Львівський державний університет внутрішніх справ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТІ ТА ПРАКТИЦІ

МАТЕРІАЛИ ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

17 грудня 2021 року

Львів 2021

УДК 004

І 78

Рекомендовано до друку Вченою радою Львівського державного університету внутрішніх справ (протокол № 5 від 30.12.2021)

РЕДАКЦІЙНА КОЛЕГІЯ:

І 78 **Інформаційні технології в освіті та практиці** : матеріали Всеукраїнської науковопрактичної конференції (Львів, 17 грудня 2021) / упорядник: Т. В. Магеровська. Львів : ЛьвДУВС, 2021. 97 с.

У збірнику вміщено наукові статті та тези за матеріалами доповідей учасників Всеукраїнської науково-практичної конференції «Інформаційні технології в освіті та практиці», що проводилася 17 грудня 2021 року у Львівському державному університеті внутрішніх справ.

УДК 004

Опубліковано в авторській редакції

Бурлака А. А.,
здобувач вищої освіти Державного податкового університету (Університету державної фіскальної служби України)

Мацюк А. М.,
доцент кафедри оперативно-розшукової діяльності Державного податкового університету (Університету державної фіскальної служби України), кандидат юридичних наук

ОПЕРАТИВНО-РОЗШУКОВА ДІЯЛЬНІСТЬ У РОЗРІЗІ КІБЕРЗЛОЧИННОСТІ В УМОВАХ СЬОГОДНЕННЯ

За умов сьогодення ефективними темпами у всі сфери людської діяльності запроваджуються високі технології. Майже відразу із появою комп'ютерних технологій появилися особи, які розпочали використовувати цей розвиток з протиправною метою. Якщо ж раніше це були люди, які володіли досить великим обсягом знань і досвідом в сфері високих технологій, то на даний час є непоодинокими випадки, коли комп'ютерну техніку з протиправною метою застосовують пересічні громадяни, які мають тільки базові навики роботи з нею.

На сучасному етапі практики правоохоронні органи не можуть лишатися осторонь і вже зараз активно протидіють кіберзлочинності. У свою чергу «кіберзлочинність» являє собою використання в процесі злочинної діяльності віртуального простору – кіберпростору. Відповідно і методи боротьби з такими злочинами в рамках здійснення оперативно-розшукової діяльності (далі – ОРД) повинні містити не лише стандартні прийоми, але й використання кіберпростору [1, с. 215].

Можна відзначити, що поняття «кіберпростір» виступає сполученням двох слів – «кібер» та «простір». Відповідно до одного з визначень великого тлумачного словника сучасної української мови [2, с. 1170] під простором розуміється вільний великий простір. Таким чином, буквально кіберпростір – це якась надтериторія. Якщо розглядати кіберпростір як скорочення словосполучення «кібернетичний простір», то кіберпростір – це простір, який створений, працює на основі принципів, методів кібернетики [2, с. 539].

Не менш значимим являється той факт, що досить часто кіберпростір асоціюється з терміном «інтернет», проте виходячи із цього випливає велике узагальнення, яке не бере до уваги певні випадки. Кіберпростір можемо розглядати так» 1) локальне середовище при функціонуванні засобу комп'ютерної техніки, який не підключено до мережі, та як розосереджене середовище, яке виникає в разі підключення засобу комп'ютерної техніки до 2) локальної або 3) глобальної мережі передачі даних [1, с. 216].

Виходячи з проаналізованих джерел, наразі є тенденція щодо трьох шляхів вирішення питання стосовно правового режиму інтернету і відповідно визначення компетенції держави в цій сфері: 1) інтернет є міжнародним простором, і його правовий режим має визначатися нормами міжнародного права; 2) інтернет є територією зі змішаним правовим режимом на кшталт континентального шельфу прибережних держав; 3) в окремих випадках інтернет можна віднести до державної території.

Так як питання регулювання відносин в інтернеті залишається не вирішеним на міжнародному рівні, Україні з цього питання слід керуватися основними принципами міжнародного права та чинним законодавством.

Після того, як було визначено поняття кіберпростору, його форми та компетенцію держави щодо нього, розглянемо питання застосування оперативно-розшукових повноважень в кіберпросторі. Відповідно до статті 8 Закону України «Про ОРД» [3] оперативно-розшукові підрозділи наділено рядом прав, які можуть бути реалізовані в тому числі і в кіберпросторі.

Слід зазначити, що використання оперативно-розшукових повноважень відносно українського сегменту кіберпростору не викликає багато правових питань. Водночас, якщо реалізація таких прав торкається іноземних юрисдикцій, можуть спричинюватися окремі правові неузгодженості. До того ж швидкість з'єднання і відсутність кордонів, які роблять кіберпростір надзвичайно зручним в користуванні, часто заважають правоохоронцям [4, с. 186].

Враховуючи вище зазначене, варто зауважити, що збирання інформації з відкритих джерел шляхом використання кіберпростору не потребує залучення інституту співробітництва.

Це складно, коли оперативникам необхідно спілкуватися через кіберпростір із очевидцями злочину або особами, які мають оперативний інтерес з інших країн. Такі дії можуть змусити інші держави

занепокоїтися про контакти своїх громадян з іноземцями, особливо якщо правоохоронці працюють під вигаданими іменами. Тому перед тим, як робити такі дії, необхідно ретельно зважити всі ризики та переваги. У разі виникнення ускладнень необхідно проконсультуватися з особою, яка відповідає за організацію та координацію міжнародної діяльності у своєму підрозділі. Те саме слід зробити у разі використання кіберпростору для заохочення осіб, які мають оперативний інтерес, прибути в Україну [1, с. 218].

В підсумку, можна стверджувати, що слід брати до уваги, що даний момент в правоохоронних органів України наявною є нагальна необхідність в розробленні методичних рекомендацій щодо використання кіберпростору. Запровадження цих документів в практичну діяльність дасть змогу заповнити присутні прогалини в даній сфері.

Література:

1. Манжай О.В. Використання кіберпростору в оперативно-розшуковій діяльності. *Право і безпека*. №4 (31). 2009. С. 215-219.
2. Бусел В.Т. Великий тлумачний словник сучасної української мови. Київ. Ірпінь : Перун, 2005. 1728 с.
3. Закон України «Про оперативно-розшукову діяльність» від 24.11.2021 року. *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua
4. Самойленко О.А., Волобуєв А.Ф. Основи методики розслідування злочинів, вчинених у кіберпросторі. *Монографія*. Одеса : ТЕС, 2020. 372 с.

Галайко Н. В.,
старший викладач кафедри соціально-поведінкових, гуманітарних наук та економічної безпеки Львівського державного університету внутрішніх справ

Шевченко Н. В.,
доцент кафедри фінансів та обліку Львівського державного університету внутрішніх справ, кандидат економічних наук, доцент

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В УПРАВЛІННІ ПІДПРИЄМСТВОМ

У наш час стрімко продовжується процес запровадження, удосконалення існуючих та розробка нових інформаційних технологій в усіх сферах суспільної діяльності. Під інформаційними технологіями слід розуміти систему методів і способів збору, передачі, накопичення, обробки, зберігання, подання і використання інформації. Інформаційні технології призначені для зниження трудомісткості процесів використання інформаційних ресурсів. Останні кілька років інформаційні технології щільно закріпилися у всіх сферах життя людини і суспільства: державне та місцеве управління, економіка, господарська діяльність, наукові дослідження, освіта, медицина та приватне життя людини. Менеджмент на підприємствах – не виняток.

Інформаційні системи та технології у сфері управління організацією – це методи, які дозволяють ефективно проводити планування, обмінюватися даними, контролювати постачання, а також здійснювати інші дії, спрямовані на оптимізацію робочих процесів та максимізацію прибутку. Вони виконуються на основі комп'ютерів чи іншої техніки.

Використання інформаційних систем і технологій у процесі управління підприємством робить його більш конкурентоспроможним, зокрема за рахунок об'єднання усіх структурних підрозділів в єдиний інформаційний простір, підвищення оперативності процесу аналізу результатів фінансово-господарської діяльності, надання керівництву різних рівнів управління економічно значимої аналітичної інформації, кращої адаптованості до змін ринкової кон'юнктури, налагодження швидкого і надійного зв'язку між структурними елементами системи тощо [1].

До основних переваг використання інформаційних технологій в управлінні підприємством віднесено: підвищення ступеню керованості; зниження впливу людського фактора; скорочення паперової роботи; підвищення оперативності і достовірності інформації; зниження витрат; оптимізація обліку та контролю; забезпечення прозорості інформації для інвесторів; можливість збільшення частки ринку [2].

Зазначимо те, що інформаційні технології на підприємствах існують у вигляді різноманітних інформаційних систем і інформаційних комплексів та використовуються в різних сегментах управлінської системи. Одні з найпоширеніших систем, що застосовують в управлінні підприємством подано в таблиці 1.

Таблиця 1.

Інформаційні системи та технології в управлінні підприємств

IT	Характеристика інформаційних систем та технологій в управлінні підприємств
MRP (Material Requirements Planning)	Планування матеріальних потоків. З використанням цієї системи керівництво корпорації здійснює придбання, виготовлення, і навіть реалізацію продукції
SCM (Supply Chain Management)	Адміністрування логістичних ланцюжків. Це концепція управління бізнесом як єдиним ланцюжком взаємозалежних об'єктів, матеріальних та інформаційних потоків підприємства, його постачальників, дистриб'юторів і клієнтів, виділяючи в свою чергу шість основних областей, на яких зосереджено управління ланцюгами поставок: виробництво, постачання, місце розташування, запаси, транспортування і інформація.
HRM (Human Resources Management)	Менеджмент людського фактора. Системи займаються пошуком потенційних співробітників, а також моніторингу їх діяльності.

CRM (Customer Relationship Management)	Управління взаємовідносинами з клієнтами. Основним завданням CRM є процес проведення автоматизованого збору даних про покупців і постійний інформаційний зв'язок з покупцями. З допомогою цієї технології можна автоматизувати частину роботи відділу маркетингу, кол-центру і так далі. Подібне рішення позитивно впливає на отримані наприкінці місяця доходи та рентабельність усієї компанії.
ERP (Enterprise Resource Planning)	Бізнес-планування і прогнозування. Ця система дозволяє управляти господарськими процесами. Вона працює на основі єдиної програми з однаковим інтерфейсом. Вона поширюється на низку сфер. До них відносяться: складання планів та прогнозів, менеджмент продажів, адміністрування випуску товарів, закупівель.
BPR (Business Process Reengineering)	Персональний внесок у процесі управління. Це аналітична система, що дозволяє менеджерам мати персоніфікований погляд на стан бізнесу.
MIS і BI (Management Information System and Business Intelligence)	Підтримка аналітичної діяльності, відслідковування циклу життя виробленого товару. Система призначена для зберігання даних, отриманих в результаті аналізу. Використання цих технологій спричиняє досягнення синергетичного ефекту; автоматизації та узгодження дії всіх відділів підприємства; успішної реалізації стратегічних програм; підвищення конкурентних переваг.
IBM Spectrum Protect	Захист даних підприємства. Даний продукт забезпечує надійне і економічно ефективне резервне копіювання і швидке відновлення в віртуальних, фізичних і хмарних середовищах будь-якого розміру. Ця платформа дозволяє централізувати контроль і адміністрування резервного копіювання та відновлення даних, захищає дані організації від апаратних збоїв та інших помилок, зберігаючи резервні і архівні копії даних в автономних сховищах

* Складено на основі [2-6].

Підсумовуючи вищенаведене, зазначимо, що якщо протягом століть інформація та знання передавалися на основі певних правил і приписів, а також традицій та звичаїв, то сьогодні найважливіша роль відводиться технологіям інформаційного характеру, що впливають не лише на виробничу сферу, а й на всі процеси та життя суспільства в цілому. Метою використання інформаційних технологій на підприємстві є вирішення завдань в управлінні об'єктами та процесами. Можемо з упевненістю сказати, що у сучасному менеджменті підприємств інформаційні технології застосовуються на різних етапах управлінської діяльності: планування ресурсів; організація постачання та збуту; взаємодія з клієнтами; регулювання споживчого попиту тощо. Важливо відзначити, що автоматизація – не самоціль, а цілеспрямована діяльність оптимізації бізнес-процесів. А з використанням описаних інформаційних систем та технологій можна максимально охопити всі сфери діяльності всередині організації. Кінцевою метою чого є розробка єдиного простору, у якому приймаються рішення.

