропетровська область.

Категорії обліку за якими інформаційна система «Гарпун» дає порядок формування [2]:

1. орієнтування про залишення ТЗ місця дорожньо-транспортної пригоди
2. орієнтування про залишення ТЗ місця вчинення іншого правопорушення
3. орієнтування оперативне про ТЗ
4. обліку за категорією "евакуйовані ТЗ"
5. розшук ТЗ за іншими кримінальними правопорушеннями
6. розшук ТЗ боржника державним виконавцем
7. розшук ТЗ боржника приватним виконавцем
8. розшук викраденого номерного знака
9. розшук втраченого номерного знака
10. знищені номерні знаки;

Інформаційна підсистема «Гарпун» є найбільш надійна система щодо фіксації злочинів. Вона здатна контролювати швидкісний режим на дорогох, фіксувати номерні знаки у разі угону автомобіля відповідно до чого звіряється з обліками викрадених транспортних засобів або номерних знаків. Відповідно до даного нарядові поліції легше та більш краще фіксується даний злочин. ІП «Гарпун» таким чином дає сигнал на пульт диспетчера відповідно до цього спрацьовує сигнал щодо потрапляння у поле зору відеокамери розшукуваного транспортного засобу.

Особливу увагу слід звернути на те що інформаційна підсистема «Гарпун» під час розшуку ТЗ та номерних знаків забезпечує взаємодію з державними та приватними виконавцями.

Інформаційна підсистема «Гарпун» створена для:

1. моніторингу тимчасових потоків даних про номерні знаки, що надходять із систем відеофіксації, на предмет їх розшуку;
2. передача розпізнаних номерів до ІПНП;
3. порівняння розпізнаних номерів з реєстром «Гарпун»;
4. забезпечення оперативного реагування посадовими особами органів поліції про розшук ТЗ та номерних знаків;
5. взаємодії з державними та приватними виконавцями під час розшуку ТЗ боржника у виконавчому провадженні.

Висновки. Отже, використання інформаційної підсистеми «Гарпун» значно підвищує ефективність процесів, зменшує затрати на їх проведення, дозволяє підвищити результативність роботи працівників правоохоронних органів. Система «Гарпун» автоматично створює картку в ЦУНАМІ та автоматично інформує наряди. Інформаційній підсистемі підлягають відомості про розшук транспортних засобів, які стали засобом або предметом кримінального або адміністративного правопорушення. У даній підсистемі міститься докладна інформація про ТЗ та подію правопорушення.

Використані джерела:

1. Бірюкова В.В теоретичні основи інформаційно-довідкового забезпечення розслідування злочинів \ Луган. держ. Ун-т. внутр.. справ ім. Е.О. Дідоренка. Луганськ: РВС ЛДУВС ім.. Е.О. Дідоренка 2009. 664 с.
2. Наказ МВС України від 13.06.2018 № 497 «Про затвердження Інструкції з формування та ведення інформаційної підсистеми “Гарпун” інформаційно-телекомунікаційної системи "Інформаційний портал Національної поліції України"»
3. Інформаційне забезпечення професійної діяльності : навч. посіб. / І.В. Краснобрижий, С.О. Прокопов, Е.В. Рижков – Дніпро : ДДУВС, 2018. – 218 с.
4. Безпека дорожнього руху: правові та організаційні аспекти: матеріали XIII Міжнародної науково-практичної конференції (в авторській редакції), (м. Кривий Ріг, 16 листопада 2018 року). – Кривий Ріг, 2018. – 195 с.

Кишкань М.А. - студент 1-го курсу юридичного факультету;
Гребенюк А.М. – науковий керівник, доцент кафедри економічної та інформаційної безпеки, кандидат технічних наук, доцент (Дніпропетровський державний університет внутрішніх справ)

РОЛЬ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ПРАВООХОРОННІЙ ТА ЮРИДИЧНІЙ ДІЯЛЬНОСТІ

Сучасне суспільство стоїть на шляху інформатизації: зростає роль інформації, формується телекомунікаційна інфраструктура, розширюється застосування інформаційних технологій. Більшість галузей діяльності людини

вже не уявляються без використання комп'ютерів та обчислювальної техніки. Проте досі існують сфери, де активне впровадження новітніх інформаційних технологій значно вповільнене. Найяскравішим з таких прикладів, внаслідок своєї консервативності, є юриспруденція. Основною частиною роботи кожного практикуючого юриста є пошук відповідних норм права, їх тлумачення та прийняття рішень. Тому логічно, що найбільш важливим та необхідним інструментом в юриспруденції мають бути всі види систем підтримки прийняття рішень [1, с. 22].

Правове забезпечення інформаційних технологій в правоохоронній та юридичній діяльності є актуальною темою, оскільки сьогодні в контексті європейської інтеграції та діджиталізації всіх сфер публічного управління надзвичайно важливим є забезпечення якісного та всеохоплюючого нормативного регулювання.

Сучасні інформаційні технології – це сукупність методів, виробничих процесів і програмно-технічних засобів, інтегрованих з метою збирання, обробки, зберігання, розповсюдження, відтворення і використання інформації в інтересах її користувачів [2, с. 76].

Основними тенденціями розвитку інформаційних технологій у правоохоронній сфері є: 1) удосконалення форм та методів управління системами інформаційного забезпечення; 2) централізація та інтеграція комп'ютерних банків даних; 3) впровадження новітніх комп'ютерних інформаційних технологій для ведення кримінологічних та криміналістичних обліків; 4) розбудова та широке використання ефективних та потужних комп'ютерних мереж; 5) застосування спеціалізованих засобів захисту інформації; 6) налагодження ефективного взаємообміну кримінологічною інформацією на міждержавному рівні. Все це забезпечує суттєве підвищення рівня боротьби зі злочинністю [3, с. 12].

Для сучасних фахівців-юристів своєчасне володіння актуальною, достовірною та повною інформацією є надзвичайно важливим елементом їх ефективної діяльності. Тому сучасні інформаційні технології не тільки міцно утвердились в юриспруденції, але й сприяють появі нових галузей та інститутів права, здійснюють безпосередній вплив на правове життя суспільства. Комп'ютерні технології є незамінним ефективним засобом роботи сучасного юриста та основним способом удосконалення її організації. Нині ефективність роботи юриста дуже часто визначає те, наскільки досконало він володіє тією або іншою комп'ютерною програмою [4, с. 39]

Боротьба зі злочинністю ведеться в країні широким фронтом різними державними органами, громадськими організаціями, громадянами. Особливо важлива роль у цій діяльності належить правоохоронним органам, для яких боротьба зі злочинністю є основною функцією. Значною мірою сьогодні ефективність діяльності правоохоронних органів залежить від технічного оснащення. Так, зокрема, в практичну діяльність органів Національної поліції України сьогодні широко впроваджується обчислювальна техніка, створюються локальні мережі, автоматизовані робочі місця, які обладнані сучасни-

ми потужними персональними комп'ютерами та базами даних. Все це дозволяє звільнити практичних працівників від виконання одноманітних операцій, допомагає знаходити оптимальні рішення при розв'язанні різноманітних питань, дає можливість глибше вивчати процеси, деталізувати їх, забезпечує можливість одночасного розгляду значної кількості фактів у взаємозв'язку та залежності при одночасній обробці різноманітної інформації. Використання обчислювальної техніки дозволяє по-новому підійти як до постановки конкретних завдань, так і до вибору оптимальних методів їх вирішення [3 с. 28].

Використання комп'ютерних технологій для вирішення тих чи інших правових завдань можливе лише за умови знання їх основних характеристик, можливостей, будови і принципу дії, а також наявності стійких навичок їх правильної експлуатації. Знання обчислювальної техніки, зокрема, персонального комп'ютера, сучасного стандартного та прикладного програмного забезпечення, уміле використання їх у практичній діяльності – це веління часу. Тому набуття всебічної комп'ютерної грамотності, підвищення загальної інформаційної культури працівників МВС та органів Національної поліції безумовно є актуальним завданням.

Серед найбільш потужних складових інформаційної системи, що використовується в правоохоронних органає, необхідно відмітити «Інтегровану інформаційно-пошукову системи МВС України» («АРМОР»), «ЄРДР», «НАІС», «АРКАН», «ЦУНАМІ». Практика боротьби зі злочинністю переконливо свідчить не тільки про суттєву, а в багатьох випадках пріоритетну роль системи інформаційного забезпечення МВС України як ланки, що значно зумовлює ефективність роботи всієї системи правоохоронних органів України [5].

Підбиваючи підсумки, необхідно зауважити, що юридична та правоохоронна діяльність мають бути належним чином забезпечені відповідними інформаційними технологіями, оскільки такі технології, окрім їх науково-технічного значення у виконанні державою своїх функцій, в тому числі захисної, дають змогу вести мову про відповідність, зокрема, національної правоохоронної системи сучасним критеріям ефективності функціонування такої системи у світі.

Використані джерела:

1. Різник О.М., Павлюченко Н.С. Аналіз існуючих систем підтримки прийняття рішень у галузі юриспруденції нові інформаційні і телекомунікаційні технології Математичні машини і системи, 2010, № 3. – 146 с.
2. Варенко В.М. Інформаційно-аналітична діяльність: Навч. посіб. / В. М. Варенко. – К.: Університет «Україна», 2014. – 417 с.
3. Інформаційні технології в правоохоронній діяльності : Посібник / В.А Кудінов., В.М.Смаглюк, Ю.І. Ігнатушко, Іщенко В.А. – К.: НАВСУ, 2013. – 82 с.
4. Сидоренко О.П. Правове забезпечення: до питання інтерпретації поняття. Актуальні проблеми вітчизняної юриспруденції. 2018. №1. 68 с.
5. Інформаційні технології. − [Електронний ресурс]. − URL: https://sites.google.com/site/infoormacijnitehnologiie/ (дата звернення 13.11.2019)

Кишкань М.А. - студент 1-го курсу юридичного факультету;
Рибальченко Л.В. – науковий керівник, доцент кафедри економічної та інформаційної безпеки, кандидат економічних наук, доцент (Дніпропетровський державний університет внутрішніх справ)

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ПРАВООХОРОННІЙ ТА ЮРИДИЧНІЙ ДІЯЛЬНОСТІ

Актуальність теми дослідження зумовлена потребою в узагальнюючому аналізі особливостей правового забезпечення інформаційних технологій в правоохоронній та юридичній діяльності, оскільки сьогодні в контексті європейської інтеграції та діджиталізації всіх сфер публічного управління надзвичайно важливим є забезпечення якісного та всеохоплюючого нормативного регулювання.

Проблеми правового забезпечення інформаційних технологій в правоохоронній та юридичній діяльності потрапила у сферу наукових інтересів таких вітчизняних дослідників, як В.Б. Авер'янов, Т.Б. Аріфходжаєва, Д.В._Артем'єва, В.В. Бабаскін, Л.В. Багрій, В.В. Іванова, С.М. Івасенко, Т.Є._Кагановська, О.Г. Кальман, О.М. Капля, І.П. Катеринчук, М.В. Ковалів, М.В. Колеснікова, М.Ю. Крєпакова, Ю.В. Пасмор, А.М. Подоляка, С.А._Подоляка, В.Я. Тацій, Д.О. Терещук, О.Г. Фролова, М.І. Хавронюк, В.С._Цимбалюк, С.О. Шатрава, Г.М. Шорохова, О.Х. Юлдашев, О.М. Юрченко та інші.

Метою дослідження є здійснення аналізу правового забезпечення інформаційних технологій в правоохоронній та юридичній діяльності.

В першу чергу пропонуємо визначити базові категорії дослідження. Інформаційні технології – це сукупність методів, виробничих процесів і програмно-технічних засобів, інтегрованих з метою збирання, опрацювання, зберігання, розповсюдження, показу і використання інформації в інтересах її користувачів [1].

Досліджуючи сутність і зміст поняття «правове забезпечення» ми доходимо до висновку про коректність визначення цього терміну, пропонованого О.П. Сидоренком, який позиціонує правове забезпечення як систему правових дій, які складаються у визначеній послідовності, спрямовані на досягнення правового результату, який може виражатись у формуванні юридичних норм, утворенні чи припиненні існування суб'єктів права, попередженні правопорушень або у виникненні, реалізації, зміні чи припиненні визначеної правової дії, а також в інших правових наслідках; кожна з правових дій, що складає процедуру, виступає як процедурна правова дія [2, с. 45].

Юридична діяльність - це вид соціальної діяльності, який здійснюють юристи з використанням юридичних засобів, дотримуються в установлених законом випадках юридичної форми з метою розв'язання різних юридичних

проблем. Правоохоронна діяльність, на нашу думку, є самостійним видом юридичної діяльності, спрямованим на припинення порушення, захист та охорону порушених прав, свобод та інтересів громадян.

На підставі вищевикладеного, пропонуємо наступне визначення правового забезпечення інформаційних технологій в правоохоронній та юридичній діяльності – це систему правових дій, які складаються у визначеній послідовності, спрямовані на досягнення правового результату у формі формування та розвитку сукупності методів, виробничих процесів і програмно-технічних засобів, інтегрованих з метою збирання, опрацювання, зберігання, розповсюдження, показу і використання інформації в інтересах її користувачів в сфері юридичної та правоохоронної діяльності.

Основними тенденціями розвитку правового забезпечення інформаційних технологій у правоохоронній сфері є:

1) розробка сучасних форм та методів управління системами інформаційного забезпечення;

2) централізація та інтеграція комп'ютерних банків даних;

3) впровадження новітніх інформаційних систем і технологій для ведення кримінологічних та криміналістичних обліків;

4) розбудова та широке використання ефективних та потужних комп'ютерних мереж;

5) застосування спеціалізованих засобів захисту інформації;

6) налагодження ефективного взаємообміну кримінологічною інформацією на міждержавному рівні. Все це забезпечує суттєве підвищення рівня боротьби зі злочинністю [3, с. 12].

На наше переконання, зазначені тенденції можуть бути доповнені такими пунктами, як неодноманітність практики вироблення правових норм, що регулюють формування та розвиток інформаційних технологій в правоохоронній та юридичній сфері; недостатній рівень технічного забезпечення, зумовлений недостатністю видатків з Державного бюджету на потреби розвитку інформаційних технологій та неактивна імплементація зарубіжного досвіду розбудови інформаційних мереж в юридичній та правоохоронній сферах.

Підбиваючи підсумки, хочу зауважити, що юридична та правоохоронна діяльність мають бути належним чином забезпечені відповідними інформаційними технологіями, оскільки такі технології, окрім їх науково-технічного значення у виконанні державою своїх функцій, в тому числі захисної, дають змогу вести мову про відповідність, зокрема, національної правоохоронної системи сучасним критеріям ефективності функціонування такої системи у світі.