Література:

1. Пурій Г. М. Інформаційні системи і технології в управлінні діяльністю підприємства. Ефективна економіка. 2019. № 6. URL: http://www.economy.nayka.com.ua/?op=1&z=7127 (дата звернення: 06.12.2021).
2. Онопко А.С., Жигалкевич Ж.М. Застосування інформаційних технологій в управлінні підприємством. URL: https://ela.kpi.ua/bitstream/123456789/22560/1/2017-11_2-18.pdf (дата звернення: 06.12.2021).
3. Laudon, K.C., Laudon, J.P., 1998. Management Information Systems, New Approaches to organization and technology. Ney Jersey: PrenticeHall, 395c.
4. Балановська Т. І., Гогуля О. П., Тужик К. Л. Особливості функціонування малого підприємництва в Україні. Інноваційна економіка. 2012. № 8 (34). С. 22–31.
5. Каюченко А.В. Информационные технологии управления предприятием как современый фактор конкурентоспособности предприятия. Креативная экономика. № 10 (34), 2009. С. 71–76.
6. Інформаційні технології в управлінні організацією: роль, мета та загальна характеристика управлінських IT. URL: https://www.cleverence.ru/articles/auto-busines/informatsionnye-tekhnologii-v-upravlenii-organizatsiey-rol-tsel/ (дата звернення: 06.12.2021).

Галайко Н. В.,
старший викладач кафедри соціально-поведінкових, гуманітарних наук та економічної безпеки Львівського державного університету внутрішніх справ

Бандерич Р. Р.,
здобувач вищої освіти Львівського державного університету внутрішніх справ

КІБЕРЗЛОЧИННІСТЬ В УКРАЇНІ

Сьогодні дуже важко уявити різні сфери діяльності суспільства без використання комп'ютерних та інформаційних технологій. Особливо чітко ми це відчули під час карантину, коли за допомогою мережі ми спілкуємось, працюємо, навчаємося, купуємо товари та послуги, здійснюємо різні банківські операції, шукаємо інформацію тощо. Використання всесвітньої мережі та нових технологій супроводжується такими явищами, як низький рівень культури безпеки, розвиток кібер-шахрайства, витоки інформації, втрата даних, несанкціонований доступ до інформації. Зловмисники дедалі частіше використовують Інтернет для своїх злочинних схем.

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», визначено поняття кіберзлочину (комп'ютерний злочин) – це суспільно небезпечне винне діяння у кіберпросторі та (або) з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та (або) яке визнано злочином міжнародними договорами України (п. 8 ст. 1) [1].

Кіберзлочинність у всьому світі щороку завдає збитків на десятки мільярдів доларів США як державам, так і приватним компаніям та людству. За офіційними даними Національної поліції України, у 2020 році було скоєно понад 5 тисяч кіберзлочинів. Серед яких найпоширенішими є: шахрайство з платіжними картками, крадіжки грошей з банківських рахунків, розповсюдження комп'ютерних вірусів, онлайн-торгівля наркотиками та зброєю, викрадення інформації тощо. Загалом у 2020 році збитків було завдано на суму понад 241 млн. грн, відшкодовано 78% – 189 млн. грн. [2]. За чотири місяці 2021 року, порівняно з минулим, кількість кіберзлочинів зросла на 25%. Основні види кіберзлочинів з якими стикається сучасне суспільство подпно на рис. 1.

Кардинг	•шахрайські операції з кредитними картками (реквізитами кредитних карток), які не погоджені власником картки.
Фішинг	•шахрайські дії, спрямовані на виманювання реквізитів картки у її власника.
Вішинг	• виманювання реквізитів картки зловмисники здійснюють за допомогою телефонних дзвінків.
Скімінг	•копіювання даних платіжної картки за допомогою спеціального пристрою (скімера).
Шимінг	•шахраї використовують майже непомітний прилад, який розміщують усередині картридера. Таким чином дані кредитки копіюються непомітно.
Онлайн-шахрайство	•фальшиві інтернет-аукціони, інтернет-магазини, сайти й телекомунікаційні засоби зв'язку.
Піратство	•протиправне розповсюдження об'єктів інтелектуальної власності в Інтернеті.
Мальваре	•створення та поширення вірусів і шкідливого програмного забезпечення.
Протиправний контент	•контент, який пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості й насильства.
Рефайлінг	•незаконна підміна телефонного трафіку.
Шахрайство з використанням ЕОТ	•власник електронного гаманця надає доступ шахраям до своїх акаунтів і вони переводять десятки тисяч доларів на інший гаманець.

Рис. 1 Найпоширеніші види кіберзлочинів [3]

Щодо класифікації кіберзлочинів, то в Конвенції Ради Європи про кіберзлочинність, яку Верховна Рада України ратифікувала й імплементувала до українського законодавства, виокремлено чотири основні типи кіберзлочинів:

- правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем – незаконний доступ, нелегальне перехоплення, втручання в дані, втручання в систему, зловживання пристроями;
- правопорушення, пов'язані з комп'ютерами, – підробка, пов'язана з комп'ютерами, шахрайство, пов'язане з комп'ютерами;
- правопорушення, пов'язані зі змістом, – правопорушення, пов'язані з дитячою порнографією;
- правопорушення, пов'язані з порушенням авторських і суміжних прав [3].

Повністю захиститися від кібератак неможливо. Однак дотримання принаймні мінімальних правил безпеки мережі значно збільшить шанси на те, що злочинці не зламають систему. Серед яких виокремимо:

- використовувати виключно офіційне програмне забезпечення, не завантажувати з ненадійних джерел та вчасно його оновлювати;
- використовувати антивіруси для роботи з комп'ютерами;
- не відкривати підозрілі листа та файли, не переходити за незрозумілими посиланнями;
- здійснювати резервне копіювання важливих файлів, не надавати доступу стороннім особам до свого комп'ютера та/або телефону, тримати свої гаджети в полі зору, коли перебуваєте у місцях, де до них може бути доступ сторонніх осіб;
- нікому не передавати особисті персональні дані (пін коди карток, CVV коди, паролі до акаунтів тощо);
- обережно здійснювати інтернет-покупки, користуватися лише офіційними й перевіреними сайтами, не здійснювати платіжних операцій у відкритій, незахищеній мережі Wi-Fi;
- намагатися користуватися двофакторною аутентифікацією [3, 4].

Виходячи з вищевикладеного, можна дійти невтішного висновку в тому, що частиною «ціни», яку доводиться сплачувати за інновації в цифровій сфері, є ризики кіберзлочинів, які набувають все більших масштабів, а кіберзлочинність є реальною загрозою національної безпеки. Тому, крім зазначених підходів та рішень, для боротьби з кіберзлочинністю необхідні ще свіжі підходи, що ґрунтуються на широкому використанні успіхів науки і техніки, а також підготовка співробітників нового покоління, що досконало володіють навичками комп'ютерних технологій та комп'ютерного програмування. А в цілому, віртуальний світ – це наша сучасність та майбутнє, тому ми повинні рухатись разом з часом та створювати безпечний кіберпростір для користувачів та держави.

Література:

1. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 р. № 2163-VIII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 06.12.2021).
2. Звіт Національної поліції України про результати роботи у 2020 році. URL: https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit2020/npu-zvit-2020.pdf (дата звернення: 06.12.2021).
3. Кіберзлочинність в Україні. Ера цифрових технологій – ера нових злочинів. URL: https://uz.ligazakon.ua/ua/magazine_article/EA013606 (дата звернення: 06.12.2021).
4. Кібербезпека: вразливі моменти. URL: https://yur-gazeta.com/publications/practice/inshe/kiberbezpeka-vrazlivi-momenti.html (дата звернення: 06.12.2021).

Гангола Н. Р.,
здобувач вищої освіти Львівського державного університету внутрішніх справ

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

ЗРОСТАННЯ ПОПУЛЯРНОСТІ ЧАТ-БОТІВ, ЯК ПЕРЕДУМОВА БІЛЬШ ШИРОКОГО ВИКОРИСТАННЯ ЇХ ПОЛІЦІЄЮ

В наш час великого поширення набуває використання чат-ботів у правоохоронній діяльності з метою протидії різним видам злочинів, таких як розповсюдження наркотиків, запобігання сімейному насильству та торгівлі людьми, тощо. Тому розглянемо поняття чат-ботів, історію їх розвитку та перспективи.

Робот або бот, а також інтернет-бот, www-бот тощо – це спеціальна програма, що виконує автоматично і/або за заданим розкладом які-небудь дії через ті ж інтерфейси, що й звичайний користувач [1]. Чат-бот (англ. Chatbot) – комп'ютерна програма, розроблена на основі нейромереж та технологій машинного навчання, яка здійснює діалог за допомогою голосових або текстових методів. Цей термін ("ChatterBot") вперше вжив творець першого Вербота Julia Майкл Маулдін у 1994 році [2].

У 2010-х роках зросла популярність месенджерів, а разом з ними і чат-ботів. Більшість чат-ботів працює на платформах популярних месенджерів: Facebook Messenger, Telegram, Viber, ВКонтакті, Skype, Slack. На чат-ботах базуються віртуальні помічники на сайтах багатьох організацій. Вони імітують людське спілкування, надають потрібну інформацію [2].

Основу для створення чат-ботів заклав Алан Тьюрінг, який займався теорією машинного інтелекту. У 1950 р. він опублікував статтю з описом тесту, призначеного для визначення можливості машини мислити, як людина. Тест було запропоновано проводити у вигляді задавання машині запитань і видачі надрукованих відповідей, що є подібним до сучасних чат-ботів [3].

На основі цих ідей у всьому світі розпочалися розробки машин, здатних відповісти на запитання тесту Тьюрінга. І у 1966 році Джозеф Вейценбаум у співпраці з комп'ютерною лабораторією Массачусетського технологічного інституту створив першу програму-бота ELIZA, яка була віртуальним співрозмовником з обробкою природної мови. Ця програма виділяла певні слова, на основі яких будувала запитання та вела діалог, що імітував дії лікаря-психотерапевта. Діалог здійснювався шляхом друку через телепринтер.

А у Стенфордському університеті вчений-психіатр Кеннет Колбі в 1972 році створив чат-бота PARRY, який моделював діалог хворого на параноїдну шизофренію. Цей чат-бот був більш досконалий і під час експерименту, в якому брали участь кілька десятків відомих психіатрів, лікарі в половині випадків не змогли відрізнити машину від справжнього хворого. ELIZA та PARRY були з'єднані через Арпанет і між ними був проведений діалог.

Також у ці ж роки були створені інші чат-боти. У 1964 році Деніел Бобров в рамках докторського дослідження створив чат-бот «Студент», який розв'язував прості приклади зі шкільного підручника з математики. У 1970 році Террі Виноград в Массачусетському технологічному інституті створив програму Шрдлу, в якій штучний інтелект виконував завдання, введені під час діалогу з машиною. Машина могла відповідати на запитання, розуміти пояснення і запам'ятовувати терміни. У 1978 році була створена база даних «LIFER/LADDER», яка містила інформацію про військово-морський флот США і могла відповісти на прості запитання, але діалог не могла підтримувати.

Надалі чат-боти розвивалися у напрямку самонавчання, впровадження штучного інтелекту та більш досконалої обробки природньої мови. На початку 80-х років британський вчений Ролло Карпентер почав розробку програми Jabberwacky із завданням пройти тест Тьюрінга. Розробка була завершена у 1997 році. Цей чат-бот був віртуальним співрозмовником, здатним підтримувати діалог на різні теми з розважальною метою. Програма Jabberwacky вигравала премію Лебнера серед програм зі штучним інтелектом у конкурсі на проходження теста Тьюрінга три рази і з 2008 році стала платформою Cleverbot для створення інших ботів.