Використані джерела:

1. Інформаційні технології. - [Електронний ресурс]. – URL: https://sites.google.com/site/infoormacijnitehnologiie/ (дата звернення 13.11.2019)
2. Сидоренко О.П. Правове забезпечення: до питання інтерпретації поняття. Актуальні проблеми вітчизняної юриспруденції. 2018. №1. С. 39-47.
3. Інформаційні технології в правоохоронній діяльності : Посібник / В.А Кудінов, В.М.Смаглюк, Ю.І. Ігнатушко, В.А. Іщенко - К.: НАВСУ, 2013. - 82с.

Кузьміна А. - курсант 1 курсу факультету підготовки фахівців для органів досудового розслідування;
Мирошниченко В.О. – науковий керівник, професор кафедри економічної та інформаційної безпеки, кандидат технічних наук, доцент (Дніпропетровський державний університет внутрішніх справ)

ФІНАНСОВЕ ШАХРАЙСТВО В СОЦІАЛЬНИХ МЕРЕЖАХ

Привабливість інтернет-магазинів важко недооцінити: багатий вибір, демократична ціна, доставка до дверей. У сучасних магазинах соціальної мережі можна знайти все, що завгодно за ціною нижче, ніж у звичайних магазинах. Ми настільки довірливі, тому можемо купувати в Інтернеті, але часто стаємо неуважними, чим і користуються шахраї. За інерцією довіряємо всім магазинам незалежно від його пізнаваності і наявності відгуків.

Зазвичай схема така: створюється один сайт, на якому викладаються товари однієї номенклатурної ознаки. Наприклад, дитяче взуття певної торгової марки. Ціна на запропоновані товари зазвичай нижче середньо ринкової. На такому сайті немає ні відгуків, ні привабливого дизайну. Тільки небагато інформації і, можливо, фільтр для зручного пошуку. Контактні дані заповнені теж дуже бідно.

Працюють такі інтернет-магазини найчастіше по 100% передоплаті. Покупець вибирає товар і потім оплачує його. Після чого протягом зазначеного терміну очікує відправку товару. Звичайно ніхто замовлення нікуди відправляти не буде. Зателефонувавши за вказаним телефоном, покупець виявить, що він не обслуговується, або просто не беруть слухавку.

Буває так, що в умовах передбачена можливість оплати за фактом отримання товару. У цьому випадку після оформлення замовлення, покупцеві на контактний E-mail або телефон приходить повідомлення, що в разі передоплати доставка безкоштовна (або інформація про інші вигоди). При цьому часто для оплати скидається не банківські реквізити, а номер електронного гаманця і після отримання грошей псевдопродавець зникає.

Також широко розповсюджені в Інтернеті схеми шахрайства з роботою. Варіантів маса, а найпоширеніші такі:

1. Пропонують виконати роботу, наприклад, написати текст, створити картинку, змонтувати відео. Отримують результат і не оплачують його.

2. Пропонують високий стабільний дохід за декілька годин, наприклад, розміщення реклами. Після тижнів старанної праці працівник отримує замість обіцяних коштів кілька сотень гривень. Це пояснюють по-різному: тільки почав, далі буде більше, не дотримана будь-яка умова, мало переходів по посиланнях і так далі. Так триває до того, поки людина не зрозуміє, що його обманюють.

3. Пропонують роботу з хорошою оплатою, але спочатку потрібно

зробити страховий внесок на той випадок, якщо ви не виконаєте роботу в строк та замовник не отримає результат. Те ж саме відбувається і зі збором ручок на дому. Потрібно заплатити за ручки, які вам надішлють за вказаною адресою. Звичайно ж, нічого ніхто надсилати не буде. Зробите внесок, і ваш дуже товариський і доброзичливий роботодавець вмить зникне.

Є й інший варіант обману. Шахрай дзвонить людині, яка є клієнтом будь-якого банку, і повідомляє, що у неї є заборгованість по кредиту і почала нараховуватися пеня. На що чує відповідь, що ніякого кредиту немає і, мабуть, помилка. Тоді дуже ввічливий «співробітник банку» просить уточнити особисті дані, щоб перевірити наявність заборгованості. А перелякана помилковим боргом людина, не замислюючись, повідомляє все, що у неї просять. Після чого з її рахунку зникають всі гроші. Пропозицій, під якими просять повідомити особисті дані, може бути дуже багато і звучать вони дуже правдоподібно. Навіть якщо карту, рахунок, аккаунт заблокують, клієнт завжди може зняти блокування при особистому візиті у відділення банку.

Щоб не бути обдуреними в Інтернет, можна порадити наступне:

•Не сприймати будь-яку отриману інформацію, як істину в останній інстанції. Перш ніж реагувати, треба задуматися, чи схоже це на правду. Ставте під сумнів навіть повідомлення в соціальних мережах, які ви отримали від друзів. Їх акаунт могли зламати.

•Не вірити обіцянкам величезної вигоди. Це стосується пропозицій заробити мільйони, віддавши пару тисяч гривень, і сенсаційних знижок. Всі знижки – це добре продуманий маркетинговий хід. Жоден продавець не стане віддавати товар нижче собівартості.

•Розголошувати особисті дані без реальної потреби. Досвідчені шахраї навіть мінімум інформації можуть перетворити на власну вигоду.

•Не реагувати на повідомлення і дзвінки з незнайомих номерів на фінансові пропозиції. Шахраї викликають сильні емоції для того, щоб було легше виманити жадані гроші.

•Бути пильними. Навряд чи можна перерахувати всі способи, як можуть обманювати в Інтернеті. Тільки уважність і недовіра до тих, хто просить, переконує і пропонує, зможе по-справжньому вберегти від шахраїв.

Варто відзначити, що шахрайство в Інтернеті – це діяльність, якою часто займаються люди, які володіють певними навичками. Наприклад, талановиті програмісти, хакери, колишні співробітники банків. Тобто їм для зняття грошей потрібно отримати мінімум інформації. Тому не варто особливо покладатися на те, що логін, пароль, підтвердження на телефон або пін-код вас по-справжньому убезпечать. Вони рятують від шахраїв-аматорів, а від профі вбереже тільки уважність. У випадку Інтернет - шахрайства завжди необхідно звернутися до спеціального відділу у структурі МВС України, який займається злочинами в Інтернет просторі [1].

Використані джерела:

1. Офіційний сайт кіберполіції України. - [Електронний ресурс]. − URL: https://cyberpolice.gov.ua.

Латиш А.В. - курсант 3-го курсу факультету підготовки фахівців для органів досудового розслідування;
Прокопов С.О. – науковий керівник**,** старший викладач кафедри економічної та інформаційної безпеки (Дніпропетровський державний університет внутрішніх справ)

ОСОБЛИВОСТІ РОЗСЛІДУВАННЯ ЗЛОЧИНІВ ПОВ'ЯЗАНИХ ІЗ НЕЗАКОННИМ ОБІГОМ НАРКОТИЧНИХ ЗАСОБІВ (НАРКОТИКІВ) ЧЕРЕЗ СУЧАСНІ ТЕЛЕКОМУНІКАЦІЙНІ СИСТЕМИ

У сучасному світі значного поширення набув певним чином новий спосіб незаконного обігу та розповсюдження наркотичних засобів через мережу Інтернет. Зазвичай дилерами (розповсюджувачами) є раніше судимі особи, а також до розповсюдження наркотиків причетні організовані злочинні групи. Спосіб розповсюдження наркотичних засобів та психотропних речовин через мережу інтернет, зокрема через час Telegram канал, дозволяє їх розповсюджувачам приховати свою злочинну діяльність від працівників правоохоронних органів, уникати безпосереднього контакту із покупцями.

Злочинці, з метою поширення своєї діяльності через мережу Інтернет, створюють різноманітні веб-сайти, блоги, канали, де розміщують весь асортимент «товару», створюють банківські рахунки з метою отримання коштів від потенційних покупців, а також підшукують осіб, основним завданням яких є забезпечення процесу передачі наркотичних речовин покупцеві, у тому числі, шляхом розміщення «закладок».

Відповідно до способів сучасного розповсюдження наркотичних засобів, слід постійно вдосконалювати підходи розслідування злочинів пов'язаних із незаконним обігом наркотичних засобів чи психотропних речовин. Враховуючи обставини збуту вказаних речовин через мережу Інтернет, наявність та повноту отриманої інформації, проаналізувавши судову практику, слід виділити основні типи слідчих ситуацій пов'язаних із подальшим алгоритмом проведення слідчих (розшукових) дій. [1, с. 18]

1) Через мережу Інтернет відбувся незаконний обіг наркотиків, є певні відомості про особу, яка розповсюджує їх.

В даному випадку слідчий встановив певні ознаки незаконного розповсюдження наркотиків за допомогою мережі Інтернет.

Основними завданнями слідчого, у даній ситуації, є фіксація ознак вчиненого злочину, встановлення особи (осіб), які продавали наркотики з використанням мережі Інтернет. Проводяться слідчі (розшукові) дії, негласні слідчі (розшукові) дії та інші заходи, характерні для розслідування злочинів пов'язаних із незаконним обігом наркотичних чи психотропних засобів [2].

При встановленні особи підозрюваного, відбувається типова слідча (розшукова) дія, а саме допит підозрюваного, під час якого, слідчий пови-

нен з'ясувати ознаки та обставини розповсюдження наркотиків через мережу Інтернет, використання спеціальних програм із метою поширення інформації про наявність «товару», визначити рахунок на який надходили кошти від продажу наркотичних речовин.

Отриманні під час допиту підозрюваного показання слідчий зобов'язаний перевірити. З цією метою проводиться огляд місця події (місце знаходження «закладки»), також огляд Інтернет-сторінки, сайту або каналу (на технічному пристрою затриманої особи) з метою знаходження оголошення, реклами, контактних даних осіб, які збувають наркотики у мережі Інтернет. Також за наявності даних щодо переписки між збутчиком та покупцем, слідчий має право отримати ухвалу слідчого судді на тимчасовий доступ до переписки, а переписку приєднати до провадження як доказ. Також слідчий призначає експертизу зразків наркотичної речовини (за її наявності) та комп'ютерно-технічну або телекомунікаційну експертизу вилучених при затриманні або в результаті обшуку технічних засобів, якими користувався підозрюваний з метою збуту.

2) Слідчому відома інформація про системний збут наркотиків з використанням мережі Інтернет, але відсутня або є незначна інформація щодо суб'єкта злочину.

В даному випадку можна говорити про самостійне виявлення слідчим або оперативним співробітником випадків збуту наркотиків через мережу Інтернет, отримання інформації про розповсюдження наркотичних речовин даним способом.

Слідчий фіксує факт незаконного збуту наркотиків через мережу Інтернет або сучасні інформаційні канали зв'язку, встановлює осіб, які збувають наркотики або є їх співучасниками та причетні до цього. Також проводяться слідчі (розшукові) дії, наприклад, допит свідка (або заявника), огляд місця події (Інтернет сторінки, веб-сайту тощо). Відповідно до ст. 40 КПК України слідчий направляє доручення працівникам оперативних підрозділів для проведення слідчих (розшукових) дій чи негласних слідчих (розшукових) дій. За погодженням з прокурором, слідчий направляє слідчому судді клопотання на здійснення тимчасового доступу до інформації про абонента якою володіє Інтернет провайдер встановлюється діапазон АР-адрес, з яких збувальник виходив у мережу. Встановлюються номери телефонів, на веб-сторінках. За погодженням з прокурором, подати клопотання слідчому судді на здійснення тимчасового доступу до інформації про абонента та деталізацію з'єднань, що міститься у оператора зв'язку, який обслуговує телефонний номер збувальника. Також слідчий проводить і інші дії, зокрема, допити, обшуки, затримання, направлення на експертизи тощо.

Таким чином, розслідування злочинів пов'язаних із незаконним обігом наркотичних засобів чи психотропних речовин через сучасні телекомунікаційні системи є досить складним та довготривалим процесом. Це вимагає від слідчого відповідного рівня знань, котрі забезпечать його діяльність на належному рівні.

Використані джерела:
1. Кваліфікація та розслідування злочинів, пов'язаних із незаконним збутом наркотичних засобів, психотропних речовин, їх аналогів та прекурсорів за допомогою мережі Інтернет: метод, реком. // О. Ю. Татаров, О. М. Стрільців, В. Б. Школьний та ін. К. : ГСУ МВС України, Нац. акад. внутр. справ, 2012. —30 с.
2. КРИМІНАЛЬНИЙ КОДЕКС УКРАЇНИ. [Електронний ресурс]. Режим доступу: http://zakon.rada.gov.ua/laws/show/2341-14.

Лозицький М.П. - курсант факультету підготовки фахівців для підрозділів превентивної діяльності;
Тютченко С.М. - науковий керівник, **с**тарший викладач кафедри економічної та інформаційної безпеки (Дніпропетровський державний університет внутрішніх справ)

ПРОБЛЕМИ ТІНЬОВОЇ ЕКОНОМІКИ В УКРАЇНІ

Одним з найбільш негативних явищ у процесі підвищення рівня економічної безпеки та становлення України як демократичної, так і соціально-правової держави є тіньова економіка. Бурхливому розвитку цього нелегального структурного явища економічної системи сприяли соціально-політичні зміни в 2014 році, спричинені війною на Сході країни. Наша країна, на жаль, на сьогодні займає перші позиції за відсотковою часткою тіньової економіки в усій економічній системі держави в цілому. Тіньова економіка в Україні стала основним детермінантом кризи в фінансово-економічному та соціальному секторі суспільних відносин. Масштаби тіньової економіки сягнули критичної точки, результатом чого стало зниження загальної конкурентоспроможності, ефективності фінансових, економічних та соціальних реформ.

Теоретичні основи функціонування тіньової економіки досліджували вітчизняні та зарубіжні вчені. На думку українських економістів, під тіньовою економікою слід розуміти економічну діяльність особи, яка пов'язана з незаконним привласненням особою, або групою осіб частини створеної споживчої вартості або частки майна через викривлення різного роду об'єктивної інформації про рух грошових коштів та матеріальних цінностей, спотворення даних первинного обліку, а також через реалізацію методом лобіювання відповідних законодавчих норм і нормативів, схем корисливого перетікання капіталу, здійснення яких не підлягає під кримінальну відповідальність, але призводить до матеріальних втрат державних або підприємницьких структур та окремих громадян [1, с. 37-38].

Для більш повного розуміння сутності тіньової економіки доцільно виділити її окремі види:

1) неформальний сектор – діяльність господарств, які виробляють та

споживають товари власного виробництва для власних потреб чи потреб членів сім'ї;

2) кримінальний сектор – виробництво та продаж незаконних товарів та послуг (наркотичні засоби, вибухівки, зброя, торгівля людьми та інше);

3) ілегальний сектор – незаконне виробництво та продаж легальних товарів без їх документального оформлення або реєстрації підприємств.