У 1995 році був створений найдосконаліший віртуальний співрозмовник, який міг вести абсолютно природний діалог з людиною на більш ніж 40 000 різних тем, – програма A.L.I.C.E. Вона кілька разів

отримувала премію Лебнера. Але повноцінно ні ця програма, ні інші, більш сучасні, не змогли пройти цей тест. Програма A.L.I.C.E. використовується як база для сучасних ботів.

Найбільший ріст створення чат-ботів розпочався з середини 2000-х років. Дуже багато чат-ботів було створено для туристичної галузі: у 2008 році – Jenn – чат-бот компанії Alaska Airlines, у 2009 році – чат-бот Alex компанії Continental Airlines, у 2011 році – віртуальний помічник Expedia. У 2011 році Apple представив Siri і це означало, що чат-боти стали голосовими.

Але найбільше цей напрямок змінився з появою месенджерів (WhatsApp з'явився в 2009, Kik і Viber — в 2010, WeChat і Facebook Messenger в 2011, Telegram в 2013). Лідерство відразу захопив Facebook Messenger, відкривши свою базу для сторонніх розробників у 2016 році. Вже за півроку на цій платформі було більше 30 000 чат-ботів, через рік – більше 100 000, а ще через рік – більше 300 000.

Також продовжився розвиток голосових чат-ботів: у 2014 році програма для розумних колонок Amazon Alexa від компанії Amazon; у 2016 році – віртуальний асистент від Google – Google Assistant, який працює на розумній колонці Google Home. Також Amazon представив програму «Alexa Skill» для сторонніх розробників і тепер будь-яка компанія може створити голосовий чат-бот. З деяким відставанням Google створив свою платформу для сторонніх розробників – «Google Actions» [3].

Дослідження показали, що внаслідок розвитку месенджерів телефони використовуються для обміну повідомленнями частіше, ніж для інших цілей. Особливо це стосується представників молодого покоління [4]. Тому зростає створення чат-ботів для вбудовування у месенджери. За результатами дослідження, проведеного Flurry Analytics, затребуваність додатків для обміну повідомленнями в соціальних мережах і мобільних мережах продовжує рости, на відміну від інших сфер [5]. Популярність чат-ботів досягла піку в 2016 році і затребуваність додатків для обміну повідомленнями зросла на 44% в порівнянні з 11% середньорічного зростання всіх додатків, а час проведений користувачами в месенджерах зріс на 394% в порівнянні з 69% середнього зросту. За даними BI Intelligence [6], сукупний обсяг користувачів чотирьох провідних месенджерів WhatsApp, WeChat, Messenger, Viber перевищив обсяг користувачів чотирьох найбільших соціальних мереж Facebook, Instagram, Twitter, Linkedin.

Станом на початок цього року на Amazon Alexa було більше 80 000 ботів, а на Google Assistant – 4 200 сторонніх ботів. А загалом на пристроях з операційною системою Android доступ до Google Assistant мають більше як півмільярда людей. Чат-боти стали частиною сьогоднішнього життя, великі компаніїї замінюють чат-ботами службу підтримки через телефон. Наприклад, за даними Business Insider 80% американських компаній користуватимуться чат-ботами у 2022 році. Чат-боти мають велику перспективу у бізнесі, бо дозволяють економити за рахунок оплати праці працівників колл-центрів [3].

Згідно статичних даних більше 70% громадян України у віці від 18 до 60 років користуються месенджерами. Найпопулярнішими в Україні є два месенджера – Viber (56%) і Facebook (41%), за ними слідують Телеграм (17%), Skype (14%), WhatsApp (12%) та інші. 95% українців віком 18 – 29 років переписуються через призначені для цього додатки. Використовують месенджери: 89% українців віком від 30 до 40 років, 79% українців віком від 40 до 50 років, 57% українців віком 50-60 років і лише 21% українців старше 60 років [7].

Висновок. Враховуючи розвиток інформаційних технологій, зростаюче використання месенджерів та чат-ботів, зростає і їх роль у діалозі населення України з поліцією, та як засобу профілактики правопорушень та протидії їм. Більш широке використання чат-ботів дозволить підвищити ефективність діяльності поліції за рахунок покращеної співпраці з громадянами.

Література:

1. П.Я.Пукач, Х.Р.Шаховська. Алгоритм формування відповіді чат-бота. // Штучний інтелект, 2017, № 2 , с. 161-167. URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/ 133674/17-Pukach.pdf?sequence=1
2. Рижкова С.А.Використання чат-ботів в діяльності Національної поліції як інструмент побудови партнерських відносин з населенням / С.А. Рижкова // Використання сучасних інформаційних технологій в діяльності Національної поліції України: матеріали Всеукр. наук.-практ. семінару (м. Дніпро, 28 листопада 2019 р.). Дніпро: ДДУВС, 2019. С. 59-62. URL: https://er.dduvs.in.ua/handle/123456789/4989.
3. Марина Шумаєва. Як чат-боти змінили IT-індустрію. // URL: https://techno.nv.ua/ukr/technoblogs/kak-chat-boty-izmenili-it-industriyu-50058587.html.

4. Kuang C. Why Chat May Be King Of The New Mobile Landscape / C. Kuang. URL: https://www.fastcompany.com/3064055/why-chat-may-be-king-of-the-new-mobile-landscape.
5. On Their Tenth Anniversary, Mobile Apps Start Eating Their Own. URL: https://flurrymobile.tumblr.com/post/155761509355/on-their-tenth-anniversary-mobile-apps-start.
6. Messaging apps are now bigger than social networks. URL: https://www.businessinsider.com/the-messaging-app-report-2015-11.
7. Рижкова С.А. Використання чат – ботів у профілактиці правопорушень. // Сучасні інформаційні технології в діяльності Національної поліції України: матеріали Всеукр. наук.-практ. семінару (м. Дніпро, 26 листопада 2020 р.). Дніпро: ДДУВС, 2020. С. 82-84. URL: http://er.dduvs.in.ua/handle/123456789/5956.

Глинський Я. М.,
доцент кафедри обчислювальної математики та програмування Національного університету «Львівська політехніка», кандидат фізико-математичних наук, доцент

Пукач П. Я.,
директор Інституту математики та фундаментальних наук Національного університету «Львівська політехніка», доктор технічних наук, професор

Пелех Я. М.,
доцент кафедри обчислювальної математики та програмування Національного університету «Львівська політехніка», кандидат фізико-математичних наук, доцент

ЗМІШАНЕ НАВЧАННЯ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ LMS MOODLE ТА YOUTUBE ЯК ПЕРСПЕКТИВНА ФОРМА ОСВІТНЬОЇ ДІЯЛЬНОСТІ

Сьогодні в умовах пандемії більшість вищих закладів освіти, знаходяться в умовах чистого дистанційного навчання, перманентно переходячи в режим змішаного. За оцінками експертів уже не буде повного повернення освітніх процесів до чистого очного навчання навіть після закінчення пандемії і змішане навчання стане масовим явищем. Тому ми розглядаємо його як перспективну форму освітньої діяльності.

Як форма освітньої діяльності змішане навчання відоме віддавна. Ще до пандемії COVID-19 змішане навчання (скорочено ЗН, інші терміни: гібридне, комбіноване навчання, англ.: blended learning, BL) утвердилося в західних університетах як перспективний напрямок розвитку сучасної освіти. У західноєвропейських, японських та американських університетах нагромадився значний досвід ЗН, який був підсумований у монографії-підручнику групи авторів під редакцією Куртіса Бонка і Чарльза Грехема [1]. ЗН є актуальною темою досліджень у нашій країні. Ці дослідження станом на 2016 рік були узагальнені в [2].

Під ЗН [1, 2] розуміють деяку комбінацію аудиторного та електронного навчання, де одна частина пізнавальної діяльності суб'єктів навчання відбувається аудиторно під безпосереднім керівництвом педагога, а друга полягає в активній самостійній позааудиторній роботі студентів з електронними ресурсами з самоконтролем за часом, місцем, маршрутами та темпом навчання.

Сучасне ЗН передбачає не просто механічне застосування різних видів комп'ютерної техніки і вмінь знаходити потрібні відомості в мережі, але й систему заходів (методів і засобів) щодо оптимальної організації, планування і реалізації навчального процесу, структуризації електронних навчальних курсів і суспільної комунікації всіх суб'єктів навчального процесу.

Курс ЗН формується з трьох традиційних видів навчання: очного (ОН), дистанційного (ДН) та самостійного (СН). Залежно від того, які види навчання лягають в основу чи в послідовність «змішування», розрізняють різні моделі ЗН. В [2] описуються такі чотири основні моделі: 1) гнучка (flex) модель, де гармонійно поєднуються елементи очного, дистанційного і самостійного навчання з переважанням дистанційної компоненти, що можна символічно зобразити так: ДН+СН+ОН; 2) так звані ротаційні моделі з чергуванням діяльностей, серед яких є модель «перевернутий (flipped) клас», де важливу роль надають самостійному навчанню (СН+ДН+ОН); 3) самостійне змішування (self-blended) як зразок навчання «поза кампусом» (позначають абревіатурою SB); 4) збагачений віртуальний клас (enriched model), яку можна трактувати як ОН+ДН+СН, тобто модель, де домінує очне навчання. Існують також інші моделі.

У даній роботі описуємо і узагальнюємо авторський досвід дистанційного і змішаного навчання на прикладі навчання інформатики студентів у НУ «Львівська політехніка». Навчальний процес базувався на використанні електронних навчально-методичних комплексів, створених засобами LMS Moodle, а також авторських електронних навчальних відеоресурсів, розташованих на відеохостингу YouTube.

Модель ЗН, яка розглядається у даній роботі, увібрала в себе елементи всіх чотирьох описаних вище моделей. Схематично її можна зобразити так (у фігурних дужках подано необов'язковий для всіх студентів елемент): аудиторне заняття (ОН+ДН) + позааудиторна робота (СН+ДН+{SB}).

Метою роботи є дослідження і узагальнення досвіду використання засобів навчання, зокрема авторських, та інформаційних технологій, характерних для ДН, зокрема, розроблених на базі LMS Moodle та YouTube, для проведення аудиторних лекційних і лабораторних занять та організації самостійної і

дистанційної роботи зі студентами очної форми підготовки, які на першому курсі вивчають інформатику. Зауважимо, що прив'язка до дисципліни «Інформатика» не є суттєвою і описаний досвід може бути корисним під час вивчення інших дисциплін.

Для навчання студентів були розроблені закриті онлайн курси у віртуальному навчальному середовищі (ВНС) університету, створеному на базі LMS Moodle – відкритої системи управління навчанням, яка підтримує всі типи викладання і пропонує інструменти для вимірювання та визначення прогресу для суб'єктів навчального процесу. Були вирішені питання, що стосуються організації і планування навчального процесу.

На першому занятті студентів ознайомлювали з планом і часовим графіком виконання всіх завдань та їх оцінюванням, зі структурою курсу, задіяними ресурсами, змістом зразка екзаменаційного білета, що корисно для самооцінки знань і вибору стратегії й траєкторії навчання.

Елементи проектування і застосування ЗН опишемо методом аналізу шести складових впровадження ЗН [2] у навчальний процес: 1) лідерство; 2) професійний розвиток; 3) здійснення навчальної діяльності; 4) усвідомлена реорганізація навчального процесу; 5) електронні освітні ресурси; 6) технологічна підтримка.

1. Лідерство. Після декількарічних експериментів зі структурою і наповненням онлайн курсів, принципами організації навчального процесу вдалося забезпечити сильне і послідовне лідерство викладацького колективу і добитися сприйняття ЗН усіма учасниками навчального процесу так, що воно стало частиною філософії і культури навчання. Вдалося зацікавити викладачів, а серед студентів швидко виявляти лідерів у навчальних групах, які підтримували нові підходи до навчання і ставали прикладами для інших студентів.

2. Професійний розвиток. Було забезпечено постійний розвиток професійних якостей і самовдосконалення педагогів через ознайомлення з новими трендами становлення і впровадження ЗН на методичних семінарах, частина з яких відбувалася в дистанційній формі шляхом доставки актуального методичного контенту електронною поштою з наступною дискусією. Частина викладачів самостійно отримали корисну підготовку, пройшовши навчання на освітньому порталі Prometheus.org і отримавши відповідні сертифікати. Відразу зазначимо, що недолік системи освіти криється в тому, що навчання на масових відкритих онлайн курсах і отримання сертифікатів не завжди офіційно визнається. Не у всіх університетах для студентів такий сертифікат зараховується навчальним закладом як еквівалент кредитів відповідної дисципліни, а для викладачів сертифікат не зараховується як еквівалент проходження курсів підвищення кваліфікації. Прикладами відкритих онлайн курсів, що знайомлять з новими формами навчання і які можна рекомендувати для викладачів інформатики як засіб індивідуального підвищення кваліфікації, є перекладений українською мовою онлайн курс з програмування «Computer Science 50 (CS50)» Гарвардського університету (США), а також вітчизняний курс «Word і Excel: інструменти та лайфхаки», з якими варто ознайомитися на освітньому порталі Prometheus.org і які варто рекомендувати студентам (перший – студентам комп'ютерних спеціальностей, другий – економічних).

3. Здійснення навчальної діяльності. Оскільки навчання базувалось на використанні закритих онлайн курсів віртуального навчального середовища університету, для здійснення навчальної діяльності були застосовані головні можливості та інструменти LMS Moodle. Використовувались онлайн системи доставки контенту. Надавалась перевага доставці текстового контенту у форматі pdf-файлів лекцій та методичних вказівок. Створювались відеоуроки зі зразками виконання лабораторних робіт, які публікувалися на відеохостингу YouTube. Застосовувались онлайн спілкування, онлайн оцінювання з використанням електронного журналу, деякі елементи геймифікації навчання. Здійснювалось відкрите інформування щодо успішності учасників навчання і мотивування до навчання шляхом проведення конкурсів робіт і написання викладачами заохочувальних чи конструктивних відгуків (рецензій на роботи), які студенти могли демонструвати один одному і, що важливо, батькам. Були ситуації коли зацікавлені студенти звертались до викладачів з проханнями написати онлайн відгуки про їхні роботи оскільки викладачі через зайнятість писали їх тільки у разі потреби.

4. Усвідомлена реорганізація навчального процесу. Змінилася роль викладача на курсі. Відбувся перехід від традиційного викладання до менторства (наставництва), що близьке до поняття і ролі тьютора в дистанційному навчанні. Лекція перестала існувати у своєму класичному форматі. Не було сенсу диктувати матеріал і його конспектувати, оскільки всі матеріали доступні студентам онлайн чи

офлайн у будь який час і в будь якому місці. Лектор давав характеристику онлайн матеріалам, керував організацією навчання і розглядав окремі важливі питання. Відбулося сприйняття і розуміння напрямків реорганізації навчального процесу. З'явилася впевненість у позитивних змінах як щодо перебігу самого процесу навчання, так і у його результативності.

5. Електронні освітні ресурси. Використання ВНС було цілком достатнім для організації навчального процесу. Однак студенти першого курсу отримують доступ до закритих ресурсів ВНС з двотижневою затримкою через об'єктивні причини, пов'язані з обробкою персональних даних (внесенням даних у систему і формуванням логінів). Тому стартові матеріали дисципліни були продубльовані у відкритих гугл-групах (наприклад, у гугл-групі fk-inform), що забезпечувало безперебійність навчального процесу, коли ВНС було недоступне. Електронні освітні ресурси використовувались двох видів: 100% авторські для основного курсу і контент сторонніх розробників для поглибленого вивчення (SB). Електронні освітні відеоресурси (ЕОВ) були доступні з авторського YouTube-каналу [3]. Власне активне використання студентами відеоконтенту забезпечило як покращення успішності, так і мотивацію студентів до навчання.

6. Технологічна підтримка змішаного навчання. Адміністрація університету забезпечувала функціонування телекомунікаційної мережі, програмного забезпечення та апаратних засобів, однак виникали деякі технічні труднощі. Потужностей серверів, які обслуговують ВНС великого університету, в умовах змішаного і дистанційного навчання деколи ставало критично недостатньо. Наприкінці семестру період очікування на реакцію сервера став настільки великим, що це унеможливлювало своєчасне написання викладачами онлайн відгуків і ведення електронного журналу, що у свою чергу викликало необхідність працювати викладачам з ВНС додатково у позаробочий час у домашніх умовах. У цьому проявляється риса ЗН, яка називається «руйнівною», оскільки ЗН може створювати додаткові, часто несподівані, проблеми як для адміністрації навчального закладу, так і для його учасників.

Кожна тема курсу підтримується відеоресурсами тривалістю 10-15 хвилин, де ілюструються теоретичні викладки або розглядаються конкретні задачі і демонструються шляхи їх розв'язування. Більшість таких відеоресурсів є авторськими. Усі відеоресурси доступні онлайн чи офлайн (після завантаження з YouTube-каналу) студентам очної форми навчання (і не тільки їм) для одноразового чи багаторазового перегляду причому у любий час, любими сучасними засобами відтворення відео, з любого розташування, де є відповідний зв'язок.

Важливим аспектом ЗН є індивідуалізація навчання. Студентам було запропоновано чотири траєкторії навчання (мінімальна, середня, висока і поглиблена), які студент міг обирати залежно від рівня попередньої підготовки, зацікавлення, особистих потреб і вимог навчальної програми. Побудова цих траєкторій відбувалась шляхом структуризація контенту, а реалізація здійснювалась головно на лабораторних заняттях в рамках моделі навчання face-to-face (F2F). Перебіг лабораторних занять також змінився. Тут застосовувалися різні прийоми навчання, які чергувалися (подібно як в ротаційних моделях навчання) і забезпечували вироблення рефлексій: спочатку студенти вчилися відтворити за відео з YouTube-каналів застосування тої чи іншої технології за принципом «Роби, як ми»; пізніше вони вчилися вносити зміни у процесі виконання роботи за принципом «Роби краще, ніж ми»; згодом намагалися самостійно знаходити в мережі матеріали для розв'язування задач. Відпрацювання таких навиків корисне для застосування у подальшій фаховій підготовці і в майбутній діяльності, де, можливо, прийдеться швидко освоювати зовсім нові інформаційні технології. Витримувались схеми використання досить складних комплексних наскрізних завдань з елементами фахових предметних областей для лабораторних робіт з метою охопити всі траєкторії навчання так, щоб у разі труднощів студент міг перейти на нижчу траєкторію, щоб цілком не провалити курс навчання.

Наші спостереження, а також у деякій мірі відгуки студентів вказують не те, що рівень рефлексії у багатьох студентів у результаті навчального процесу виробився достатньо високим і всі рівні таксономії Блума за результатами рефлексії рівномірно розподілені між учасниками навчання.

Розглянута реалізація змішаного навчального процесу відповідає підходу Ган'є, який описаний в [4] як дев'ять кроків створення дистанційних курсів і проведення дистанційного навчання, а саме: привернути увагу студента, інформувати студентів про мету, стимулювати використання попередніх знань, правильно подати матеріал, надати керівництво для навчання, викликати уявлення, надавати відгук, оцінювати ефективність, тримати студента в курсі.

Детальніше наш досвід і рекомендації щодо організації змішаного і дистанційного навчання описані в [5].

Література:

1. Bonk C. J., Handbook of blended learning: Global perspectives, local designs. C. J. Bonk, C. R. Graham. San Francisco, CA: Pfeiffer, 2005. pp. 3–21. URL: http://goo.gl/0LwXKV.
2. Кухаренко В. М. та ін. Теорія та практика змішаного навчання. Харків, Україна: "Міськдрук", НТУ "ХПІ", 2016.
3. YouTube-канал «Ярослав Глинський». URL: https://www.YouTube.com/results?search_query=ярославглинський.
4. Кухаренко В. М. Тьютор дистанційного та змішаного навчання: посібник. Київ, Україна: Міленіум, 2019.
5. Глинський Я. М., Пукач П. Я. Досвід змішаного навчання інформатики студентів економічних спеціальностей з використанням засобів LMS Moodle та YouTube: Інформаційні технології і засоби навчання, т. 83, №3, с. 113–119, 2021.

Головко Д. П.,
здобувач вищої освіти Дніпропетровського державного університету внутрішніх справ

Рижков Е. В.,
завідувач кафедри економіки та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ, кандидат юридичних наук, професор

ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ

Актуальність використання інформаційних технологій зростає у зв'язку з інтенсивним впровадженням у діяльність правоохоронних органів засобів комп'ютерної техніки. Цей процес впливає на організацію розслідування кримінальних правопорушень, методичне забезпечення працівників Національної поліції України (далі – НП України), а здійснення автоматизованого пошуку відомостей щодо будь-яких об'єктів (осіб, предметів, подій тощо) сприяє науковій організації праці, оптимізує збирання, зберігання, систематизацію та аналіз інформації оперативно-розшукового, доказового та іншого характеру.

Для вирішення розшукових задач нині накопичений чималий досвід застосування новітніх технологій у процесі попередження, виявлення та розслідування злочинів, розшуку підозрюваного та обвинуваченого, провадження окремих слідчих (розшукових) дій, здійснення судових експертиз [1].

Інформаційні технології – це сукупність методів, інформаційних процесів із використанням засобів обчислювальної техніки, що забезпечують високу швидкість оброблення даних, ефективнийий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця розташування [2].

Для вирішення оперативно-розшукових завдань нині накопичений чималий досвіт застосування новітніх технологій у процесі попередження, виявлення та розслідування злочинів, розшуку підозрюваного та обвинуваченого, провадження окремих слідчих (розшукових) дій, зокрема негласних слідчих (розшукових) дій.

Оперативність і ефективність застосування положень Кримінального процесуального кодексу України (далі – КПК України) як і здійснення самого досудового розслідування неможливі без застосування сучасних інформаційних технологій та автоматизованих баз даних.

Технічне забезпечення оперативних підрозділів НП України є актуальним з огляду на новації, що містяться в положеннях КПК України, які закріплюють сучасні інструменти для боротьби зі злочинністю та застосування яких повинно чітко відповідати вимогам чинного законодавства.

Очевидно, що однією з важливих умов підвищення рівня протидії злочинності є широке використання сучасних досягнень науково-технічного прогресу, які останніми роками зробили прорив у сфері інформаційних технологій [3].

Одним з основних завдань функціонування системи інформаційного забезпечення діяльності стала інформатизація підрозділів, що здійснюють оперативно-розшукову діяльність. В України вже накопичено чималий досвід використання різноманітних інформаційних та інформаційно-телекомунікаційних систем оперативно-розшукового та інформаційно-довідкового призначення.

Наказом НП України від 30 грудня 2015 р. № 228 створено Департамент інформаційної підтримки та координації поліції «102» НП України (згодом реорганізувався у Департамент інформаційно-аналітичної підтримки), який організовує та здійснює передбачені законодавством України заходи, спрямовані на інформаційно-аналітичне та інформаційно-пошукове забезпечення правоохоронної діяльності й захист персональних даних під час їх обробки у структурних підрозділах апарату НП України. ДІПКП визначає основні напрями діяльності поліції у сфері інформатизації, здійснює інформаційно-пошукову та інформаційно-аналітичну роботу, бере участь у розроблені проектів нормативно-правових актів МВС із питань, що належать до компетенції поліції та стосуються інформаційно-аналітичного забезпечення, а також оброблення персональних даних в органах і підрозділах поліції.

Завданнями використання інформаційно-комунікаційних технологій у підрозділах НП України є:

- забезпечення можливості оперативного отримання інформації у повному, систематизованому та зручному для користування вигляді співробітниками та підрозділами НП України для розкриття, розслідування, попередження кримінальних правопорушень і розшуку злочинців;

- збирання, оброблення та узагальнення оперативної, оперативно-довідкової, аналітичної, статистичної та контрольної інформації для оцінки ситуації та прийняття обґрунтованих оптимальних рішень на всіх рівнях діяльності підрозділів НП України;
- забезпечення динамічної та ефективної інформаційної взаємодії всіх галузевих служб і підрозділів НП України, інших правоохоронних органів, державних установ, різних груп громадськості, мас-медіа;
- забезпечення захисту інформації [4].