За даними Всесвітнього економічного форуму Україна станом на 2018 рік посіла 127 місце серед 136 країн світу, на території яких проводилися дослідження тіньової економіки. Гірші позиції займають тільки Гондурас, Єгипет, Кенія, Венесуела, Нігерія, Пакистан, Сальвадор, Ємен та Колумбія. Також аналітики стверджують, що небезпека зростання тіньової економіки стосується країн, в яких недавно пройшли громадянські конфлікти, війни, країни з недемократичним урядом, наркомафії [3, с. 33].

Відповідно до розрахунків Міністерства економічного розвитку та торгівлі України обсяг тіньової економіки в Україні за останні 5 років становить від 28 % до 39 % ВВП [4].

Високий рівень тінізації національної економіки України породжується певними причинами, серед яких можна виділити наступні:

1) неефективне державне регулювання економіки, а саме, відсутність довіри бізнесу до держави та держави до бізнесу; висока бюрократизація та недосконале інституційне та законодавче забезпечення;

2) неефективне адміністрування податків, що підтверджують рейтингові оцінки цієї сфери;

3) проблеми ринку праці, пов'язані з низькими економічними стимулами до офіційного працевлаштування працівників та зростання рівня безробіття;

4) недосконале кредитне-грошове регулювання, яке полягає в непрозорому рефінансуванні комерційних банків та встановленні гнучкого валютного курсу;

5) недосконаліть бюджетної системи, низький контроль за використанням бюджетних коштів;

6) недосконаліть судової та правоохоронної системи, відсутність чіткої державної програми боротьби з економічною злочинністю;

7) непродуктивний відплив капіталу з України;

8) корупція [1, с. 69].

Процеси тінізації властиві для будь-якої країни незалежно від типу та ступеня розвитку її економічної системи. Допустимою вважається частка, яка становить 5-10% від всієї національної економіки. Тож, Урядом України повинні бути розроблені практичні економічні заходи та прийняті конкретні правові рішення щодо зменшення рівня тінізації в економіці. До таких заходів протидії тіньовому сектору економіки можна віднести:

1) створення сприятливих умов для легалізації зайнятості населення;

2) запровадження податкових стимулів та інвестування коштів в національну економіку;

3) покращення інвестиційного клімату в країні;

4) розробка відповідного правового забезпечення процесу легалізації доходів;

5) формування мотиваційного нормативно-правового середовища, яке б забезпечило високоефективну та прибуткову роботу легальної економіки;

6) підсилення відповідальності правопорушників та посилення санкцій проти них для цілей виховання;

7) переорієнтація системи оподаткування з фіскальної на регулятивну функцію [2, с. 71].

Отже, важливість вирішення проблеми тіньової економіки України є дуже важливою та актуальною. Розвиток процесів тінізації в будь-якій економіці знижує рівень ВВП, загальну конкурентоспроможність, ефективність фінансових, економічних, соціальних реформ. Реалізація зазначених заходів сприятиме повноцінному надходженню фінансів до державного бюджету країни, сприятиме оздоровленню національній економіці, підвищенню інвестиційних показників, конкурентоспроможності, зниженню частки тіньової економіки до 5-10% від економічної системи України та побудові на цій основі ефективного ринкового середовища.

Використані джерела:

1. Липчанський О.В, Фільштен М.В. «Деякі питання боротьби з тіньовою економікою» // Наукові праці Кіровоградського національного технічного університету. Економічні науки. Ввипуск 21 // м. Кіровоград.- 2012, с. 37-39 , УДК 685
2. Мартинюк В.П., Хом'як К.А. «Боротьба з тіньовою економікою як пріоритетний напрям зміцнення фінансової безпеки» // Вісник Прикарпатського університету, Випуск XI.- 2015., с. 68-72 , УДК 330.338.24;
3. Усик П.С. «Окремі питання дослідження тіньового ринку зброї України» // Національна безпека . Міжнародний науковий журнал «Інтернаука» № 11 (51), 1 т.-2018;с. 31-36 ,УДК 338.583

Носач А.М. - студентка 1 курсу юридичного факультету;

Гавриш О.С. – науковий керівник, старший викладач кафедри економічної та інформаційної безпеки (Дніпропетровський державний університет внутрішніх справ)

БУЛІНГ - ПРОБЛЕМА ВІКОВОЇ ПСИХОЛОГІЇ

Актуальність проблеми виявляється в тому, що проблема булінгу в Україні до сих пір не є повністю відкритою. Відповідно до Конституції України (Частина перша стаття 3) людина, її життя і здоров'я, честь і гідність, недоторканість і безпека, визнаються в Україні найвищою соціальною цінніс-

тю. Цю істину повинен усвідомити кожний підліток. Булінг є предметом дослідження не тільки юридичної, але й психологічної та педагогічної наук. Найперші статті з питання булінгу (шкільного цькування) з'явилися у 1905 р. Дослідження вже більш ґрунтовні належать науковцям Скандинавії та Британії. Серед них Д. Лейн, Е. Мунте, Д. Ольвеус, А. Пікас, П. Рендолл, Д. Таттума та ін., які досліджували психологічні особливості учасників булінгу. С. Бурова, М. Дмитренко, О. Лавриненко, Л. Лушпай, О. Ожийова, В. Панок, В. Синьов та ін. є українськими науковцями, які вивчали булінг, спираючись на зарубіжний досвід.

Відповідно до даного ВОЗ, отримані в результатах моніторингового дослідження в Україні регулярно піддаються цькуванню в школі близько 17% дівчат і 16% хлопців 11-15-річного віку. Самі регулярно пригнічують інших 22% українських школярів.[1].

Ці дані підтверджують результати інших операцій, що перевірені Інтернет-сайтом KidsPoll (1200 дітей). Відповідно до нього, жертвами булінгу було 48% опитуваних, з них 15% дітей неодноразово підвергалися насиллю; 42% відгукуються, що самі займаються булінгом, 20% - постійно його бачать.

У перекладі з англійської буллінг (bullying) означає цькування, залякування, третирування [2]. Булінг – особливий вид психологічного насилля, який проявляється систематично, протягом тривалого часу по відношенню до більш слабкого учня, який відчуває страх, безсилля, пригніченість, ізольованість у відповідь.

Розглянемо наступні види булінгу. Фізичний булінг – штовхання, підніжки, зачіпання, бійки, стусани, ляпаси, «сканування» тіла, нанесення тілесних ушкоджень тощо. Економічний булінг – крадіжки, пошкодження чи знищення одягу та інших особистих речей жертви, вимагання грошей тощо. Психологічний булінг – принизливі погляди, жести, образливі рухи тіла, міміки обличчя, поширення образливих чуток, ізоляція, ігнорування, погрози, жарти, маніпуляції, шантаж тощо. Різновидом психологічного булінгу є кібербулінг – приниження за допомогою мобільних телефонів, Інтернету, інших електронних пристроїв (пересилка неоднозначних фото, обзивання по телефону, знімання на відео бійок чи інших принижень і викладання відео в мережу Інтернет, цькування через соціальні мережі) [3].

Самі основні аспекти булінгу – це страх; заздрощі та конкуренція; бажання підпорядковувати когось власній волі; бажання принизити іншого. Уважають, що жертвами булінгу стають діти чутливі, замкнуті, сором'язливі, тривожні, невпевнені в собі, нещасні, з низькою самоповагою, схильні до депресії, діти, які не мають жодного близького друга й успішніше спілкуються з дорослими, ніж з однолітками (Дан Ольвеус)

Представлені статистичні дані показують, що булінг – є явищем дуже глобальним та масовим. Школа – місце навчання, де діти перебувають у більшій частині дня, тут вони отримують знання, досвід, розвиваються, і також тут відбувається процес розподілу особистості, соціалізація. Зазначивши вищесказане, найголовнішим є, що важлива задача сучасної школи - визнання

істотності проблеми булінгування та створення відповідного середовища в освітніх навчальних закладах для профілактики та боротьби з негативними соціально-педагогічними наслідками цього явлення. Результати дослідження «Насильство в школі», проведеного в чотирьох регіонах України, показали, що третина з 1236 учнів з 20 шкіл Київської, Кіровоградської, Вінницької та Черкаської областей (від 24 до 37%) зазнавала фізичного чи психологічного насильства у школі [4].

На даний момент є дуже важливим, привернути увагу на превентивні заходи, а саме: ефективному управлінню навчальним закладом, коли чітко робиться акцент на неприпустимості булінгу; включенню тематики булінгу в навчальні програми; організації соціальних заходів (конференцій), присвячених означеній проблематиці. Важливе місце займає виховна робота батьків, психологічних служб, педагогічних працівників, церкви та правоохоронних органів. Зокрема, позитивну роль в даному випадку можуть відіграти підрозділи Національної поліції України, які розробляють та реалізують спеціальні програми для запобігання та протидії булінгу серед дітей.

Отже: булінг- явище, яке може виникнути в будь-якому шкільному колективі, за основу якого взято приниження честі на гідності особи. Булінг та катування є спорідненими поняттями. На відміну від катування, за вчинення булінгу настає не кримінальна, а адміністративна відповідальність. Проблема булінгу як явища, що зачіпає права та свободи дитини, повинна неодмінно бути утверджена в освітній політиці нашої держави.

Використані джерела:

1. Социальные детерминанты здоровья и благополучия подростков. Исследование «Поведение детей школьного возраста в отношении здоровья» : международный отчет по результатам обследования 2009–2010 гг. / под ред. С. Currie и др. – Копенгаген : Европ. регион. бюро ВОЗ, 2012 г. (Сер. Политика охраны здоровья детей и подростков. – Вып. №6).
2. Bullying / Мюллер В.К. // Новый англо-русский словарь; перераб. и доп. изд. [Электронный ресурс]. – Режим доступа: http://www.rambler. ru/dict/new-enru.
3. Права людини. Булінг як форма насилля. [Електронний ресурс]. – Режим доступу: // https://vseosvita.ua/library/prava-ludini-buling-akforma-nasilla-107015.html
4. Шершень А. Психологічне насильство серед школярів є більш болючим, ніж фізичне / А. Шершень. [Електронний ресурс]. – Режим доступу: // http:// www.mpravda. com

Остапенко Б. - курсант 1-го курсу факультету підготовки фахівців для органів досудового розслідування групи ДР-945;
Краснобрижий І.В. – науковий керівник, доцент кафедри економічної та інформаційної безпеки, кандидат юридичних наук (Дніпропетровський державний університет внутрішніх справ)

УДОСКОНАЛЕННЯ ОСВІТИ ЧЕРЕЗ АЛГОРИТМІЧНУ ПОСЛІДОВНІСТЬ ТЕСТОВИХ ЗАВДАНЬ.

У наш час проблематика удосконалення освіти набуває все більшої актуальності, у тому числі у сфері підготовки фахівців Національної поліції, тому зміни, з метою її покращення, стають все частішими і доступнішими. Поліція, як центральний орган виконавчої влади, який служить суспільству [1], повинен орієнтуватись у всіх життєвих випадках, що пов'язані з її діяльністю, але не завжди так трапляється, що всі ситуації зрозумілі з першого погляду для молодого працівника.

Ця теза є пропозицією, доповненням, або, так би мовити, додатковою функцією для вже існуючої квест-гри, що знаходиться у використанні у Дніпропетровському державному університеті внутрішніх справ на кафедрі економічної та інформаційної безпеки. Але ця квест-гра більш зосереджена на висвітлення роботи тільки "лінії 102" національної поліції, тобто можна побачити великі можливості для впровадження ще однієї програми чи квест-гри у сучасну систему навчання працівників національної.

Мова йде про труднощі у вирішені задач серед початківців, хоча ці ж життєві ситуації для досвідченої людини будуть здаватись простими. Звісно, проходження навчання у спеціально обладнаних кабінетах курсантами третього та четвертого курсу більш наближене до реального життя ніж та програма, яка запропонована у цьому тексті, але і можливості її застосування будуть актуальні для курсантів першого та другого курсів.

Перш за все про саму програму. Пропонується використання тестів, з різними діями на одну й ту саму ситуацію, які будуть тягнути за собою іншу алгоритмічну послідовність дій, що у кінцевому результаті буде вирахувана послідовність, та їх правильність.

Для прикладу можна навести класичну ситуацію приїзду патрульної поліції за викликом на місце події [2], цей приклад – спростована версія :

І. Поліція приїжджає на місце події, вони побачили труп невідомого чоловіка на вулиці. Що з початку повинен зробити патрульний?

А) викликати слідчо-оперативну групу(СОГ)

Б) проводити опитування людей, що знаходяться неподалік,

В) робити поверхневий огляд з метою виявлення предметів, що

пов’язані зі злочином.

Відповівши на одне з питань наступне питання буде подане відповідно до минулої відповіді, навіть якщо відповідь була не правильною, то курсант, який проходить тестування не буде усвідомлювати свою помилку, доки кількість помилок не буде досягати трьох. Ураховуючи, що кожна наступна відповідь після одного неправильного рішення вже буде автоматично, але непомітно вважатися як помилка. Минула відповідь буде записана поряд із наступним питанням, для більшої складності при повторному проходженні слід міняти місцями варіанти відповідей, для того щоб відповідь не зводилась до звичайного запам’ятовування літер. Наприклад:

II. {В} Після того як поліцейський зробив поверхневий огляд трупа він знайшов гаманець, що він повинен зробити ?

III. {В, Б} Викликавши СОГ, наступні дії поліцейського?

Така послідовність дій буде стимулювати курсантів до запам’ятовування дослівно алгоритму дій, що потім зробить навчання на старших курсах більш легшим.

Звісно, таке тестування може бути зосереджено не тільки у діяльності патрульної поліції, але й у інших фахових спрямуваннях:

- Робота оперативника, при роботі у СОГ;
- Робота слідчого при досудовому розслідувані [3];
- Дії дільничного при заяві про домашнє насильство;
- Виклик патрульної поліції на місце події;

Такий список є початковим і не досконалим, але більша зосередженість професіоналів на темі послідовності і точності дій при таких випадках дає змогу удосконалити її до ідеальних умов.

Завдяки впроваджені цієї програми в освітню систему правоохоронних органів рівень освіченості значно зросте, через набуття досвіду не з старших курсів, як це зазвичай буває, а з молодших (першого або другого). Варіативність можливостей при одній й тій самій ситуації визначає її неоднозначність та інтерес, а в перспективі й користь у майбутньому. Головне це підготувати спрощений матеріал для розуміння всіх аспектів для людини з малим досвідом у сфері діяльності поліції.

Використані джерела:

1. Закон України про Національну поліцію.
2. Наказ № 111 від 16.02.2018 "Про затвердження інструкції з організації реагування на заяви та повідомлення про кримінальні, адміністративні правопорушення або події та оперативного інформування в органах (підрозділах) Національної поліції України".
3. Наказ № 575 від 07.07.2017 "Про затвердження інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні".

Підопригора К.Б. – слухачка магістратури юридичного факультету;
Косиченко О.О. – науковий керівник, доцент кафедри економічної та інформаційної безпеки, кандидат технічних наук, доцент (Дніпропетровський державний університет внутрішніх справ).

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ОСОБИСТОСТІ, ТОВАРИСТВА І ДЕРЖАВИ

Сучасний розвиток суспільства породжує безліч загроз природного, техногенного, екологічного, конфліктного характеру, а також в частині поширення внутрішнього і міжнародного тероризму, погіршення транспортної безпеки, управлінських ризиків. Особливе місце з цього переліку відводиться загрозам інформаційної безпеки, до яких відносяться:

- порушення інформаційного забезпечення діяльності органів державної влади, муніципальних підприємств і служб;
- перехоплення трансляцій телерадіомовлення, систем оповіщення та інформування населення;
- несанкціонований доступ до інформації про діяльність органів державної влади, муніципальних підприємств і служб;
- несанкціонований доступ до управління інформаційними ресурсами;
- надання цілеспрямованого негативного інформаційного впливу на населення через засоби масової інформації і інформаційно-телекомунікаційну мережу Інтернет;
- неповна реалізація прав громадян в області отримання і обміну достовірної інформації, в тому числі маніпулювання масовою свідомістю з використанням інформаційно-психологічного впливу;
- провокування соціальної, міжнаціональної і релігійної напруженості через діяльність окремих (в тому числі електронних) засобів масової інформації;
- поширення зловживань в кредитно-фінансовій сфері, пов'язаних з проникненням в комп'ютерні системи і мережі.

В умовах таких загроз і ризиків громадяни потребують підвищення загального рівня суспільної безпеки, правопорядку і безпеки середовища проживання за рахунок істотного поліпшення координації діяльності сил і служб, відповідальних за рішення цих задач.

Завдання по нейтралізації загроз, мінімізації ризиків, запобігання збиткам в умовах інформаційного суспільства необхідно вирішувати шляхом

впровадження комплексної інформаційної системи, що забезпечує прогнозування, моніторинг, попередження і ліквідацію можливих загроз. Інформаційні технології необхідні для контролю і усунення наслідків надзвичайних ситуацій і правопорушень з інтеграцією під її управлінням дій інформаційно-керуючих підсистем чергових, диспетчерських, муніципальних служб для їх оперативної взаємодії в інтересах муніципальної освіти. [2]

Однією з основних невідкладних причин впровадження інформаційних технологій в управлінську та правоохоронну діяльність є інформаційно-технічний характер сучасної злочинності. Правозастосовна практика свідчить про те, що з кожним роком зростає число злочинів як в сфері комп'ютерної інформації, так і злочинів з використанням комп'ютерних технологій, в результаті чого формуються цифрові сліди злочинів. Із цього випливає, що розкривати і розслідувати злочини з використанням інформаційних технологій можливо тільки з використанням правоохоронними органами інформаційних технологій. Необхідність розвитку і впровадження інформаційних технологій пов'язана зі швидкістю прийняття рішень. В умовах динамічної економіки, всіх видів людської діяльності, заснованої на інформаційних технологіях, в критичних ситуаціях необхідно приймати грамотні управлінські рішення в найкоротші терміни. Названі і неназвані причини впровадження інформаційних технологій ставлять перед правоохоронними органами та органами державної, муніципальної влади завдання формування комунікаційної платформи з метою запобігання і усунення ризиків громадської безпеки, правопорядку і створення безпечного середовища проживання на базі міжвідомчої взаємодії. Для цього необхідно визначити потенційні точки уразливості, своєчасно реагувати на виникаючі загрози в надзвичайних ситуаціях. [1].

У сфері правоохоронної діяльності планується більш інтенсивно розвивати інформаційно-керуючі системи, системи обробки та ідентифікації дактилоскопічної, генної, балістичної та іншої криміналістично значимої інформації, програмне і інформаційне забезпечення перспективних та сучасних автоматизованих систем управління, інформаційно-довідкову роботу в інтересах підрозділів МВС.

Серед діючих ефективних інформаційних технологій, що забезпечують безпеку, слід назвати відеоспостереження і відео фіксацію, в тому числі зняття, обробку і передачу відео потоку з камер відеоспостереження про правопорушення і ситуаціях надзвичайного характеру, в тому числі пошкодження комунікацій, інфраструктури і майна. У цьому випадку проводиться аналіз відео- та аудіо потоків, включаючи: автоматичну реєстрацію подій на базі системи відео аналізу потоку; відео аналіз подій; аналітику відео-потоку в режимі реального часу; ідентифікацію і розпізнавання осіб.

Унікальні можливості використання інформаційних технологій в правозастосовній діяльності містяться в позиціонуванні рухомих об'єктів (геолокація). Геоінформаційні системи МВС - це складні інформаційні системи, створювані завдяки інтеграції баз даних звичайних інформаційних систем, функціонуючих в підрозділах МВС на певному рівні з базами даних відпові-

дної картографічної інформації, з метою представлення інформації певних об'єктів наочно в просторовому їх розташуванні на картах або планах. [3]

З метою розвитку геолокації і технологічної інфраструктури системи в інтересах державних та інших інформаційних систем, які здійснюють збір і обробку навігаційної інформації, що надходить від транспортних засобів, оснащених апаратурою супутникової навігації державою вживаються заходи щодо реалізації цих технологій. Для цього повинна бути створена комунікаційна платформа або єдиний інформаційний простір з урахуванням розмежування прав доступу до інформації різного характеру дозволить забезпечити інформаційний обмін між учасниками всіх державних і муніципальних органів виконавчої влади в області забезпечення безпеки.

В сучасних умовах інформаційні технології відіграють ключову роль в інформаційному забезпеченні розслідування злочинів. З інформаційних позицій інформаційне забезпечення - це сукупність єдиної системи збору та отримання інформації з зовнішніх і внутрішніх джерел, схем інформаційних потоків, що циркулюють в ході розкриття і розслідування злочинів, а також методологія використання наявних баз даних і побудови нових баз даних.

Нові інформаційні технології розширили не тільки слідчу картину злочинів, а й перелік предметів і документів речових доказів, що підлягають криміналістичної реєстрації. Реєстрація та довготривале зберігання інтернет-трафіку, всіх телефонних з'єднань, наявність взаємозв'язку абонента і базової станції, а також технічні можливості сучасних комп'ютерних засобів і систем управління базами даних дозволяють досить оперативно обробити колосальні обсяги комунікаційної інформації та отримати відомості, які полегшують розслідування злочинів. [1]

Крім цього, існують проблеми відомчої роз'єднаності, недостатності фінансування для закупівлі та впровадження інформаційних технологій. Названі проблеми необхідно враховувати всім зацікавленим суб'єктам інформаційних технологій і в зв'язку з цим формувати нові інформаційні правовідносини.

Узагальнюючи вищевикладене, можна сказати, що в сучасному інформаційному суспільстві, в умовах зростання загальних і інформаційних загроз, зростання комп'ютерної злочинності, повсюдного поширення штучного інтелекту, застосування інформаційних технологій у всіх сферах правоохоронної, економічної, регулятивної діяльності є необхідним, неминучим і найперспективнішим напрямом діяльності для забезпечення безпеки особистості, суспільства і держави. Для цього потрібне створення єдиного інформаційного середовища, що забезпечує ефективну і негайну взаємодію всіх сил і служб, відповідальних за громадську безпеку і правопорядок. Для підвищення ефективності діяльності по розкриттю і розслідування злочинів необхідно створити інтегровані банки даних криміналістично значимої інформації, досягти більш високого рівня інформатизації правоохоронних органів. Ступінь технічної оснащеності всіх органів попереднього розслідування телекомунікаційної інфраструктурою та інформаційними ресурсами повинен відповідати су-

часним викликам і технічним вимогам. При впровадженні інформаційних технологій в усі сфери державної і правоохоронної діяльності в гонитві за забезпеченням безпеки суспільства і держави не можна допустити перегинів, нехтування конституційними гарантіями прав особистості в сфері приватного життя. У новій структурі інформаційних правовідносин необхідно враховувати існуючі інформаційні загрози і ризики, забезпечувати гарантії права особи на приватне життя, безпеку суспільства і держави.

Використані джерела:

1. Белова Л. Г., Стриженко А. А. Информационное общество: трансформация экономических отношений в мировой экономике. М.; Барнаул: МГУ им. М. В. Ломоносова; Азбука, 2007. 387 с.
2. Петренко С.А., Курбатов В.А. Политика информационной безопасности. – М.: Компания АйТи, 2006.

Рец В.В. - курсант 3-го курсу факультету підготовки фахівців для органів досудового розслідування;
Прокопов С.О. - науковий керівник, старший викладач кафедри економічної та інформаційної безпеки (Дніпропетровський державний університет внутрішніх справ)

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ ЯК ІНСТРУМЕНТАРІЙ У БОРОТЬБІ ЗІ ЗЛОЧИННІСТЮ

Сучасна діяльність Національної поліції, пов’язана із виконанням базових завдань центрального органу виконавчої влади, в подальшому потребує вдосконаленого інформаційного забезпечення і розгалуженої системи інформаційних систем, які виконуватимуть, перш за все, превентивну функцію.

«Інформаційне забезпечення» є ключовою категорією в управлінській діяльності Національної поліції, ключовим її інструментом є поняття «інформація», за допомогою чого, власне, реалізується вся адміністративна функція та виконуються базові завдання правоохоронного органу. Тому цілком очевидно, що дана категорія привертає увагу багатьох фахівців у сфері інформатизації правозахисної і правозабезпечувальної діяльності поліції.

Під поняттям «інформаційне забезпечення» можна розуміти на тільки процес забезпечення інформацією, але і сукупність форм документів, нормативної бази та реалізованих рішень щодо обсягів, розміщення та форм існування інформації, яка знаходиться в системі і використовується у процесі функціонування інформаційне наповненого ядра [1, с. 299]. Таким чином інформаційне забезпечення має неоднозначну природу, тому що може бути

представлене як процес акумулювання і переробки інформації або як сукупність носіїв інформації.

Комплексний характер сфери охорони громадського порядку і безпеки вимагає належного інформаційно-аналітичного забезпечення. Ефективність роботи поліції у боротьбі зі злочинністю зміщується в бік розвитку аналітичної роботи, а саме накопичення і систематизації інформації у базах даних, виведення корисного інтегралі для підвищення коефіцієнту корисної дії органів та підрозділів Національної поліції України.

Інформаційне забезпечення діяльності Національної поліції, як і будь-яка інша галузь управлінського характеру, безперервно удосконалюється. Власне, таке удосконалення відбувається в аспекті взаємодії підрозділів Національної поліції в рамках інформаційної системи.

Сучасні інформаційні технології активізують діяльність поліції з приводу виконання її фундаментальних завдань. Зокрема, це стосується ситуаційних центрів «102», які за декілька років роботи довели дієвість і ефективність їх функціонування у складі правоохоронного органу. За такого високого результату роботи існує доволі проста схема, яка полягає у тому що:

- У цілодобовому режимі працівники служби «102» приймають телефонні дзвінки від громадян про правопорушення та інші події;
- Оператор вносить інформацію до електронної картки, яка автоматично надходить до диспетчера, відповідального за керування нарядами поліції, а також оперативному черговому відділу поліції, на території якого було вчинено злочин або правопорушення. Наряди поліції або групи швидкого реагування оперативно виїжджають на місце події;
- Крім цього, працівники служби «102» працюють з громадянами, тобто по телефону надають емоційно-психологічну підтримку заявнику після зіткнення з проблемною ситуацією, розповідають, що потрібно робити і як себе поводити в тих чи інших випадках, в які інстанції треба звертатися [2].

Щодо взаємодії, то уваги потребує питання можливості взяття первинної інформації слідчими підрозділами для подальшого опрацювання в рамках кримінального провадження. Іноді особливу цінність для встановлення обставин кримінального правопорушення містить первинна інформація, яка встановлює ланцюг дій та може навіть відобразити хронологію і розвиток подій. Багатьох практиків, які працюють в слідчих відділах цікавить питання взяття такої інформації у ситуаційному центрі в повному обсязі. Реальна можливість взяття такої інформації існує, тому що вся отримана впродовж певного проміжку часу інформація, направляється до аналітичного відділу, де належним чином систематизується і зберігається. Саме тому слідчий органу досудового розслідування може направити запит до аналітичного відділу колл-центру «102» і таким чином отримати вичерпну і всю наявну інформацію стосовно розслідуваного ним факту. Така інформація не є доказовою, але в подальшому вона може відіграти важливу роль для висунення слідчої версії.

Отже, сьогодні стрімко оновлюють форми і методи Національної полі-

ції у боротьбі зі злочинністю, одним із яких є суцільна інформатизація її діяльності. Саме тому виникають численні питання, на які вітчизняна наука ще має відповісти. Досить актуальним є питання взаємодії органів і підрозділів в системі Національної поліції України на основі інформаційного забезпечення і підвищення таким чином ефективності роботи правоохоронного органу.

Використані джерела:

1. Стокороса Т.М. Інформатизація та інформаційне забезпечення: підходи до трактування понять. Науковий вісник НЛТУ України. 2008. Випуск 18.9. с. 296-301.
2. Служба «102» як критерій оцінки роботи сучасної поліції. ВістіЛуг: [Електронний ресурс]. Режим доступу: URL: http://vistilug.com.ua/news/3028-sluzhba-102-yak-kriterii-otsinki-roboti-suchasnoi-politsii/ (дата звернення: 09.11.2019).

Русева А. - студентка 1 курсу юридичного факультету;
Гавриш О.С. – науковий керівник, старший викладач кафедри економічної та інформаційної безпеки (Дніпропетровський державний університет внутрішніх справ)

БУЛІНГ, ЯК ОДНА ІЗ ПРОБЛЕМ XXI СТОЛІТТЯ

В умовах сьогодення тема яка пов’язана з агресією та насильством, стає з кожним днем найбільш проблематичною та актуальною. Та, нажаль є місце, де ці слова звучать ледве не завжди. І територія, ця маленька модель суспільства, зветься школою. Діти та молодь є найбільш чутливими до змін, які відбуваються у сучасному соціумі. Коли раптом виявляється, що нове покоління на наш погляд стає більш жорстокішим та менш людяним. Тому дорослі мусять чесно відповісти на запитання – що ж вони повинні були б, могли б, і досі не зробили, - щоб наші діти не стали такими?