За допомогою комп'ютерної техніки не тільки раціоналізуються інформаційні процеси, але й упроваджуються комп'ютеризовані системи підтримки прийняття слідчими, експертами, оперативними співробітниками, суддями відповідних рішень. За останні роки розроблено кілька десятків систем, які, по суті, моделюють діяльність слідчих, які допомагають розслідувати найбільш складні злочини, формулюючи за результатами вивчення кримінальних правопорушень конкретні рекомендації [5].

Як свідчить практика, щоб комп'ютеризована інформаційна система була працездатною, необхідно дотримуватися таких правил:

1) вся інформація, що вводиться, повинна записуватися з використанням спеціальної термінології мовою, що виключає різне тлумачення;
2) перероблення інформації має здійснюватися точно відповідно до лгоритму, з певною послідовністю операцій, що дає можливість вирішити будь-яку конкретну задачу з деякого класу однотипних задач, причому вихідні дані можуть у певних межах змінюватися.

Отже, впровадження та використання нових інформаційно-комунікаційних технологій є головною умовою покращення роботи щодо встановлення підозрюваного або його розшуку, а також діяльності підрозділів НП України та функціонування правоохоронної системи загалом. При цьому є проблеми фінансового забезпечення, низький рівень володіння співробітниками відповідними інформаційними ресурсами та навичками роботи з новою технікою або новими системами [6]. У нинішніх умовах швидкого технічного процесу кожен працівник НП України повинен бути прогресивним користувачем інформаційно-комунікаційних технологій. Крім того, оперативним працівникам необхідно проходити курси підвищення кваліфікації з метою отримання нових знань, умінь і навичок під час застосування в повсякденній роботи інформаційних технологій.

Література:

1. Рогатюк І.В. Використання інформаційних технологій у досудовому розслідуванні: сучасний стан і перспективи розвитку / І.В. Рогатюк // Науковий вісник Національної академії внутрішніх справ. – 2013. – № 3. – С. 312–320.
2. Інформаційні технології / Вікіпедія [Електронний ресурс]. – Режим доступу : https://uk.wikipedia.org/wiki.
3. Інформатика : [навч. посібник] / [А.Ю. Гаєвський]. – 2-ге вид., доповн. – К. : «Видавництво А.С.К.», 2007. – 512 с.
4. Кормич Б.А. Організаційно-правові засади політики інформаційної безпеки України : [монографія] / Б.А. Кормич. – О. : Юридична література. – 2003. – 271 с.
5. Іщенко П.П. Інформаційне забезпечення слідчої діяльності : [науково-практичний посібник] / П.П. Іщенко ; під ред. Є.П. Іщенко. – М.: Юрлитинформ, 2011. – 168 с.
6. Рижков Е.В. Оптимізація деяких підсистем ІІПС ОВС та ІТС НПУ та інші питання в діяльності працівників ІАП ГУНП / О.О. Дворецький, Р.І. Калюга, О.М. Паштета, Е.В. Рижков // Використання сучасних інформаційних технологій в діяльності Національної поліції України : матеріали всеукраїнського наук.-практ. семінару, м. Дніпро, 23 листопада 2018 року – Дніпро: ДДУВС, 2017. – С. 18 – 23; Рижков Е.В. Деякі проблемні питання в роботі секторів інформаційної підтримки територіальних органах та підрозділах Національної поліції / Е.В. Рижков // Застосування інформаційних технологій у діяльності НПУ: науково-практичний семінар (21 грудня 2018 року, ХНУВС, м. Харків). – Харків: ХНУВС, 2018. – С. 57-58

Грищук А. Б.,
доцент кафедри адміністративно-правових дисциплін Інституту права Львівського державного університету внутрішніх справ, кандидат юридичних наук

ІНФОРМАЦІЙНО-ДИСТАНЦІЙНІ ТЕХНОЛОГІЇ НАВЧАННЯ ДЕРЖАВНИХ СЛУЖБОВЦІВ

На початку XXI ст. дистанційні технології у системі вищої освіти розробляються у більшості країн світу. Слід зауважити, що традиційні університети зарубіжних країн надають перевагу змішаному навчанню: поруч із дистанційними технологіями майже половину часу складає традиційний навчальний процес.

Ефективність державного управління значною мірою залежить від кадрів, фахово й світоглядно підготовлених до активної професійно-компетентної інноваційно-творчої роботи в нових умовах: демократії, економічної та політичної конкуренції, глобалізації. Тому необхідною умовою ефективного державного управління є його професіоналізація. Важливим інститутом професіоналізації державного управління є система підвищення кваліфікації державних службовців та посадових осіб місцевого самоврядування, інтелектуального й інституційного зміцнення фахової спроможності у галузі державного управління [1].

Нетрадиційні форми та методи освіти, які забезпечують оперативність отримання нових знань при мінімальних затратах часових та фінансових ресурсів, все активніше завойовують світ. Серед них і дистанційна освіта. Так, у США за програмами дистанційної освіти сьогодні навчається близько 1 млн студентів; 32% американців віддають перевагу Інтернету замість стаціонарного та заочного навчання, а 39% взагалі вважають, що Інтернет зробить аудиторії непотрібними [2].

На думку А. Бойко., А.Чечель «…дистанційне навчання (ДН) – тип навчання, заснований на освітній взаємодії віддалених один від одного педагогів та учнів, що реалізується за допомогою телекомунікаційних технологій і ресурсів мережі Інтернет. Для дистанційного навчання характерні всі притаманні навчальному процесу компоненти системи навчання: зміст, цілі, зміст, організаційні форми, засоби навчання, система контролю та оцінки результатів».

В основу дистанційної освіти покладена певна модель передачі знань, де джерелами знань є інформаційні ресурси мережі, як спеціальним чином підготовлені, так і вже існуючі в базовій телекомунікаційному середовищі, наприклад: бази даних, інформаційні системи тощо. Телекомунікації також забезпечують доставку учасникам процесу досліджуваного матеріалу або їх роботу з навчальним матеріалом, розміщеним на сервері, інтерактивна взаємодія викладача й учня в процесі навчання надають учням можливість самостійної роботи з інформаційними джерелами мережі, можливість працювати в групі, а також оцінку знань і умінь, отриманих в ході навчання. Дистанційна освіта забезпечує ефективний оперативний зворотний зв'язок, закладений в самому навчальному матеріалі, та безпосередній систематичний зворотний зв'язок з викладачем по мережі, а також можливість спілкування в мережі з колегами [3, с. 4].

Процес упровадження курсів електронного навчання із застосуванням дистанційних інформаційних технологій в освітній процес державних службовців у країнах ЄС, можна констатувати прагнення до встановлення єдиної комплексної процедури державної акредитації. Зокрема здійснюється спеціальне ліцензування установ, які повністю застосовують дистанційні освітні технології (наприклад, у Великій Британії для державних і муніципальних службовців понад 70% навчального часу в разі навчання за програмами різного рівня відводиться на навчання з використанням дистанційних освітніх технологій.

Адаптація українського законодавства до стандартів ЄС, завершення політичних й економічних реформ, вироблення скоординованої державної політики тощо вимагають значного фінансування, якого недостатньо у розпорядженні уряду України. Європейська Комісія підтримує країни-партнери Європейської політики сусідства та надає технічну допомогу через засоби, що підтвердили свою ефективність у країнах із перехідною економікою (нові держави-члени ЄС): через цільову експертну допомогу (Технічна допомога та інформаційний обмін TAIEX), довготермінові твінінгові проекти, секторальну бюджетну підтримку, яка дозволяє дофінансувати з бюджету ЄС національні програми реформування певних секторів економіки. В Україні, на відміну від країн Центральної Європи, де засоби міжнародної технічної допомоги довели свою ефективність, вищезазначені інструменти

використовуються неефективно, не беруться до уваги їх значущість та корисність, практичні рекомендації експертів реалізовуються частково [4].

В Україні, як і в багатьох інших країнах Європейського співтовариства, посилюється увага довкола проблеми інформатизації професійної підготовки державних службовців як однієї з найважливіших стратегічних проблем розвитку державного управління. Під інформатизацією відтак розуміється цілеспрямована діяльність з розробки та впровадження інформаційно-комунікаційних технологій, зокрема у: – навчальний процес для підготовки державних службовців до діяльності в умовах сучасного інформаційного суспільства, підвищення якості загальноосвітньої та професійної підготовки фахівців на основі широкого використання інформаційно-комунікаційних технологій; – управління системою освіти для підвищення ефективності й якості процесами управління; – методичну та науково-педагогічну діяльність для підвищення якості роботи педагогів, розробки та впровадження нових освітніх технологій на основі використання інформаційно-комунікаційних технологій [5].

З вище наведеного, потрібно зазначити, що дистанційні освітні технології – це організаційно-правовий механізм з можливістю отримання освіти більш «швидким» та доступним способом використовуючи при цьому наприклад комп'ютер чи телефон підключений до інтернету або програми чи курси, що можна завантажити на телефон чи будь-який інший гаджет для того щоб можна було б у зручний час навчатись чи поновлювати свої знання державним службовцям.

Проте слід зауважити, що створення єдиної системи електронного навчання не повинно заважати самостійності освітніх установ і розвитку різних форм електронного навчання, що забезпечують дотримання вимог державного освітнього стандарту.

З огляду на важливість інформаційних технологій у сучасному світі, а також їх використання для інтеграції держави в глобальне інформаційне суспільство, є необхідність системного правового регулювання, що забезпечує певні гарантії стабільного розвитку та захисту інтересів учасників єдиного освітнього простору в Україні.

Література:

1. Про затвердження Положення про систему професійного навчання державних службовців, голів місцевих державних адміністрацій, їх перших заступників та заступників, посадових осіб місцевого самоврядування та депутатів місцевих рад: Постанова Кабінету Міністрів України від 06.02.2019 р. № 106. URL: https://zakon.rada.gov.ua/laws/show/106-2019-%D0%BF#Text
2. Антропова Т. Дистанционное образование: взвесим «за» и «против» URL: http://www.job-today.ru/nnovgorod/issue/s34_05_8.htm.
3. Бойко А., Чечель А. Дистанційне навчання в системі підвищення кваліфікації державних службовців. А. Бойко, А. Чечель. Журнал Державне управління № 4 (136), спецвипуск, травень 2015 р. С. 3-7.
4. Горецька Т. О. Використання інструментів міжнародної технічної допомоги Європейського Союзу як передумова ефективної модернізації державного управління в Україні. Т. О. Горецька. Ефективність державного управління. 2012. Вип. 32. С. 346-353. URL: http://nbuv.gov.ua/UJRN/efdu_2012_32_45
5. Европейское обучение URL: http://www. smart-edu.com/learning-in-europe-2020.html

Дуфенюк О. М.,
доцент кафедри кримінального процесу та криміналістики Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент

ІННОВАЦІЇ У РОЗСЛІДУВАННІ ДТП НА ПРИКЛАДІ ЗАСТОСУВАННЯ 3D ТЕХНОЛОГІЙ

Криміналістична наука постійно дбає про розвиток технологій, здатних оптимізувати діяльність працівників органів досудового розслідування, а одним із таких прикладів є впровадження технологій 3D сканування. Досвід застосування цієї інновації у діяльності польських, американських та інших поліцейських служб дає підстави для оптимізму та очікування активного застосування і українськими фахівцями, зокрема при розслідуванні ДТП.

Технологія 3D сканування має численні переваги у порівнянні із традиційним способом вербальної фіксації інформації у процесуальних документах, особливо коли йдеться про складну слідчу ситуацію, зумовлену насиченою слідовою картиною. Основними перевагами застосування такого підходу обробки інформації є: універсальність, портативність, швидкість, легкість у використанні, оперативність, безпечність, поліфункціональність та економічність, про що докладно йшлося у попередніх публікаціях авторки [1; 2].

У багатьох випадках від якості проведення огляду місця події ДТП залежить успішне розслідування цієї категорії кримінальних правопорушень. Важливо якісно та ефективно зафіксувати обставини події, сліди правопорушників, вилучити матеріальні предмети та речовини для подальших експертних досліджень, викрити осіб, які намагаються уникнути кримінальної відповідальності. Недоліками традиційного способу фіксації слідової інформації на місці ДТП відносять тривалі часові витрати на збирання потрібних даних, можливість помилки (людський чинник) під час вимірювання та фіксації даних у складних умовах дослідження, а також тривалий час оформлення схеми ДТП, якість якої є доволі низькою [3, с. 166]. Труднощі зумовлює те, що реально ми маємо можливість провести докладний огляд місця ДТП тільки один раз. Звісно, криміналістична тактика передбачає проведення повторних та додаткових оглядів, однак обстановка події на момент таких «вторинних» спостережень, як правило, зазнає суттєвих змін, особливо тоді, коли йдеться про відкриту смугу руху з насиченим транспортним потоком. Натомість застосування ***3D технології при огляді місця події*** дозволяє:

- збільшити інформативність зібраних даних про ДТП, їх точність;
- зафіксувати найдрібніші сліди, деталі деформацій транспортних засобів, пошкоджень дорожньої інфраструктури, у тому числі в умовах темної пори доби, що не впливає на результати;
- візуалізувати дані, створити віртуальну модель місця події з високою ілюстративною якістю, що дозволяє «повернутися на місце події» не виходячи з кабінету слідчого, експерта, прокурора чи залу судових засідань;
- оптимізувати вимірювання параметрів, необхідних для визначення механізму та причинно-наслідкових зв'язків події;
- виготовити за наявності спеціального програмного забезпечення 2 D схеми до протоколів процесуальних дій;
- скоротити час процесуальних дій, що не потребує тривалого перекриття смуг руху;
- посилити безпеку осіб, залучених до процесуальних дій при ДТП.

Останній пункт потребує додаткового роз'яснення. Часто за необхідності діяти в умовах напруженого транспортного трафіку важливо не тільки ретельно дослідити місце події, але й зробити це швидко та безпечно, адже на відміну від багатьох інших місць вчинення кримінальних правопорушень, виконуючи передбачені першочергові алгоритми дій в рамках реагування на повідомлення про ДТП, працівники поліції часто змушені перебувати у зоні підвищеного ризику. Неодноразово у практиці траплялися випадки, коли працівники поліції при виконанні своїх службових обов'язків на місці ДТП самі ставали потерпілими через неуважність інших учасників дорожнього руху, які не помітили сигнальних знаків, не впоралися з керуванням транспортних засобів тощо [4]. Експериментальні дослідження показали, що середній час сканування ДТП займає близько 9−15 хв. [3, с. 168]. Саме тому закордонні колеги переконують, що ці технології сприяють забезпеченню безпеки фахівців спеціальних служб, адже зменшується тривалість документування, що запобігає появі вторинних ДТП, що приводили до ушкоджень та навіть смертей поліцейських при виконанні обов'язків [5, с. 8; 6; 7].

Втім застосування 3D технологій не обмежується тільки оглядами. Часто такі засоби використовуються для ***реконструкції обставин події, слідчих експериментів, судових експертиз***. До прикладу, з метою моделювання та симуляції руху транспортних засобів у процесі розвитку ДТП спеціальні програми дозволяють отримати 3D-анімацію події [8, с. 498] або ж навіть виготовити 3D-фізичні моделі для потреб наочної презентації в суді [5, с. 3].

Технологія 3D сканування дозволяє проводити дослідження трупів осіб, які загинули на місці ДТП. Останні розробки в рамках проекту Віртопсія (*Virtopsy)* швейцарських науковців із Бернського університету переконливо доводять достатню ефективність так званої «віртуальної посмертної експертизи» або «віртуального розтину», що передбачає поєднання технологій 3D сканування та рентгенологічну діагностику. Дані отримують під час лазерного сканування поверхні трупа, комп'ютерної томографії та магнітно-резонансної томографії з використанням технології 3D-візуалізації та спектроскопії. Результатом цього дослідження є створення 3D-реконструкцій, які передають зображення внутрішніх частин людського тіла та окремих органів. Ключовою перевагою цього методу є те, що такі дослідження не знищують жодних доказів, що, за звичай, відбувається під час традиційного розтину. Отримане детальне зображення внутрішніх частин тіла, його органів та скелета, м'язів та м'яких тканин дозволяє експерту сформувати повне уявлення про ушкодження, які виникли у результаті ДТП, механізм кримінального правопорушення [9, с. 99; 10; 11].

Сьогодні технології 3D сканування використовують поліцейські служби США, Швейцарії, Німеччини, Нідерландів, Люксембургу, Італії, Іспанії, Данії, активно напрацьовується досвід у Польщі. За межами європейського континенту така технологія використовується у Мексиці, Бразилії, Чилі [12, с. 7−8]. Впровадження таких інновацій у кримінальному провадженні має перспективи і в Україні. Ще в 2011 р. проводились випробування 3D-сканера у криміналістичній діяльності фахівців у Харківській області. Відповідно до досліджень С. Данця вже апробовано можливості лазерного сканування під час огляду місця ДТП за допомогою сканера «LeicaScanStation 2» (Швейцарія). Таку ж апробацію технології сканування місця ДТП за допомогою сканера компанії FARO® (США) було проведено на базі Державного науково-дослідного експертно-криміналістичного центру МВС України [3, с. 167; 13, с. 191]

Зважаючи на стрімкий розвиток цифрової епохи та візуалізації даних, можна впевнено прогнозувати світову тенденцію розширення сфери застосування таких технологій у діяльності правоохоронних органів у найближчій перспективі. Разом з тим, освоєння інновацій завжди вимагає додаткового фінансування, підготовки спеціалістів відповідного напрямку, а в умовах пандемії, соціально-економічних проблем, військових загроз та багатьох інших викликів навряд чи варто сподіватися на швидкий результат впровадження технології 3D сканування у кримінальному провадженні в Україні.

Література:

1. Blahuta R. I., Blikhar V. S., Dufeniuk O. M. Transfer of 3D Scanning Technologies Into the Field of Criminal Proceedings. Sci. innov. 2020. 16 (3). P. 84–91.
2. Дуфенюк О. М., Марко О. І. Інноваційні технології 3D сканування у криміналістичній діяльності. Порівняльно-аналітичне право. 2018. № 1. С. 313–315.
3. Данець С.В. Застосування новітніх технологій лазерного сканування під час огляду місця дорожньо-транспортної пригоди. Криміналістичний вісник. 2014. № 2 (22). С. 166 –171.
4. У Києві під час оформлення ДТП збили поліцейську. Слово і діло. 14 червня 2020. URL: https://www.slovoidilo.ua/2020/06/14/novyna/suspilstvo/kyyevi-oformlennya-dtp-zbyly-policejsku (дата звернення: 06.05.2021).
5. Pagounis V., Tsakiri M., Palaskas S. and others. 3D Laser Scanning for Road Safety and Traffic Accident Reconstruction. Proceedings of the XXIIIth international FIG congress. 2006. Vol. 8. P. 1−15.
6. How 3D laser scanners are changing crime scene investigations. URL: https://www.policeone.com/police-products/accident-reconstruction/articles/8720378-How-3D-laser-scanners-are-changing-crime-scene-investigations/ (дата звернення: 07.05.2021).
7. CSI's use 3D Laser Technology to Save Time, Record Evidence, and Protect Officers. URL: https://www.crimesceneinvestigatoredu.org/2015/09/csis-use-3d-laser-technology-to-save-time-record-evidence-and-protect-officers/ (дата звернення: 07.05.2021).

8. Сараєв О. В., Данець С. В. Використання прикладних комп'ютерних програм при дослідженні дорожньо-транспортної пригоди. Наукові нотатки. 2014. Вип. 45. С. 492−499.
9. Gąsiorowski J. Nowoczesne technologie w kryminalistyce. Kultura Bezpieczeństwa. Nauka-Praktyka-Refleksje. 2016. Nr 21. S. 73−114.
10. Buck U., Naether S., Braun M. and others. Application of 3D documentation and geometric reconstruction methods in traffic accident analysis: with high resolution surface scanning, radiological MSCT/MRI scanning and real data based animation. Forensic science international. 2007. Vol. 170 (1). P. 20−28.
11. Thali, M., Buck, U., Naether, S. Virtopsy: Expert opinion based on 3d surface and radiological scanning and documentation in forensic medicine. 2008. URL: https://www.semanticscholar.org/paper/Virtopsy%3A-Expert-opinion-based-on-3d-surface-and-in-Thali-Buck/a9ed012c542be8357b7f65b0276b0a09b59ba108 (дата звернення: 07.05.2021).
12. Wieczorek T., Mączka K., Szymczak M. Analiza możliwości wykorzystania skanów 3D z miejsca zdarzenia jako materiału dowodowego w postępowaniu sądowym w warunkach prawnych obowiązujących w Polsce. Przegląd Policyjny. 2018. Nr 2. S. 5−19.
13. Данець С. В. Застосування автоматизованих засобів дослідження обставин ДТП. Вісник Харківського національного автомобільно-дорожнього університету. 2013. Вип. 61−62. С. 190−194.

Д'яков А. В.,
доцент кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів Львівського державного університету внутрішніх справ, кандидат технічних наук

ПРОБЛЕМИ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ТА ШЛЯХИ ЇХ ВИРІШЕННЯ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ

Проблема захисту інформації та інформаційної безпеки є однією з найважливіших для розвитку сучасного суспільства. В даний час вирішення цієї проблеми в галузі створення та експлуатації інформаційних систем різного призначення пов'язане з розробкою різноманітних вимог до створення безпеки програмно-апаратних засобів від несанкціонованого доступу. На сьогодні одним із найперспективніших напрямків у системах контролю доступу стає використання біометричних даних людини.

Біометричні методи ідентифікації сьогодні мають безперечні переваги перед іншими методами завдяки своєї зручності, надійності та достовірності. Використання фізіологічних параметрів суб'єкта таких, як код ДНК, відбитки пальців, райдужну оболонку ока, зображення обличчя, тембр голосу та інші біометричні ознаки дозволяють швидко та відносно просто ідентифікувати (або верифікувати) особу, а розвиток комп'ютерно-інформаційних та телекомунікаційних технологій дозволяють це здійснити в режимі реального часу.

Біометрична ідентифікація – це особливий рівень захисту, оскільки біометричні дані людини складно підробити. Біометричні дані незмінні та унікальні для кожної людини, що є безумовною перевагою.

Таким чином, основна перевага ідентифікації за біометричними параметрами очевидна: їх неможливо забути, втратити, передати іншій людині або вкрасти, відтворити у повному обсязі

Класифікація біометричних технологій передбачає їх поділ на дві великі групи:

- використання статичних біометричних параметрів, таких як, відбитки пальців, геометрію руки, зображення особи, райдужну оболонку ока і т.п.;
- використання динамічних параметрів – динаміку відтворення підпису або рукописного ключового слова, тембр голосу і т.п.

Біометричні методи обумовлені відмінностями, що відрізняють їх від звичних методів, а саме:

- публічність біометричних даних. Існує можливість знайти обличчя, відеозапис, аудізапис голосу майже будь кого та використати їх для ідентифікації;
- фактично неможливо замінити свої біометричні дані так же легко, як змінити пароль, номер телефону та інш;
- біометрична ідентифікація підтверджує особистість з визначеною точністю та виключає можливість ідентифікації на 100%.

Окреслити проблеми, що пов'язані із біометричною ідентифікацією особи можна наступними чинниками: фальсифікація, витік та крадіжки, низька якість зібраних даних, а також багатократний збір даних однієї особи багатьма користувачами біометричних даних.

Одним з напрямків щодо вирішення вищезазначених проблем є застосування мультибіометричних рішень. У мультибіометричних системах розпізнавання здійснюється не за одним, а декількома біометричними ідентифікаторами. Крім мультибіометричних технологій, в один клас з ними можна поєднати мультимодальні та багатофакторні рішення.

У мультимодальних системах ідентифікатори того самого типу (наприклад, відбитки пальців) обробляються з допомогою різних алгоритмів та використовуються різні біометричні ідентифікатори (наприклад, голос та обличчя, обличчя та відбитки пальців). Головна мета – підвищення надійності ідентифікації.