Шкільне насильство завжди було однією із проблем освітнього середовища. В кожному класі, є дитина яка завжди стає для своїх однолітків так би мовити «козлом відпущення». Однак за останні 30 років психологи, вчені. педагоги б’ють тривогу - настільки частим, жорстоким, цинічним стає це явище, що призводить до важких психологічних наслідків. Британські вчені дали цьому явищу визначення “булінг” [1 - с.177]. Проблема шкільного насильства були описанні в закордонних статтях ще в 1905 р. Перші систематичні дослідження терміну булінг належать скандинавським вченим, серед яких: Д.Олвеус, А.Пікас, Е.Роланд, П.Хайнеманн. Згодом інтерес до цієї проблеми виник у Великобританії. Серед британських дослідників слід виділити: Д.Лейна, Е.Мунте. В.Ортона, Д.Таттума, [1с.177]

У США особливу увагу до булінгу почали виявляти на початку 90-х років XX ст. Одне із цих досліджень проводилося в 1993 році в штаті Південна Ка-

роліна, було опитано 1420 підлітків, їхніх батьків та опікунів щодо цькувань на їхню адресу. Через 20 років медичне обстеження показало, що ті, хто раніше був жертвами переслідувань, частіше страждають на депресії, тривожні розлади, панічні атаки та агорафобії. Ініціатори переслідувань також увійшли у групу ризику, до того ж за чинником суїцидальних намірів [2 - с.216].

Якщо говорити за нашу країну, то проблема до кінця невивчена. Проте неможливо не зазначити такі робити, як О.Барліт, А.Барліт О.Л.Глазман, А.Король, Л.Лушпай, та інших, хоча ці дослідження ґрунтуються на закордонних розробках теорії булінгу [1 - с.177].

Відповідно до думки більшості дослідників, булінг включає чотири головних компоненти:

- це агресивна й негативна поведінка;
- вона здійснюється регулярно;
- вона відбувається у стосунках, учасники яких мають неоднакову владу;
- ця поведінка є навмисною [2 - с. 217].

Тому можна зробити висновок, що боулінг - це агресивна поведінка щодо окремої особи або групи, з метою приниження, домінування, фізичного чи психологічного самоствердження. Розрізняється два типи булінгу фізичний і психологічний. У вигляді психологічного тиску (образи, приниження, погрози, ігнорування тощо) та фізичних знущань (удари, поштовхи, принизливий фізичний контакт, побиття та інше). Нерідко фізичний і психологічний тиск об'єднуються.

Явища булінгу, має свої вікові, гендерні та інші особливості. Більшість досліджень показує , що в межах 5-9 класах середньої школи кількість випадків булінгу сягає максимуму, а вже у старших класах – знижується [2с. 217]. Щодо молодших школярів, більш раннє пілотажне дослідження показує, що вже у 8 років діти вміють користуватися всіма засобами булінгу, але справжніми булерами є лише деякі з них. Згідно попередніх результатів найбільш поширеними формами булінгу для молодших школярів були вербальні знущання, на другому місці – фізичні знущання та моральне пригнічення, на останньому – заборони та ігнорування [2 - с.217].

Стосовна гендерного аспекту, то вчений та дослідник І.Кон , вказує що це більш поширене в середовище хлопців. Це пов'язано не стільки з підвищеною агресивністю хлопчиків, скільки з особливостями хлоп'ячої нормативної культури, що помітно міняється з віком. Поняття як «крутість» і агресивність сприяють підвищенню статусу хлопчика в колі однолітків чоловічої статі, а потім і серед дівчат. Деякі дослідження показують, що більш напористі хлопчики мають більший успіх у дівчат, частіше мають побачення з ними. Стосовно протилежної статі, дівчата теж практикують булінг в реальному житті. Просто хлопчики й дівчата користуються різними формами булінгу. Якщо хлопчики частіше прибігають до фізичного булінгу (стусани, поштовхи й т.п.), то дівчата частіше користуються непрямими формами тиску (поширення слухів, виключення з кола спілкування тощо).

Булінг, тобто знущання дітей над дітьми, поширений в Америці, європейських та інших країнах (дослідження проводились в Норвегії, Англії, Ірландії, Нідерландах, Португалії, Австралії, Японії, Бразилії, Канаді), хоча згідно з дослідженнями, найчастіше він відбувається саме в американських школах. Так, наприклад, 86% дітей Сполучених Штатів у віці 12-15 років зазначили, що з них знущалися або дражнилися в школі. Австралійські дослідження показують, що 5-10% учнів залишаються вдома задля уникнення булінгу.

Згідно з результатами анкетування, проведеного Міністерством юстиції України, приблизно 67% українських дітей піддаються цькуванням, навіть не усвідомлюючи цього [3]. Якщо говорити за певні області нашої країни , то можна побачити такі показники : у Закарпатській області, половина опитаних школярів Київської області, і більше половини юних одеситів (45%) були свідками чи жертвами булінгу в школі. Серед чернівецьких школярів морального приниження хоч раз у житті зазнавали 48% учнів; фізичного кривдження − 27%; нападу з боку групи − 14%; пограбування − 12%; сексуальної загрози − 8% опитаних [1 - с. 178].

На запитання “Де, на Ваш погляд, підлітки найчастіше стикаються з проявами булінгу?” були отримані наступні відповіді: 11% респондентів вважають, що найчастіше підлітки зазнають насильства по дорозі до школи, 37% назвали місцем насильства вулицю біля школи, 42% - шкільний коридор, 5% шкільний туалет, 5% шкільну їдальню [1 - с. 178].

Отже , з вищесказаного можна зробити висновок, булінг – це специфічна форма агресивної поведінки, коли учень повторно чи постійно зазнає негативних дій з боку одного чи більше інших учнів. Виявлено, що булінг, за статистикою, є достатньо розповсюдженим явищем в шкільних підліткових колективах. Тому треба зазначити що роботу з запобіганням булінгу необхідно проводити не тільки з ймовірними булерами, а й зі спостерігачами (учнями та вчителями), адже часто діти не усвідомлюють, а дорослі не хочуть усвідомити всю серйозність і небезпеки булінгу.

Використані джерела:

1. Стремецька В.О. , Алєксєєнко Г.О. Булінг у підліткових шкільних колектива. Серія «Педагогіка, соціальна робота». Випуск 31. С. 177-179
2. Абсалямова К.З., Луценко О.Л. Булінг у середовищі молодшої школи – соціально-психологічні й особистісні аспекти. Вісник Харківського національного університету №1046. Розділ: Соціальна психологія. 2013. С. 216-221
3. Безп'ятчук Ж. Булінг у школі: чому українські діти такі жорстокі? BBC NEWS Україна. 2018. [Електронний ресурс]. – Режим доступу: // https://www.bbc.com/ukrainian/features-44425003

Сальнікова М.А. - курсант факультету підготовки фахівців для органів досудового розслідування;
Прокопов С.О. – науковий керівник, старший викладач кафедри економічної та інформаційної безпеки (Дніпропетровський державний університет внутрішніх справ)

ПРОБЛЕМИ МОНІТОРИНГУ БУЛІНГУ

Школа як один із агентів первинної соціалізації людини відіграє надзвичайно важливу роль у становленні й розвитку особистості, закладаючи в співпраці з родиною систему ціннісних координат, яку нинішня дитина надалі буде розвивати у своєму дорослому житті. Зрозуміло, що необхідною умовою для досягнення такої амбітної мети є створення безпечного та комфортного освітнього середовища, що підтримує особистість, яка розвивається, вчасно реагує на її потреби та з повагою ставиться до її особливостей. Разом з тим, насильство серед школярів – явище міждисциплінарне, тому існує безліч різних теорій, що пояснюють агресивну, насильницьку поведінку школярів. В наш час проблема булінгу (цькування) стала доволі розповсюдженим та масовим явищем: в багатьох країнах світу серед підлітків продовжують набувати поширення прояви жорстокості, агресії та психологічного тиску. Таким чином, наразі в нашій країні існує гостра потреба визначення заходів протидії та попередження даного явища.

Слід зауважити, що вивчення громадської думки надає необхідне інформаційне забезпечення для прийняття конкретних управлінських рішень, зокрема для прийняття стратегічних і тактичних планів із поліпшення ситуацій булінгу в країні, регіоні, локальній місцевості; визначення спільних інтересів у населення й поліції у сфері боротьби із булінгом; прийняття найбільш ефективних шляхів налагодження співпраці з населенням тощо [1, с. 209].

Моніторинг є цільовим спостереженням з орієнтацією на виявлення тенденцій розвитку з метою прогнозування ситуації, що змінюється. Мета моніторингу – понятійне інформативне забезпечення для визначення пріоритетів, методів і засобів підвищення ефективності діяльності чи реагування на події, факти [2, с. 321].

Зміст моніторингу складають процеси отримання, обробки й аналізу необхідної для формулювання кінцевих висновків інформації. Застосування відповідного методу не відрізняється особливою глибиною досліджень, його завдання – забезпечити своєчасне реагування на системні зміни.

Отже, одним із видів вищевказаного моніторингу є віктимологічний моніторинг (опитування) осіб, які стали жертвами булінгу. Одразу виникає проблема, оскільки явище булінгу існує серед дітей, які часто не розповіда-

ють про випадки насильства нікому, включаючи правоохоронні органи. Беручи до уваги вказану проблему, можливо її вирішити шляхом проведення анонімних опитувань серед школярів з метою виявлення тенденцій булінгу у певних соціальних колах дітей.

Разом з тим, опитування (моніторинг) вчителів також може мати перепони у встановленні об'єктивного інформаційного забезпечення. Маються на увазі випадки, коли навчальний колектив, бажаючи самостійно розібратися з булінгом у школі, не надає правдивої інформації щодо реального положення справ всередині колективу. Вирішенням зазначеної проблеми може бути закликання працівниками Національної поліції, зокрема представниками ювенальної поліції, до співпраці з метою попередження та боротьби із булінгом.

Окрім жертв булінгу та вчителів важливими об'єктами моніторингу залишаються батьки дітей, які або стали жертвами цькувань, або власне булери, оскільки вивчення типу виховання дітей у сім'ї, а також корекція порушень відносин є причиною зниження емоціонального благополуччя дитини та відхилень в її оптимальному психічному розвитку [3, с. 274].

Таким чином, у питанні моніторингу булінгу доцільно підходити комплексно, симбіотично поєднуючи намагання правоохоронних органів, педагогічного колективу, психологів та батьків у руслі протидії цькувань серед школярів. Так, на нашу думку, моніторинг слід проводити серед усієї рольової структури булінгу, тобто серед жертв, серед булерів, їх послідовників, а також пасивних свідків цькувань. Окрім цього, моніторинг слід проводити на загальношкільному рівні, а також на колективному (серед учнів визначеного класу) та індивідуальному рівнях.

Використані джерела:

1. Бесчастний В.М. Методи інформаційного забезпечення як інструментарій збору та обробки інформації про злочинність. *Право і суспільство.* № 1. 2017. С. 206-212.
2. Оболенський Ю.М. Розробка системи показників для моніторингу діяльності державних органів. *Університетські наукові записки.* 2005. № 3(15). С. 321-329.
3. Янішевська К.Д. Деякі проблеми протидії булінгу в Україні та шляхи їх вирішення. *Науковий юридичний журнал «Правові новели».* № 4. 2018. С. 270-275

Сауліна А.І. – слухачка магістратури юридичного факультету;
Рибальченко Л.В. – науковий керівник, доцент кафедри економічної та інформаційної безпеки (Дніпропетровський державний університет внутрішніх справ).

ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Сучасний етап соціально-економічного розвитку характеризується значними політичними, економічними, соціальними та екологічними змінами, стрімким розвитком науково-технічного прогресу, що проникає у всі сфери життєдіяльності людини. Кризові явища, що наростають в державі, посилюють невизначеність економічного становища та вимагають від суб'єктів господарювання посилення уваги до питань власної економічної безпеки, виявлення та нейтралізації можливих загроз, небезпек та ризиків, здатних негативним чином вплинути на стан та результати їх діяльності.

Економічна безпека підприємства – це запобігання усіляких загроз діяльності господарюючого суб'єкта, ефективне використання ресурсів для того, щоб забезпечити стале функціонування комерційної структури. Правильно побудована система забезпечення економічної безпеки дозволить проводити постійний моніторинг за діяльністю організації з метою виявлення загроз і профілактики в діяльності конкурентів, а також дозволить побудувати ефективну методику боротьби з виникаючими проблемами. Загрози діляться на внутрішні і зовнішні. До внутрішніх загроз можна віднести витік інформації, всілякі дії працівників організації, які можуть нашкодити діяльності організації, проблеми з партнерами фірми і так далі. До зовнішніх загроз відноситься недобросовісна конкуренція на ринку товарів і послуг, правопорушення законодавства з боку посадових осіб, а також постійна зміна законодавства. Для того, щоб правильно оцінити можливість виникнення такого роду загроз, необхідно проводити профілактичну роботу і боротьбу з подібними проблемами з метою побудови ефективної системи забезпечення економічної безпеки комерційної структури.

Важливими завдання економічної безпеки підприємства виступає: оцінка ризиків підприємства та їх аналіз; уникнення можливих ризиків та прогноз стану захисту підприємства; захист конфіденційності інформації та комерційної таємниці; ефективне та стратегічне управління системою економічної безпеки підприємства. До останньої належить: захист комерційної таємниці та конфіденційної інформації, інформаційна безпека, внутрішня та зовнішня безпека, конкурентна розвідка, кадрова, виробнича, фінансова, податкова та силова безпеки, а також інші.

Корпоративне шахрайство – одна з актуальних проблем сучасності. За статистикою, 5% прибутку світові компанії втрачають щорічно через несум-

лінні дії своїх співробітників. В Україні цей показник ще більший – у різних випадках він досягає 10–15 %. Ідеться тільки про ті втрати, які оприлюднені компаніями [1]. Ключовими ризиками, які провокують шахрайство у 2019 році є: відсутність систем внутрішніх контролів; самоусунення власника від прямого управління компанією; відсутність критеріїв виміру ефективності бізнесу; особисте небажання власника впроваджувати заходи протидії шахрайству; акцент на готівку при проведенні фінансових транзакцій.

Найкрупнішою у світі організацією по боротьбі із шахрайством ACFE досліджено, що у 2018 році у Східній Європі, а також Західній і Центральній Азії із 86 випадків найбільшим з професійних шахрайств є незаконне присвоєння активів, частка якого становить 83% від загальної частки усіх порушень. Ці випадки спричинили втрату у розмірі 150 000 доларів США. Фінансові схеми шахрайства були найменш поширеними і становили 10% від усіх випадків, а корупційні схеми траплялися у 60% випадків та спричинили у середньому втрату 300 000 доларів США. До організацій, які є жертвами професійного шахрайства належать: приватні компанії – 50% (збитки 115 тис.дол.США), публічні компанії – 43% (збитки 155 тис.дол.США), урядові – 1; неприбуткові – 2%, інші – 3% [2]. Із 86 випадків професійного шахрайства у Східній Європі, а також Західній і Центральній Азії у 2018 році в Україні лише 3, що менше, ніж середнє значення 4,3 з усіх випадків. Найбільше випадків професійного шахрайства у Сербії (9), Румунії (11), Турції (13) та Росії (15).