Можна виділити наступні переваги мультимодальної біометрії:

- більша різноманітність ідентифікаторів з можливістю їх альтернативного застосування (наприклад, розпізнавання за відбитками пальців у випадку, якщо особа або голос користувача суттєво змінено);

- за рахунок скорочення кількості помилок відмови реєстрації з’являється можливість охопити значно більшу кількість респондентів;
- підвищення надійності та якості розпізнавання, що приводить до зниження рівня помилок першого та другого роду (коли дозволяється доступ незареєстрованому користувачеві або відмова у доступі отримує зареєстрований користувач);
- зберігається точність при ідентифікації у випадку роботи з базами великого розміру – одні біометричні ознаки можуть компенсувати недоліки, що притаманні іншим ознакам;
- скорочуються помилки хибної відмови в результаті зменшення чутливості до шумів, а також розширення діапазону умов навколишнього середовища, при яких можливо розпізнавання за рахунок використання декількох модальностей;
- суттєво підвищується стійкість до атак порушників та фальсифікаціям – досить складно підробити декілько біометричних ідентифікатора.
- прискорення процесу ідентифікації.

У багатофакторних системах поряд з біометричними використовуються також інші ідентифікатори (PIN-код, пароль, смарт-карта та інше). У цьому випадку для підтвердження своєї особи та/або повноважень користувачеві необхідно пройти біометричну ідентифікацію та пред'явити (ввести) додаткові ідентифікатори з числа згаданих вище.

Основна мета застосування багатофакторних систем - прискорення процесу ідентифікації або надання можливості розпізнавання без звернення до централізованої бази даних ідентифікаторів (наприклад, коли відомості про відбитки пальців заносяться в пам'ять смарт-картки, що пред'являється під час ідентифікації, та модель відбитка, внесена в пам'ять картки, порівнюється з моделлю знову пред'явленого ідентифікатора).

Єсімов С. С.,
професор кафедри адміністративно-правових дисциплін Інституту права Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент

СИСТЕМИ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ В УМОВАХ ЦИФРОВІЗАЦІЇ ЕКОНОМІКИ

Національна економічна стратегія на період до 2030 року ставить завдання впровадження цифрових технологій у фінансову сферу України [1]. Це ставить завдання підготовки спеціалістів-правників, які мають високий рівень знань у сфері інформаційних технологій, що застосовуються у фінансовій сфері держави. Процеси цифровізації економіки України розвиваються експоненційно та породжують відповідне прискорення поширення електронного документообігу.

Велика кількість операцій, здійснюваних між продавцями і покупцями різних товарів та послуг, проводяться через систему безготівкових платежів комерційних банків або безпосередньо через розрахунки між банком та клієнтом, або з використанням міжбанківських розрахунків.

Операції, що проводяться, враховуються в електронному документообігу банка. Подібні завдання виникають при організації фінансової звітності, оподаткування та інших видів інформаційної взаємодії між підприємствами та державою.

Для здійснення електронних розрахунків між банками та організаціями укладаються відповідні договори на розрахунково-касове обслуговування із застосуванням документів в електронній формі (платіжні доручення, витяги з рахунку клієнта).

На підготовчому етапі забезпечення електронних платежів комерційний банк забезпечує організацію (клієнта) програмним забезпеченням, консультує клієнта з використання, видає ключі для шифрування інформації, використовуваної програмою. Відбувається реєстрація відкритих ключів підписів уповноважених співробітників організації, погодження з клієнтом системи паролів для екстреного призупинення операцій з рахунку та вирішення подібних моментальних завдань.

Узгодження обміну інформацією між підприємствами, банками та державними контрольними органами відбувається на засадах взаємодії відкритих систем. На відповідних рівнях інформаційної взаємодії вирішується проблема доступу до закритих даних, що становлять комерційну, банківську чи державну таємницю. Здійснюються й інші дії щодо забезпечення безпеки електронних платежів, у тому числі у рамках боротьби з відмиванням злочинних доходів.

Банківська автоматизована система класу «Клієнт-Банк», створена для віддаленого обслуговування, спростила процес здійснення операцій юридичних осіб з банківським рахунком. Система «Клієнт-Банк» може діяти як самостійна система, а може бути компонентом складнішої, ієрархічно організованої комплексної системи.

У більшості систем «Клієнт-Банк» клієнтське програмне забезпечення оновлюється автоматично у міру змін, що вносяться до законодавчих та нормативних актів, вимог банку, пропозицій клієнтів. Для ефективної роботи комерційних банків прагнуть модернізувати систему «Клієнт-Банк».

Пропонують не лише обмін стандартним набором платіжних документів, а й індивідуальні блоки з огляду на специфіку роботи клієнта. Одним із пріоритетних напрямів розвитку системи «Клієнт-Банк» у комерційних банках стала система «Інтернет – Клієнт – Банк». При використанні електронного фінансового документообігу виникають різні види ризиків, які можна віднести до традиційних і до специфічних, нових (цифрових).

Перші ризики пов'язані з помилками працівників, порушення правил проведення платіжних операцій (несвоєчасне чи неправильне зарахування – списання коштів у рахунках, невиконання чи належне виконання доручення клієнта про здійснення платежу користь одержувача коштів).

Друга група ризиків пов'язана з технічними збоями, через які відбувається ненадійне виконання зобов'язань або порушення вимог безпеки електронних розрахунків, комп'ютерне шахрайство, що призводить до збитків учасників електронного документообігу.

При недостатньо якісному програмному забезпеченні може виникнути проблема із зашифровкою або розшифровкою інформації фінансових документів, статися технічний збій, при якому вірний електронний підпис може бути сприйнятий як фальшивий. Існуючий електронний документообіг можна поділити на три види: універсальний, індивідуальний, комбінований.

При здійсненні безготівкових платежів за допомогою електронних документів комерційними банками встановлюються відповідний порядок, визначений правилами ведення таких операцій або договором дистанційного банківського обслуговування, або інструкціями [2], що включають:

- по-перше, для формування електронних документів використовується шаблон для цього виду документа. Сформоване електронне повідомлення має бути підписане електронним підписом.
- по-друге, при надсиланні та доставці електронних документів дотримуються певних правил відправлення, доставки та отримання документів. При отриманні документа обов'язково перевіряється о відповідність існуючому формату, справжність, перевіряється електронним підписом.

При позитивному результаті перевірки відбувається підтвердження отримання електронних документів з присвоєнням категорії документа. У разі потреби учасник системи електронного документообігу, до початку виконання одержувачем, може відкликати електронний документ. З цією метою він надсилає одержувачу повідомлення про відкликання з причиною відкликання електронних документів.

- по-третє, під час здійснення електронного документообігу здійснюється обов'язкова реєстрація всіх вхідних і вихідних електронних документів. З цією метою ведеться електронний журнал обліку. Головне завдання комерційного банку в даному випадку забезпечити захист від несанкціонованого доступу та ненавмисного знищення, спотворення облікових даних.

Одне з основних завдань при використанні електронних фінансових документів пов'язане із захистом керованого файлового обміну між учасниками, як між платником та одержувачем, клієнтами та банком, банком та Національною платіжною системою [3].

Цифрова епоха, що настала, диктує необхідність радикального вдосконалення законодавчої бази, принципів роботи правоохоронних органів у боротьбі з новими видами злочинів.

Системи «Клієнт-Банк» повинні бути стійкими до можливих атак, зламів та шахрайських операцій. Для відображення загроз повинні постійно вдосконалюватись на методологічному, алгоритмічному та апаратному рівнях.

Література:

1. Про затвердження Національної економічної стратегії на період до 2030 року : Постанова Кабінету Міністрів України від 03.03.2021 р. № 179. URL. https://zakon.rada.gov.ua/laws/show/179-2021-%D0%BF#n25
2. Про затвердження Змін до Інструкції про безготівкові розрахунки в Україні в національній валюті : Постанова Національного банку України від 25.05.2021 р. № 44. URL. https://zakon.rada.gov.ua/laws/show/v0044500-21#n2
3. Про внесення змін до деяких законодавчих актів України щодо спрощення залучення інвестицій та запровадження нових фінансових інструментів : Закон України від 19.06.2020 р. № 738-IX. URL. https://zakon.rada.gov.ua/laws/show/738-20#n3852

Зачек М. О.,
здобувач вищої освіти Львівського державного університету внутрішніх справ

Сеник В. В.,
завідувач кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів Львівського державного університету внутрішніх справ, доцент кафедри обчислювальної математики та програмування Національного університету «Львівська політехніка», кандидат технічних наук, доцент

СТРАТЕГІЯ CLOUD FIRST – ВИКЛИКИ ТА ПРОБЛЕМИ РЕАЛІЗАЦІЇ В УКРАЇНІ

Однією із проблем, які виникли останніми роками в Україні є стримування розвитку інформаційно-телекомунікаційних технологій у сфері електронного урядування. Однією із причин такого стримування є відсутність нормативно-правового підгрунття для їх розвитку. Показовим прикладом цього факту є затягування у прийнятті та впроваджені положень Закону України «Про хмарні послуги», який «…закладає засади для розвитку платформ інформаційно-комунікаційних технологій, що базуються на хмарних обчисленнях та реалізації політики переваги (пріоритету) хмарного середовища (Cloud First) у сфері державного управління, освіти, науки та інших сферах суспільного життя [1].

Стратегію Cloud First уже давно запровадили розвинені держави світу. Зокрема, США, Великобританія, Німеччина розпочали запровадження стратегії цифрової трансформації держави ще понад десять років тому. На нинішній час дана стратегія успішно застосовується і в інших державах, таких як: Шотландія, Сінгапур, Індія, Республіка Корея, Австралія, Данія, Канада, Саудівська Аравія та інші. Передумови, за якими стратегія Cloud First стала актуальною, однакові практично у всіх вищеперелічених державах. За десятиріччя фахівцями ряду держав проведені розрахунки та визначено економічну ефективність її запровадження. Так, наприклад, впровадження хмарних технологій державними органами Великобританії дозволило зменшити витрати на цифровій трансформації та інформаційних технологіях з 2012 до 2015 року на 3,56 млрд фунтів стерлінгів [2].

За даними журналу The Economist, обсяги цифрової інформації збільшуються в десять разів кожні п'ять років. Враховуючи темпи росту та попередні підрахунки експертів відносно України, за умови відсутності кардинальних змін щодо структури та динаміки закупівель, сукупні витрати державного сектора на IT закупівлі в період 2020–2024 років досягнуть 100 млрд грн (в 2018 році ця сума була 15,8 млрд грн, а обсяг витрат на хмарні рішення був всього лише 0,2%). У 2017 сума складала 9,8 млрд грн. У разі хоча б часткової реалізації стратегії Cloud First (приблизно 50% потреб в IT сфері буде задовольнятися за рахунок хмарних послуг, а не капітальних інвестицій), а сукупна економія може досягти 40 млрд грн. за період 2020-2024 рр [3].

Аналіз використання даної стратегії у згаданих країнах також показав ряд переваг, зокрема:

- ефективність – отримання максимального результату за мінімальні витрати на розбудову інформаційно-телекомунікаційних систем, та на придбання програмного забезпечення;
- успішність – запроваджені IT-проєкти є довгостроковими;
- зниження умов для корупційних діянь – використання стратегії Cloud First дозволяє виключити у ряначній мірі корупційні ризики, у звязку із відсутністю фізичного контакту між сторонами, наприклад, закупівлі товарів;
- гнучкість та оперативність – органі державної влади можуть працювати швидко під час впровадження інновацій, формування технічних завдань, а також під час закупівлі апаратного та програмного забезпечення для державних інформаційних систем;
- захищеність – покращений рівень захищенності державних інформаційно-телекомунікаційних систем від алгоритмічних та програмних помилок;
- кваліфікація – рівень підготовки фахівців, які працюють у державному секторі відповідає рівню підготовки фахівців із комерційних структур тощо.

Окремими проблемами, які потребують нормативно-правового регулювання під час запровадження стратегії Cloud First є необхідність визначення ряду термінологічних понять (наприклад: «хмарні послуги», «хмарні обчислення», «хмарні ресурси»), уведення переліку хмарних сервісів, встановлення вимог до надавача хмарних послуг, визначення особливостей надання та споживання хмарних послуг органами державної влади та органами місцевого самоврядування, оброблення персональних даних та захисту інформації під час надання хмарних послуг.