Цікавим фактом є те, як розмір організації пов'язаний із ризиком професійного шахрайства. З рис. 1 видно, що найбільший відсоток таких випадків у Східній Європі, а також Західній і Центральній Азії належить підприємствам, в яких кількість працівників становить від 100 до 999 (32%). Ці організації зазнали найбільших втрат на 1 млн.дол.США. Організації з кількістю від 1000 до 9999 працівників становлять 31% випадків, мали середню втрату у розмірі 30 тис. доларів США. Великі організації, де понад 10 000 працівників, складали 26% від усіх випадків понесли в середньому втрату в розмірі 275 тис.дол.США.

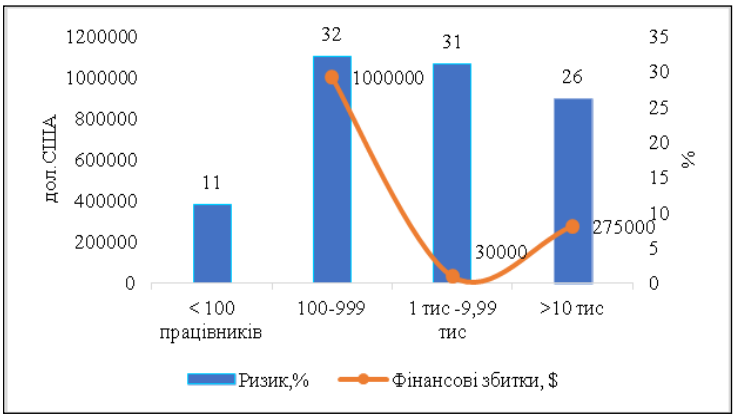


Рис. 1. Залежність розміру збитків від кількості працівників в компанії

Таким чином, для підприємств професійне шахрайство завдає значні збитки. Тому необхідно або залучати консультантів з боку, або збільшувати підрозділ, який займається забезпеченням економічної безпеки всієї організації в цілому. На підприємстві користуються певним набором математичних методів аналізу підприємства. У той же час, необхідно використовувати неструктуровані методи аналізу, що ускладнює отримати кількісні оцінки рівня забезпечення економічної безпеки. Сюди можна віднести: випуск продукції, рівень заробітної плати працівників, витрати на маркетингові заходи, щодо реалізації продукції на ринку товарів і послуг тощо.

Використані джерела:

1. Артем Ковбель. Шахрайство в компанії: що потрібно знати бізнесу. [Електронний ресурс]. – Режим доступу: https://uteka.ua/ua/publication/commerce-12-pravovie-soveti-67-moshennichestvo-v-kompanii-chto-nuzhno-znat-biznesu
2. Report To The Nations. 2018 Global Study On Occupational Fraud And Abuse. [Електронний ресурс]. – Режим доступу: https://www.acfe.com/report-to-the-nations/2018/#download

Свиридова М.С. - курсант 4 курсу факультету підготовки фахівців для підрозділів кримінальної поліції;
Прокопов С.О. – науковий керівник, старший викладач кафедри економічної та інформаційної безпеки (Дніпропетровський державний університет внутрішніх справ)

АКТУАЛЬНІ ПИТАННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Актуальним питанням на сьогоднішній день постала гібридна агресія до нашої країни з боку Росії. Постійно, зарубіжні країні планують ввести новітні зміні в інформаційний простір та намагаються вдосконалити технології його захисту.

Увага до цього питання дуже довго не була загострена з боку влади нашої держави, аж поки в червні 2017 року не сталась кібератака. Ця кібератака, повністю на певний період часу заблокувала діяльність не тільки тисячі компаній, але й нормальну діяльність державних органів[2]. Вірус, яким були заражені персональній комп’ютери, вимагав викуп у розмірі певної суми (валюта-доллар). Саме цією подією, весь світ зрозумів наскільки важлива кібербезпека та наскільки вона в нас не розвинена. Тому, з боку законодавства було прийнято новий закон, яким має напрям діяльності – сформувати загальнодержавну кібезбезпеку. На основі цього було створено відповідні підрозді-

ли в різних відомствах, які виконують покладені на них функції. Новим для України є факультет кіберзлочинності в Харкові. Вищий навчальний заклад зі специфічними умовами навчання подібний нашому ДДУВС, проте в ньому функціонує новий для інших ВНЗ факультет – боротьби з кіберзлочинністю. В такий спосіб, держава вирішила не тільки запровадити новітні зміни щодо захисту інформації та протидії кіберзлочинам, а повністю розробити систему, яка буде функціонувати та забезпечить безпеку інтересів громадян, та і України в цілому [1].

Також, ще одним прикладом забезпечення кібербезпеки є СБУ. На Службу безпеки України покладається розслідування кіберінцидентів та кібератак, здійснених проти державних інфосистем. Паралельно цьому Міністерство оборони має бути підготовленим так би мовити «до відбиття військової агресії в кіберпросторі». Ще одним прикладом є Національний банк України – в його повноваженнях, забезпечення кібербезпеки у сфері банківської діяльності.

За захищений доступ держорганів, антивірусний захист і аудит інформаційної безпеки відповідатиме Державний центр кіберзахисту.

Розвиток сучасних країн, дозволяє виділяти не просто злочини як убивство, крадіжка, незаконне поводження з вогнепальною зброєю тощо, а виділяє нові злочини – вчинені в кіберпросторі. В свою чергу це дасть можливість призначати покарання та засуджувати винних за вчинення таких діянь в Україні. Тобто, навряд чи будуть рецедиви в даній сфері, а отже запобігти майбутнім кіберзлочинам можливо.

Велику підтримку в забезпеченні кібербезпеки отримала Україна з боку зарубіжних країн. Не виключенням стали і США. Ще в в лютому 2018 конгресмени схвалили проект Закону про співпрацю з Україною з питань кібербезпеки, спрямований на просування активної взаємодії між Україною та США в сфері кібербезпеки [1]. Законопроект розроблено на Капітолійському пагорбі під керівництвом члена комітету з міжнародних справ палати представників Брендана Бойла – безпосередньо для української держави. В ході обговорення документа Бойл заявив: «Впродовж останніх років Росія використовувала Україну як полігон для кібератак, які ставлять під загрозу національну безпеку нашого великого союзника, України, а також її сусідів по регіону» [2]. Експерти зазначають, що це буде перший закон США в сфері кібербезпеки, де слово Україна винесено в заголовок.

Отже, підсумовуючи вищезазначене, слід вказати, що забезпечення кібербезпеки це одна з найважливіших складових в системі забезпечення нормальної діяльності країни. Забезпечення кібербезпеки завдання не окремої країни, це завдання всіх країн світу. Тому, для розроблення єдиного плану дій, необхідна підтримка один одного на законодавчому рівні та максимальне об’єднання сил. Забезпечення кібербезпеки в контексті глобальних загроз, поряд з спільними зусиллями міжнародного співтовариства, диктує важливість розробки і здійснення превентивних дієвих заходів проти кібератак і кіберзлочинів в світовому кіберпросторі

Бібліографічні посилання:

1. Від кібератаки вірусом Petya.A постраждали до 10 % комп'ютерів в Україні – Шимків [Електронний ресурс] / Новое Время. – Режим доступу : http://nv.ua/ukr/ukraine/events/vid-kiberatakivirusom-petya-a-postrazhdali-do-10- komp-juteriv-v-ukrajini-shimkiv-1442363.html
2. Спільно з Україною в ролі лідерів з кібербезпеки: Законопроект Конгресу США [Електронний ресурс] – Режим доступу : https://www.ukrinform.ua/rubric-polytics/2399870-spilno-z-ukrainou-v-rolilideriv-z-kiberbezpeki-zakonoproekt-kongresu-ssa.html

Сокол Р. - студентка 3 курсу факультету соціально-психологічної освіти та управління;
Гавриш О.С. – науковий керівник, старший викладач кафедри економічної та інформаційної безпеки (Дніпропетровський державний університет внутрішніх справ)

АГРЕСІЯ В СОЦІАЛЬНІЙ МЕРЕЖІ: РОЗПОВСЮДЖЕННЯ КІБЕРБУЛІНГУ В УКРАЇНІ

Фахівці зі сфери соціальних комунікацій та психологи зазначають, що чим більше ми занурюємось у соціальні мережі та стаємо співучасниками різноманітних дискусій — тим далі ми від справжнього життя. Всі ми пов'язані з мережами, існуємо в уявному світі, віримо в його символи, ніби вони реальні та по-справжньому емоційно реагуємо на віртуальну взаємодію з іншими людьми. Науковці вже не говорять про інтернет-залежність. Вони говорять про травму від інтернет-насилля та використовують для її ідентифікації спеціальний термін – кібербулінг.

Щодо світової практики, яка визначає булінг - як прояв дискримінації дитини, що виражається у фізичних і психічних формах насильства [1]. Форми прояву булінгу досить різноманітні: фізична (завдання ударів, штовхання, пошкодження або крадіжка власності), словесна (обзивання, глузування або висловлювання, якими ображається стать, раса або сексуальна орієнтація), соціальна (виключення інших із групи чи розповсюдження пліток або чуток), письмова форма (написання записок або знаків, що є болючими чи образливими) та безпосередньо електронна форма або кібербулінг (розповсюдження чуток та образливих коментарів з використанням електронної пошти, мобільних телефонів, сайтів соціальних мереж) [2].

Психолог із Києва, Світлана Паніна підкреслює, що: «Насильство у мережі має низку особливостей, через які ми стаємо більш вразливими до нього. І головна — це те, що конфлікт відбувається в уявному світі людини, а реакція на нього — на фізичному рівні людини. Якщо кількість переслідувачів, які цькують людину офлайн, зазвичай обмежена, у мережі масштаб кібербулінга може бути практично безмежним. Кібербулінг зазвичай розвиває-

ся «вірусно»: раптом виявляється, що велика кількість, зовсім не пов'язаних із постраждалими людей долучаються до переслідувачів. Це може завдати сильного психотравмуючого впливу.[3]

Наслідки онлайн-булінґу можуть бути різними. Зазвичай це зростання соціальної тривоги, часто аж до розвитку соціального тривожного розладу, посттравматичного стресового розладу, депресії, соматичних захворювань. А якщо масштаб насильства перетне адаптаційні можливості особистості, наслідки можуть бути фатальними, аж до суїциду.

Незважаючи на те, що кібербулінг є віртуальним, воно може завдавати абсолютно реальну шкоду емоційному здоров'ю постраждалих і змушувати їх замовкати у соціальних мережах. Численні образливі коментарі під постами чи погрози фізичним та сексуальним насильством з різних акаунтів можуть викликати стрес, депресію, апатію, посттравматичний стресовий розлад і навіть, суїцид».[4]

Згідно зі ст. 16 Конвенції про права дитини, остання має право на захист від незаконного посягання на її честь і гідність. Тому головним обов'язком держави є вжиття усіх заходів соціального, адміністративного, кримінально-правового та іншого характеру з метою надання дитині права на повноцінний та гармонійний розвиток особистості. З огляду на поширення явища булінгу в середовищі малолітніх і неповнолітніх осіб, необхідно розробити антибулінговий закон в Україні, внести це поняття до Цивільного кодексу України, Кримінального кодексу України. Для порівняння: у США учень, який постраждав 2012 року від проявів булінгу (справа Zeno v. Pine Plains Central School District) відсудив у школи 1 млн доларів компенсації за те, що адміністрація вжила лише формальних заходів для припинення його принижень та не пересвідчилась, чи припинилися онлайн переслідування.

В Україні існує проблема зі статистикою проявів кібербулінгу. Ні дорослі, ні діти не захищені від цього явища, а порушники не будуть притягнені до кримінальної відповідальності. Тому превентивний компонент — запобігання кібер-насильству та психологічна реабілітація тих, хто постраждав від кібербулінгу — одне з завдань експертної спільноти та громадських організацій, які працюють з проблематикою безпеки в громадах. Якщо для протидії проявів кібербулінгу по відношенню до дітей в Україні працюють різні програми (наприклад, Український інститут дослідження екстремізму та Інформаційне агентство «Главком» за підтримання Уповноваженого президента України з прав дитини реалізують спеціальний проект з протидії булінгу в школі «Стоп шкільний терор» («Безпечна школа»), то для дорослого населення превентивних заходів бракує.

Без сумніву, у сучасному інтернеті можна знайти різну інформацію: що публікувати у соцмережах, а що — ні, як забезпечити власну приватність — кожен може прочитати поради та зробити висновки. Але поки ми не маємо програм, які спрямовані на запобігання кібербулінгу і є частиною стратегії розвитку безпечної громади. Так само не маємо програм із корпоративної соціальної відповідальності, які б враховували протидію кібер-насиллю.

Використані джерела:
1. Куртова С. Булінг у школі // Освіта.UA : сайт. URL: http://osvita.ua/school/lessons_summary/upbring/42788/ (дата звернення: 23.10.2017)
2. Поляруш С. І. Поняття та проблема правового захисту від шкільного булінгу // Актуальні проблеми правової науки і державотворення в Україні в контексті правової інтеграції : матеріали X Міжнар. наук.-практ. конф., присвяч. 100-річчю підготовки охоронців правопорядку в Харкові (м. Суми, 20–21 трав. 2017 р.) / МВС України, Харків. нац. ун-т внутр. справ. Суми, 2017. С. 211–213
3. Нерівність. [Електронний ресурс]. – Режим доступу: // https://aimedia.org.ua/
4. Кібербезпека: як попередити віртуальне насилля?. [Електронний ресурс]. – Режим доступу: // https://ecpl.com.ua/news/14432/

Сорока А.О. - курсант 4 курсу факультету підготовки фахівців для підрозділів кримінальної поліції;
Прокопов С.О. – науковий керівник, старший викладач кафедри економічної та інформаційної безпеки (Дніпропетровський державний університет внутрішніх справ)

ПІДГОТОВКА ФАХІВЦІВ КРИМІНАЛЬНОЇ ПОЛІЦІЇ В ДДУВС

Досить швидка розбудова Національної поліції України зумовила високі та новітні реформи у даній сфері . зумовила виникнення потреби у забезпеченні підрозділів оновленою кадровою політикою [1]. Тому викладацький склад ДДУВС прикладає максимум зусиль для того, щоб надати всі необхідні знання та навички майбутнім фахівцям кримінальної поліції. З метою підвищення теоретичної підготовки та відпрацювання практичних навичок серед курсантів та студентів у Дніпропетровському державному університеті внутрішніх справ організовано комплексно-оперативні заняття «Лінія 102» [2]. Вони є прикладом того, як взаємодіють працівники правоохоронних органів при реагуванні та розкритті злочинів. За допомогою даної розробки , курсанти та студенти ДДУВС мають змогу практично відточити свої навички.

На нашу думку , великим позитивним моментом є вдале поєднання викладеної теорії у збірнику, розробленому викладачами ДДУВС, та практичними заняттями. Це дає змогу виявляти помилки та вчасно на них реагувати для своєчасного виправлення помило та недопущення їх у подальшій роботі. Досить зрозуміло та чітко викладено інформацію , яка має досить важливий характер.

Кожного року випускні (а саме четверті) курси та педагоги ДДУВС проводять комплексно-оперативні заняття «Лінія 102». Запроваджена новітня

форма підготовки дозволяє майбутнім офіцерам та юристам відчути себе в умовах максимально наближених до реальних, набути вміння та навички, які їм знадобляться в процесі виконання оперативно-службових завдань, юридичної та судової практики. Комплексно-оперативні заняття «Лінія 102» було розроблено в Дніпропетровському державному університеті внутрішніх справ з метою підвищення теоретичної підготовки та відпрацювання практичних навичок серед курсантів та студентів. Використання інноваційних методів під час відпрацювання даного тренінгу , надало змогу відточити навички правильного реагування на факти вчинення правопорушень та поєднати правове виховання з практичною підготовкою.

Заняття організовані у такий спосіб , що дозволяють чітко розподілити ролі, а відповідно і функції: слідчий виконує слідчі дії, оперативні співробітники проводять розшук по гарячим слідам. Свої обов'язки знають і криміналісти, починаючи від дактолоскопії, огляду місця скоєння злочину, закінчуючи затриманням злочинця. Також курсанти у такий спосіб вчаться складати процесуальні документи. Майбутні офіцери , тренуючись відпрацьовувати реагування на факт вчинення злочину можуть допустити помилки через необізнаність в певній сфері діяльності , але безмовно вони можуть розраховувати на допомогу з боку викладачів .

Також, завдяки «Лінії 102» курсанти унікальну можливість попрацювати з декількома робочими місцями заповнюючи електрону картку. А саме прослідкувати зміни , що відбуваються з нею – це етап обробки , етап коли патрульний екіпаж відреагував на виклик та етап в якому викладено кінцевий результат .

Дана «Лінія 102» була освоєна не тільки курсантами ДДУВС , а й представниками Литовської школи поліції. У травні 2018 року до ДДУВС завітали закордонні колеги та були досить приємно здивовані розробкою наших викладачів. Гостям показали матеріально-технічну базу університету, тренінгові центри та єдину в Україні , на сьогоднішній день, навчальну залу судових засідань. Також литовські поліцейські побували на самих комплексно-оперативних заняттях «Лінія 102», де змогли спостерігати, як відпрацьовується практична складова майбутніми поліцейськими в українському виші. Литовці не тільки захоплювалися нашими заняттями , а й поділилися досвідом як саме вони реагують на певні труднощі під час виконання службових завдань: при затриманні особи , при зупинці транспортного засобу , при веденні особою активного вогню тощо.

Отже, підготовка фахівців кримінальної поліції в ДДУВС – готує майбутніх поліцейських до виконання поставлених конкретних цілей на найвищому рівні , прикладаючи до цього максимальних зусиль не тільки нашими викладачами ДДУВС , а й залучаючи закордонних колег для обміну досвідом, тобто надає всі практичні та теоретичні навички , що будуть досить корисними під час безпосередньої роботи . Така розробка , як «Лінія 102» дає змогу на практиці відпрацювати та застосувати теоретичні знання отримані за роки навчання та відпрацювати швидке та неупереджене реагування на

факти скоєння злочинів. Це є добрим досвідом та великим вкладом від викладацького складу.

Використані джерела:

1. Кіщенко С. Реформа системи органів внутрішніх справ: аналіз державних рішень. Київ: Міжнародний центр перспективних досліджень, 2015. С. 13.
2. Гавриш О.С., Махницький О.В., Прокопов С.О. Інформаційно-технічна платформа інтерактивного комплексу з підготовки здобувачів вищої освіти та практичних працівників Національної поліції в ДДУВС/ Наукова стаття. Науковий журнал Право і суспільство. – 2017. – № 1-1. – С. 128–141.

Федорцов Д. В. - курсант факультету підготовки фахівців для підрозділів превентивної діяльності;
Тютченко С.М. – науковий керівник, старший викладач кафедри економічної та інформаційної безпеки (Дніпропетровський державний університет внутрішніх справ)

ІНФОРМАЦІЙНІ ВІЙНИ

Інформаційні війни – це заволодіння, використання та управління інформацією з метою набуття конкурентоздатної переваги над суперником із подальшим отриманням особистої вигоди різного характеру[1].

На сьогоднішній день понад 80% населення усієї планети користуються послугами мережі Інтернет, нехтуючи офіційними друкованими виданнями, або хоча б офіційними сайтами цих видань. У деяких випадках користувачів може ввести в оману недостовірна інформація, якою сьогодні переповнена майже вся мережа.

Допущені неточності, що за часту виникають через недосвідченість авторів публікацій призводить до затуманення свідомості осіб, що прагнуть якомога більше дізнатися про ту чи іншу інформацію, довіряючи неперевіреним джерелам.

Але й існують інші причини розміщення неправдивої інформації у мережі – умисно завантажена інформація з метою введення в оману значного кола осіб, що користуються цим джерелом. Причиною також може бути отримання власної вигоди завдяки своєчасній публікації певних даних. Як приклад останнього – публікація вкраденої наукової роботи, яка ще не отримала патент, тобто порушення права людини на інтелектуальну власність, і, відповідно – отримання матеріальної або іншої вигоди особою, що нажилася на чужій праці [2].

Достатньо розповсюджений вид інформаційного маніпулювання дани-

ми – це передвиборча агітація, що напередодні дня офіційного проведення виборів просто заполоняє весь простір рекламного ресурсу в мережі Інтернет.

Всі ці явища є проявом так званих інформаційних війн. Найнегативнішим наслідком цього явища є хронологічна невизначеність того, хто розпочав розповсюдження цієї інформації .

Більшість країн стають жертвами інформаційних війн. Коли до урядових серверів проникає вірус, що викрадає або підмінює чи взагалі видаляє досить важливі дані, що на пряму впливають на тактичні плани розвитку країн. Страждає не одна чи дві-три особи, а певний сегмент населення. Інформація може мати різний характер – як дані, що складуються та зберігаються на серверах до даних банківських систем, за допомогою яких можна проводити незаконні багатомільйонні операції з грошима людей. Такий різновид інформації відноситься до підриву якості інформації супротивника і збір тактичної інформації супротивником.

До різновидів інформаційних війн також можна віднести поширення інформації з метою деморалізувати населення . Приклади таких дій:

- Постійні провокації з боку журналістів. Прагнучи підвищити рейтинг ЗМІ, вони опускаються до лобіювання фактами на важливих конференціях та зустрічах, виставляючи владу у негативному світлі;
- Блогери – провокатори. З настаннями доби цифрових технологій вже ні для кого не складає особливих труднощів у використанні камери – як засобу фіксації певних подій; відеоредактором – як засобом монтажу відео; YouTube – як засобом поширення змонтованого ролика з метою висвітлення органів захисту або інших державних структур в образі ворога;
- Продажні «активісти». Це люди, що створюють негативну реакцію з боку населення у вигляді відгуків та коментарів на офіційних сайтах державних структур, за що отримують певну матеріальну.

Все вищесказане, можна привести до логічного висновку про нищівну потужність інформаційних війн. Інформація – це інструмент, що контролює усі сучасні процеси. За його допомогою можна створити щось суспільно корисне, так і завдати нищівний удар по державі. Найстрашнішим є те, що на відміну від бойових дій на передовій – інформаційні війни ведуться таємно, тобто не завжди можна визначити втручання у структуру державних систем.

Використані джерела:

1. Указ Президента України від 24 вересня 2001 р. № 891 "Про деякі заходи щодо захисту державних інформаційних ресурсів у мережах передачі даних".
2. Кузьменко А. М. Інформаційно-психологічна війна епохи глобалізації // Юридичний журнал. - 2008. - № 7-8.

Хитрук Р.О. - курсант факультету економіко-правової безпеки
Тютченко С.М. – науковий керівник, старший викладач кафедри економічної та інформаційної безпеки (Дніпропетровський державний університет внутрішніх справ)

ЕКОНОМІЧНІ ЗЛОЧИНИ У СФЕРІ ЗОВНІШНЬОЕКОНОМІЧНОЇ ДІЯЛЬНОСТІ

На сьогодні Україна є активним учасником у міжнародних зовнішньоекономічних відносинах. З виходом на міжнародний ринок розширилися й можливості для ефективного та вигідного ведення підприємницької діяльності для всіх суб'єктів господарювання. Після лібералізації у сфері зовнішньоекономічної діяльності значно розширились права її учасників. Їх отримали всі без винятку суб'єкти підприємницької діяльності, серед яких і фізичні особи, і міжнародні об'єднання та об'єднання фізичних і юридичних осіб, а також державні органи та органи місцевого самоврядування.

З визнанням України суверенною та демократичною державою, набуття ознак повноважного суб'єкта світового співтовариства стали поштовхом, що зумовив стрімкий розвиток активності учасників зовнішньоекономічних відносин у різних фрагментах економіки. На міжнародній арені ми підтвердили своє прагнення до встановлення рівноправного діалогу, який би ґрунтувався на поетапній державній стратегії щодо захисту національної економіки від різних видів злочинних посягань.

Але, на жаль, статистичні дослідження та висновки незалежних експертів містять дані про те, що вітчизняна сфера зовнішньоекономічної діяльності переповнена численними тіньовими капітал-оборотними схемами, які супроводжуються операціями з імпорту та експорту продукції. Однією із найрозповсюдженіших схем є «оптимізація» податків(ухилення від сплати податків), або ж переведення валюти на банківські рахунки фіктивних фірм українських резидентів за кордоном, зашифровування реальних власників інвестицій, які надходять для розвитку найбільш «вигідних» галузей української економіки, а також вчинення інших дій, що не передбачені законодавством. Всі ці протиправні дії створюють явну загрозу зовнішньоекономічній безпеці та негативно впливає на національну безпеку України [2].

Все це є наслідком негативного впливу штучно сформованого дисбалансу сукупного функціонування фінансово-господарського та правового механізмів , де координаторами виступають корумповані працівники правоохоронних органів та представники у контролюючій сфері. У таких ситуаціях їхні дії є наступними: у ручному режимі дані суб'єкти незаконних схем на власний розсуд приймають рішення щодо розміру митних платежів, податків,

кількості та якості кінцевого товару тощо. Така злочинна діяльність даних осіб тягне за собою настання помітних матеріальних збитків, які в результати знаходять своє відображення на мінімізації бюджетних надходжень, неправомірному зменшенні фінансових результатів від підприємницької діяльності суб'єктів цієї сфери при нарахуванні розмірів платежів до централізованих та децентралізованих фондів коштів, неправомірному виведенні валюти за межі України [4].

До злочинів у зовнішньоекономічній діяльності необхідно відносити:

- злочини, пов'язані з порушенням резидентами та органами валютного контролю (Державна податкова служба, Державна митна служба, НБУ інші уповноважені банки) вимог законів про зовнішньоекономічну діяльність, передусім при укладанні контрактів, здійсненні розрахунків, відшкодування ПДВ;
- злочини, скоєні на підприємствах усіх форм власності при здійсненні експорту або імпорту товарів;
- міжнародних фінансових операцій та операцій з цінними паперами; кредитних і розрахункових операцій (у т. ч. повернення валютної виручки) між вітчизняними та іноземними суб'єктами господарської діяльності; товарообмінних (бартерних) операцій та іншої діяльності, побудованої на формах зустрічної торгівлі між вітчизняними та іноземними суб'єктами господарювання;
- лізингових операціях між вітчизняними та іноземними суб'єктами господарської діяльності;
- незаконному ввезенні в Україну і вивезені за її межі товарів;
- злочини при проведенні службової діяльності працівників митних органів [1].

Аналіз ситуації доводить, що лише тісна співпраця компетентних органів з владою зможе запобігти розвитку тіньового аспекту у сфері зовнішньоекономічної діяльності, зменшити матеріальні втрати бюджету від незаконного перевезення товарів через кордон до України та забезпечити надходження додаткових коштів у відповідні фонди.

Використані джерела:

1. Щодо єдиного порядку обліку злочинів у сфері економіки: (Спільна вказівка Ген. прокуратури, МВС, ДПА та Служби безпеки України від 02.06.2004 р. № 12-157) [Електронний ресурс]. – Режим доступу : stat@uvddon.donec.ua
2. Документування злочинних дій хабарників: [методич. рекомендації] / за ред. В. І. Литвиненка ; [упоряд.: В. С. Гарлицький, О. О. Дульський, В. М. Конорєв, В. Б. Мо- цар]. – К. : РВВ МВС України, 2001. – 80 с. – С. 6.
3. Загрози без кордонів [Електронний ресурс] / Український Інтерпол: шляхом розвитку. – Режим доступу : http://www.niss.gov.ua/Tasko/017.htm
4. Про рішення РНБОУ «Про стан злочинності у державі та координацію діяльності органів державної влади у протидії злочинним проявам і корупції» : Указ Президента України від 27 жовт. 2009 р. № 870/2009 [Електронний ресурс]. – Режим доступу : http://zakon.rada.gov.ua

Чечель А.О. - курсант 2 курсу факультету підготовки фахівців для органів досудового розслідування;
Рижкова С.А. - науковий керівник, старший викладач кафедри адміністративного права, процесу та адміністративної діяльності (Дніпропетровський державний університет внутрішніх справ)

ДОСВІД ВИКОРИСТАННЯ ЧАТ- БОТІВ У ПРОТИДІЇ ЗЛОЧИННОСТІ

В умовах світового інформаційно-технологічного прогресу та інтеграційного руху до європейських стандартів в Україні почали активізуватися процеси реформування майже в усіх сферах життєдіяльності суспільства. Перш за все, це пояснюється новим рівнем свідомості сучасного населення та появою нових потреб, які необхідно задовольнити. Через велику кількість таких потреб виникає необхідність в їх відповідному регулюванні в рамках закону.

В період розвитку інформаційних технологій, виникають проблемами неврегульованої протиправної діяльності в соціальних мережах, наприклад, інтернет-булінг, торгівля наркотичними засобами, поширення інформації сексуального характеру, торгівля людьми, тощо. Тому сьогодні майже не можливо уявити підрозділи Національної поліції без належного технічного обладнання та інформаційного забезпечення, яке значною мірою покращує та полегшує їх діяльність.

На нашу думку, рівень протидії злочинності можливо значно підвищити за допомогою використання надбань сучасного науково-технічного прогресу. Одним з таких винаходів стали додатки під назвою «Чат-бот».Чат-бот - це програма, яка розроблена на основі поєднання машинного механізму та штучного інтелекту [1].

Нещодавно у Харківському національному університеті внутрішніх справ була презентована програма, розроблена в «Telegram», за допомогою якої користувачі можуть блокувати Інтернет магазини, які поширюються та продають наркотичні засоби. Робота вище зазначеного додатку полягає в тому, що користувач може зареєструватися в даній програмі в якості активіста. Бот буде надсилати такому користувачеві нарко-адреси, на які раніше надходили скарги, та матиме змогу за допомогою великої кількості таких активістів заблокувати той чи інший нарко-магазин. За допомогою цього додатку за короткий термін вже вдалося заблокувати 14 таких ресурсів [2].

З огляду на наведені позитивні аргументи, впровадження та використання «Чат-ботів» є необхідним нововведенням у протидії інтернет- злочинності. За допомогою машинного механізму та штучного інтелекту в цю програму вносяться відповідні дані, за допомогою яких можна виявити наркомагазини або інші негативні ресурси, які сприяють реалізації злочинних на-

мірів. Також з використанням сучасних інформаційних технологій в підрозділах Національної поліції вдасться регулювати не лише діяльність людей в реальному матеріальному світі, але й у віртуальному - в соціальних мережах, де за статистикою існує досить великий відсоток нелегальної та забороненої законами діяльності, яка залишається без покарання.

Отже, необхідно зазначити, що інтеграція сучасних інформаційних технологій до структурних підрозділів Національної поліції надає змогу реалізувати ефективний та сучасний механізм реагування на протиправні прояви злочинності в Інтернеті. За допомогою програми «Чат-бот», яка оснащена відповідними необхідними функціями, вдасться виявити не лише наркомагазини але і інші небезпечні інтернет-ресурси,. За умови впровадження новітніх технологій в діяльності поліцейських вдається підвищити їх оперативність та професіоналізм.

Список використаної літератури:

1. Что такое Чат-бот – Значение. SendPulse: веб-сайт. [Електронний ресурс] – Режим доступу: URL:https://sendpulse.ua/support/glossary/chatbot (дата звернення 14.11.2019).
2. В Харькове студенты создали чат-бота для борьбы с онлайн-наркоторговцами. 5 канал. веб-сайт. [Електронний ресурс] – Режим доступу: URL:https://www.5.ua/ru/amp/obshchestvo/v-kharkove-studenti-sozdaly-chat-bota-dlia-borbi-s-onlain-narkotorhovtsamy-kak-on-rabotaet-200901.html (дата звернення 14.11.2019).

Шевченко Т., Гринберг О. – курсанти 3-го курсу факультету підготовки фахівців для органів досудового розслідування групи ДР-744;
Краснобирижй І.В. – науковий керівник, доцент кафедри економічної та інформаційної безпеки, кандидат юридичних наук (Дніпропетровський державний університет внутрішніх справ)

АНАЛІЗ СТУПЕНЮ РОЗВИТКУ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ В СТРУКТУРІ ОРГАНІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

Нині, широко поширено використання сучасних технологій в повсякденному житті, тому стало актуальним їх використання і в роботі правоохоронних органів України. Створення нових виняткових можливостей для стрімкого та ефективного розвитку економічної, політичної та соціальної сфери життєдіяльності держави та громадськості. На сучасному етапі ми в змозі спостерігати зміни в кримінальному світі: у своїй діяльності вони застосовують новітні технології й досягнення науки, комп'ютерні системи. Іншими словами, у всьому світі відбувається процес інтенсивної інтелектуалізації злочинності [1, с. 48].

Однією з найбільш важливих і значущих проблем є одержання точної інформації на всіх стадіях протидії злочинності.

Аналізуючи останні дослідження та публікації ми дійшли до висновку, що інформатизація підрозділів органів Національної поліції на сучасному етапі стала більш глобальною та актуальною. Через стрімкий розвиток технічного прогресу виникає необхідність форсування процесу отримання і обробки інформації в роботі підрозділів, які здійснюють оперативно-розшукову діяльність. Над зазначеною проблемою працювали М. С. Вертузаєв, О. М. Бандурка В. Ю. Журавльов, А. Минаєв, В. В. Шендрик, які значно вплинули на процес дослідження цього питання. Окремо слід виділити роботи викладачів Дніпропетровського державного університету внутрішніх справ: Прокопова С.О., Рижкова Е.В. Проте питання інформатизації ще не опрацьовано в повному обсязі.

Значну роль при розслідуванні широкого спектра правопорушень відіграє її інформаційне забезпечення, об'єктивна організація та розумне використання отриманої інформації, яка знаходиться в обліках та автоматизованих інформаційних системах правоохоронних органів.

Перевагою електронно-інформаційних баз є: в першу чергу, вони містять індивідуальні відомості про кримінальне правопорушення, завдяки чому з'являється можливість встановити кримінологічні ознаки та тип кожного посягання, оцінити ступінь його суспільної небезпечності. Дані відомості дають можливість об'єктивно проаналізувати стан злочинності в реальному часі на певній території та оперативно реагувати на них, а також точніше прогнозувати її стан у майбутньому. [2, с. 52-57].

Вагому роль системи інформаційного забезпечення управління в правоохоронних органах підтверджується на нормативному рівні, зокрема наказом НПУ від 30 грудня 2015 р. № 228 створено Департамент інформаційної підтримки та координації поліції «102» НПУ, що організовує та здійснює передбачені законодавством України заходи, спрямовані на інформаційно-пошукове та інформаційно-аналітичне забезпечення правоохоронної діяльності та захист персональних даних під час їх обробки у структурних підрозділах апарату НПУ. Департамент інформаційної підтримки та координації поліції визначає основні напрями діяльності поліції у сфері інформатизації, здійснює інформаційно-пошукову та інформаційно-аналітичну роботу, приймає участь у розробці проектів нормативно-правових актів МВС із питань, що належать до компетенції поліції , а також обробки особистих даних в органах і підрозділах поліції [4].

Інтеграція та застосування новітніх інформаційних технологій є найголовнішою умовою покращення роботи діяльності підрозділів Національної поліції України та функціонування правоохоронної системи в цілому.

Однак існують такі проблеми:

- фінансове забезпечення;
- низький рівень володіння співробітниками наявними інформаційними ресурсами ;

- навички роботи з інноваційною технікою або новими системами.

Таким чином, ми дійшли до висновку, що використання потенціалу автоматизованих систем, програмно-апаратних комплексів, баз даних в органах державної влади в змозі кардинально підвищити рівень оперативного реагування на злочинність і пов'язані з нею фактори. Обмін інформацією та співпраця у діяльності правоохоронних органів, на даному етапі знаходиться на низькому рівні розвитку, і тому потребує вдосконалення. Її слід розглядати з двох сторін: зовнішня співпраця підрозділу з іншими службами (відомствами) та внутрішня співпраця між структурними підрозділами поліції та територіальними органами. Гальмуючим фактором в об'єднанні сил співробітників в підрозділах МВС є встановлена система показників розкриття злочинів як оцінки діяльності оперативних працівників, що спрямовує працівників на виконання роботи самостійно і відокремлено кожним підрозділом для урахування у статистичній звітності.

Використані джерела:

1. Максименко Ю.Є. Боротьба с тероризмом в умовах інформатизації / Ю.Є. Максименко // Правові проблеми сучасності. – К : Вид. Ліпкан О.С., 2013. – С. 48-50.
2. Кулик О. Кримінологічний аналіз злочинності в Україні: напрями вдосконалення методології та методики. Право України. 2009. № 7. С. 52–57
3. Бесчастний В.М. Окремі аспекти удосконалення інформаційного забезпечення протидії злочинності в системі Міністерства внутрішніх справ України [Електронний ресурс] – Режим доступу : http://www2.lvduvs.edu.ua/documents_pdf/biblioteka/nauk_konf/23_03_2018.pdf
4. Департамент інформаційної підтримки та координації поліції / Національна поліція України [Електронний ресурс] – Режим доступу http://old.npu.gov.ua/mvs/control/main/uk/publish/article/1820541

Шерстюк М. П. - курсант факультету підготовки фахівців для підрозділів превентивної діяльності;

Тютченко С.М. – науковий керівник, старший викладач кафедри економічної та інформаційної безпеки (Дніпропетровський державний університет внутрішніх справ)

ПРОБЛЕМИ ТІНЬОВОЇ ЕКОНОМІКИ В УКРАЇНІ

Одним з найбільш негативних явищ у процесі підвищення рівня економічної безпеки та становлення України як демократичної, так і соціально-правової держави є тіньова економіка. Бурхливому розвитку цього нелегального структурного явища економічної системи сприяли соціально-політичні зміни в 2014 році, спричинені війною на Сході країни. Наша країна, на жаль, на сьогодні займає перші позиції за відсотковою часткою тіньової економіки в усій економічній системі держави в цілому. Тіньова економіка в Україні

стала основним детермінантом кризи в фінансово-економічному та соціальному секторі суспільних відносин. Масштаби тіньової економіки сягнули критичної точки, результатом чого стало зниження загальної конкурентоспроможності, ефективності фінансових, економічних та соціальних реформ.

Теоретичні основи функціонування тіньової економіки досліджували вітчизняні та зарубіжні вчені. На думку українських економістів, під тіньовою економікою слід розуміти економічну діяльність особи, яка пов'язана з незаконним привласненням особою, або групою осіб частини створеної споживчої вартості або частки майна через викривлення різного роду об'єктивної інформації про рух грошових коштів та матеріальних цінностей, спотворення даних первинного обліку, а також через реалізацію методом лобіювання відповідних законодавчих норм і нормативів, схем корисливого перетікання капіталу, здійснення яких не підлягає під кримінальну відповідальність, але призводить до матеріальних втрат державних або підприємницьких структур та окремих громадян [1, с. 37-38].

Для більш повного розуміння сутності тіньової економіки доцільно виділити її окремі види:

4) неформальний сектор – діяльність господарств, які виробляють та споживають товари власного виробництва для власних потреб чи потреб членів сім'ї;

5) кримінальний сектор – виробництво та продаж незаконних товарів та послуг (наркотичні засоби, вибухівки, зброя, торгівля людьми та інше);

6) іллегальний сектор – незаконне виробництво та продаж легальних товарів без їх документального оформлення або реєстрації підприємств.

За даними Всесвітнього економічного форуму Україна станом на 2018 рік посіла 127 місце серед 136 країн світу, на території яких проводилися дослідження тіньової економіки. Гірші позиції займають тільки Гондурас, Єгипет, Кенія, Венесуела, Нігерія, Пакистан, Сальвадор, Ємен та Колумбія. Також аналітики стверджують, що небезпека зростання тіньової економіки стосується країн, в яких недавно пройшли громадянські конфлікти, війни, країни з недемократичним урядом, наркомафії [3, с. 33].

Відповідно до розрахунків Міністерства економічного розвитку та торгівлі України обсяг тіньової економіки в Україні за останні 5 років становить від 28 % до 39 % ВВП [4].

Високий рівень тінізації національної економіки України породжується певними причинами, серед яких можна виділити наступні:

1) неефективне державне регулювання економіки, а саме, відсутність довіри бізнесу до держави та держави до бізнесу; висока бюрократизація та недосконале інституційне та законодавче забезпечення;

2) неефективне адміністрування податків, що підтверджують рейтингові оцінки цієї сфери;

3) проблеми ринку праці, пов'язані з низькими економічними стимулами до офіційного працевлаштування працівників та зростання рівня безробіття;

4) недосконале кредитно-грошове регулювання, яке полягає в непрозо-

рому рефінансуванні комерційних банків та встановленні гнучкого валютного курсу;

5) недосконаліть бюджетної системи, низький контроль за використанням бюджетних коштів;

6) недосконаліть судової та правоохоронної системи, відсутність чіткої державної програми боротьби з економічною злочинністю;

7) непродуктивний відплив капіталу з України;

8) корупція [1, с. 69].

Процеси тінізації властиві для будь-якої країни незалежно від типу та ступеня розвитку її економічної системи. Допустимою вважається частка, яка становить 5-10% від всієї національної економіки. Тож, Урядом України повинні бути розроблені практичні економічні заходи та прийняті конкретні правові рішення щодо зменшення рівня тінізації в економіці. До таких заходів протидії тіньовому сектору економіки можна віднести:

8) створення сприятливих умов для легалізації зайнятості населення;

9) запровадження податкових стимулів та інвестування коштів в національну економіку;

10) покращення інвестиційного клімату в країні;

11) розробка відповідного правового забезпечення процесу легалізації доходів;

12) формування мотиваційного нормативно-правового середовища, яке б забезпечило високоефективну та прибуткову роботу легальної економіки;

13) підсилення відповідальності равопорушників та посилення санкцій проти них для цілей виховання;

14) переорієнтація системи оподаткування з фіскальної на регулятивну функцію [2, с. 71].

Отже, важливість вирішення проблеми тіньової економіки України є дуже важливою та актуальною. Розвиток процесів тінізації в будь-якій економіці знижує рівень ВВП, загальну конкурентоспроможність, ефективність фінансових, економічних, соціальних реформ. Реалізація зазначених заходів сприятиме повноцінному надходженню фінансів до державного бюджету країни, сприятиме оздоровленню національній економіці, підвищенню інвестиційних показників, конкурентоспроможності, зниженню частки тіньової економіки до 5-10% від економічної системи України та побудові на цій основі ефективного ринкового середовища.

Використані джерела:

1. Липчанський О.В, Фільштен М.В. «Деякі питання боротьби з тіньовою економікою» // Наукові праці Кіровоградського національного технічного університету. Економічні науки. Ввипуск 21 // м. Кіровоград.- 2012, с. 37-39 , УДК 685
2. Мартинюк В.П., Хом'як К.А. «Боротьба з тіньовою економікою як пріоритетний напрям зміцнення фінансової безпеки» // Вісник Прикарпатського університету, Випуск XI.- 2015., с. 68-72 , УДК 330.338.24;
3. Усик П.С. «Окремі питання дослідження тіньового ринку зброї України» // Національна безпека . Міжнародний науковий журнал «Інтернаука» № 11 (51), 1 т.-2018;с. 31-36 ,УДК 338.583

Наукове видання

ВИКОРИСТАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Матеріали Всеукраїнського науково-практичного семінару

(м. Дніпро, 28 листопада 2019 р.)

Упорядник: ***Косиченко О.О***. - доцент кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ, кандидат технічних наук, доцент

Підп. до друку 20.01.2019 р. Формат 60х84/16. Гарнітура – Times.
Друк трафаретний (RISO), цифровий. Папір офісний. Ум.-друк. арк. 8,25.
Обл.-вид. арк. 8,75. Тираж 50 прим. Зам. № 03/20-р,

Надруковано у Дніпропетровському державному університеті внутрішніх справ
49000, м. Дніпро, просп. Гагаріна, 26, т. (056) 370-96-59
Свідоцтво суб'єкта видавничої справи ДК № 6054 від 28.02.2018