Ще одним питаням є необхідність внесення змін та доповнень до ряду нормативно-правових документів, які регулюють обіг інформації в Україні з метою врегулювання відносин щодо оброблення окремих видів інформаційних ресурсів у системах хмарних обчислень та закупівлі хмарних послуг органами державної влади, органами місцевого самоврядування, військовими формуваннями, утвореними відповідно до законів України, державними підприємствами, установами та організаціями, суб'єктами владних повноважень та іншими суб'єктами, яким делеговані такі повноваження. До таких нормативно-правових документів належать закони України «Про захист інформації в інформаційно-телекомунікаційних системах» [4], «Про захист персональних даних» [5], «Про публічні закупівлі» [6].

Таким чином, прийняття та впровадження Закону України «Про хмарні послуги» сприятиме активізації робіт із запровадження новітніх інформаційно-телекомунікаційних технологій у публічному секторі, що дозволить створити умови для ефективного використання державних ресурсів відповідно до Стратегії розвитку інформаційного суспільства в Україні шляхом впровадження новітніх технологій під час оброблення інформацій них ресурсів, зокрема, сприятиме економії коштів державного бюджету та можливостям їх перерозподілу, у тому числі на реалізацію проєктів електронного урядування, проєктів дистанційного навчання та забезпечення більшої доступності державних послуг фізичним і юридичним особам, а також сприятиме надходженню до України більш 10 млрд приватних інвестицій у найближчі п'ять років.

Література:

1. Про хмарні послуги : Закон України (проект) від 20 грудня 2018 р. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/JI01021A.html
2. Government Digital Service. URL: https://gds.blog.gov.uk/2015/10/23/how-digital-and-technology-transformation-saved-1-7bn-last-year/
3. Куничак О. Країні потрібне законодавче регулювання сфери хмарних сервісів. URL: https://eba.com.ua/krayini-potribne-zakonodavche-regulyuvannya-sfery-hmarnyh-servisiv-eva/
4. 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/
5. 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/
6. Про публічні закупівлі : Закон України від 25 грудня 2015р. № 922-VIII. База даних «Законодавство України» / ВР України. URL : https://zakon.rada.gov.ua/laws/show/922-19#Text

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

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

ПРАКТИКА ТА ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ЧАТ-БОТІВ НАЦІОНАЛЬНОЮ ПОЛІЦІЄЮ УКРАЇНИ

Чат-боти непомітно стали реальністю нашого життя. Все більша кількість компаній використовують чат-ботів замість голосових помічників. Цей актуальний тренд не оминув і діяльність Національної поліції України. Розглянемо основні напрямки та перспективи використання чат-ботів поліцією.

Чат-бот (англ. Chatbot) – це комп'ютерна програма, яка використовує нейромережі та технології машинного навчання, і здійснює спілкування за допомогою голосових або текстових методів. Сьогодні чат-боти відіграють роль віртуальних помічників на сайтах багатьох організацій для надання потрібної інформації. Чат-боти – це програмні продукти, які імітують спілкування з людиною в месенджерах [1].

Зупинимося саме на використанні чат-ботів у діяльності Національної поліції України. Чат-боти у цій сфері можуть використовуватись для:

- Підвищення рівня правової свідомості громадян та взаємодії з поліцією;
- Протидії, шляхом моніторингу в соціальних мережах, кібербулінгу, торгівлі наркотичними засобами, поширенню інформації сексуального характеру, тощо;
- Оперативного реагування на заяви та повідомлення громадян органами та підрозділами Національної поліції (надається доступ до відео, фото фіксації тієї чи іншої події);
- Надання юридичних консультацій, підготовка юридичних документів, оплата штрафів і зборів, тощо [2].

Розглянемо приклади практичної реалізації цих напрямків.

Працівники Національної поліції в м. Суми створили Telegram-чат «Безпечне місто Суми», користувачами якого є вже понад 5000 осіб. Подібні чати також існують в Кропивницькому, Ужгороді, Рівному, Мукачеві та Вінниці. Це не Telegram-бот, а саме Telegram-чат, де інформацію, яка надходить, цілодобово обробляє людина-адміністратор та здійснює заходи реагування. Вдень в чаті працює адміністратор, а вночі – працівник чергової частини, який ознайомлюється з інформацією в чаті та з'ясовує, чи належить подія до компетенції поліції. І якщо питання не підвідомче поліції, повідомлення передається до відповідної служби. У чаті весь склад патрульної поліції міста і, виїжджаючи на виклик, вони вже мають інформацію щодо події, мають орієнтування щодо пошуку маршруту та певних осіб, або можуть зателефонувати через Telegram заявнику, щоб дізнатися деталі події. Після створення цього чату у Сумах констатують збільшення звернень до поліції, в тому числі щодо адміністративних правопорушень у сфері безпеки дорожнього руху, порушення правил паркування транспортних засобів, порушення тиші у нічний час, а також надання допомоги особам, які потребують поліцейського піклування [2].

Колишній патрульний поліцейський Олександр Харченко створив Telegram-бот «БамперБот», для надання допомоги водіям, які потрапили у ДТП: наводить алгоритм дій, допомагає скласти євро протокол, дає поради щодо спілкування з поліцією.

Громадський активіст Богдан Пашковський створив у Telegram @ifpolice_bot – це бот ГУНП в Івано-Франківській області. Сторінка боту прикріплена до чату «Франківськ 112» і на ній поліція реагує на важливі повідомлення через бота, надсилає інформацію в «Франківськ 112», кожен може зв'язатися з поліцією в Telegram, написавши приватне повідомлення. Але пріоритетною залишається «Лінія 102» [2].

Викладач Рівненської комп'ютерної академії ШАГ та його учні розробили чат-бот KidsPolice на базі месенджеру «Telegram», з метою інформування дітей та їх батьків щодо роботи ювенальних поліцейських, а також надання їм підтримки та оперативної допомоги. У розділі «Ювенальна поліція» користувачі зможуть ознайомитися із поліцейським, що служить на їх території, зателефонувати йому або написати особисте повідомлення; за допомогою «Карти» можна подивитися геолокацію найближчого поліцейського відділу; клавіша «СТОП Кібербулінгу» перенаправить у бот-програму "Кіберпес", в якій

розповідається про можливі дії дітей, батьків та вчителів у випадку кібербулінгу. Також можна дізнатись, як самостійно видалити образливі матеріали із соціальних мереж, та куди звертатись по допомогу. Натиснувши «Дій проти насильства», користувач перейде на чат-бот МВС #ДійПротиНасильства [3].

Співробітники відділу ювенальної превенції Управління превентивної діяльності ГУНП в Миколаївській області на базі «Telegram» розробили чат-бот «Ювенальна превенція Миколаївської області» з метою забезпечити превентивну роботу в дитячому середовищі, налагодити більш тісну комунікацію працівників ювенальної превенції із дітьми та їхніми батьками, оперативно реагувати на надзвичайні події за участю дітей. Тут можна отримати інформацію про ювенального поліцейського, який закріплений за територією, а саме: прізвище, ім'я, по батькові разом із фотокарткою поліцейського; адресу підрозділу; номери телефонів чергової частини підрозділу та мобільний номер працівника поліції; електронну адресу та номери телефонів соціальних служб, із якими співпрацює поліцейський у сфері захисту прав дитини. Можна отримати також інформацію і про поліцейських офіцерів громади. Є карта, на якій позначені всі територіальні підрозділи поліції та поліцейські станції області. Є посилання на нормативно-правові акти у сфері захисту прав та законних інтересів дітей. Розміщено актуальні оголошення про умови проведення конкурсів та відбору на посади поліцейських.

Користувачі чат-боту зможуть дізнатись про останні новини в офіційних інтернет-ресурсах ГУНП в Миколаївській області у Facebook «Ювенальна превенція Миколаївської області», Служби розшуку дітей, а також новини чат-боту «СТОП насильству». Небайдужі громадяни матимуть змогу ознайомитися із орієнтуваннями щодо пошуку безвісно зниклих дітей та долучитися до їхнього розшуку.

Користувач може поставити запитання безпосередньо співробітнику поліції за допомогою створеної групи у «Telegram», повідомлення в якій постійно моніторять два співробітника відділу ювенальної превенції УПД ГУНП в Миколаївській області [4].

Чат-бот #Вибори2020 створено для захисту волевиявлення громадян і реагування на факти порушення виборчого процесу під час виборів до Верховної Ради України. З його допомогою територіальні органи Національної поліції зареєстрували 4209 повідомлення, пов'язаних із виборчим процесом. Усього до ЄРДР внесено відомості щодо 309 кримінальних правопорушень. Також складено 1067 протоколів про вчинення адміністративних правопорушень, пов'язаних з виборчим процесом [5].

МВС відкрило у Telegram чат-бот #ДійПротиНасильства, який допомагає запобігати домашньому насильству. Він може допомогти викликати поліцію та "швидку", надати контакти інших служб допомоги, переадресувати на спеціалістів безоплатної правової допомоги, які дадуть онлайн юридичну консультацію. Чат-бот також може роз'яснити, що таке домашнє насильство, та як йому протидіяти, розповісти про повноваження органів і установ, котрі здійснюють заходи для запобігання домашньому насильству [6].

Зараз МВС у співпраці з Міністерством у справах ветеранів вже випустило оновлення чат-боту #ДійПротиНасильства. Тепер в ньому доступна інформація про територіальні органи Міністерства у справах ветеранів для тих, хто цього потребує. Користувачі можуть отримувати інформацію щодо контактів служб допомоги на регіональному рівні. А в розділі «Заходи впливу на кривдника» є інформація про те, що таке терміновий заборонний та обмежувальний приписи [7].

Співробітники Управління превентивної діяльності ГУНП в Миколаївській області запустили Telegram-бот «Стоп насильству». Його завдання – оперативне надання консультацій, допомога та підтримка громадян в умовах карантину, коли існують обмеження в особистих прийомах. У зв'язку із запровадженням карантину люди змушені проводити більше часу разом, що інколи може спричиняти напруженість у стосунках та вчинення домашнього насильства [8].

1 квітня 2021 р. було запущено чат-бота для Ніжинського відділення поліції та співробітників Муніципальної Варти. Чат-бот буде працювати одразу на двох платформах: Telegram та Viber. Він буде пересилати повідомлення користувачів в окрему групу, де на них будуть реагувати представники Варти (оператори) та Ніжинського відділу поліції. Основне завдання чат-бота прийом анонімних повідомлень про місця паління вогнищ, а також про правопорушення [9].

Громадська організація «Турбота» за підтримки німецького фонду «Пам'ять, Відповідальність, Майбутнє» (EVZ) та благодійного фонду «Гендер Зед», розробила чат-бот «161» (стаття 161 Кримінального кодексу «Про порушення рівноправності громадян залежно від їх расової, національної належності, релігійних переконань, інвалідності та за іншими ознаками»). Чат-бот допоможе всім охочим,

у тому числі поліцейським, розібратися з тим, що таке злочини на ґрунті ненависті, як їх фіксувати, як захистити себе і краще розбиратися у темі. Чат-бот діє на основі месенджера у Facebook [10].

Чат-бот «СтопНаркотик» був розроблений курсантами та науково-педагогічними працівниками факультету № 4 (кіберполіції) Харківського національного університету внутрішніх справ. Уперше чат-бот був презентований 19.09.2019 на засіданні Координаційної ради з протидії наркоманії Харківської міської ради [11].

Telegram чат-бот «СтопНаркотик» може отримувати від користувачів: фотографії написів («графіті») та наліпок з «рекламою наркоадрес» із зазначенням GPS-координат або фізичних адрес, де вони були виявлені; знімки екранів (скріншоти) з «рекламою наркоадрес» у популярних соціальних комп'ютерних мережах; електронні адреси в Telegram та вебсайтів в Інтернет, що використовуються для продажу наркотиків; адреси, за якими здійснюється продаж наркотиків в населених пунктах. Також він може залучати громадян до блокування електронних адрес у Telegram шляхом надсилання скарг до адміністрації месенджеру з відомостями про адреси, за допомогою яких здійснюється незаконне розповсюдження наркотиків; та до зафарбовування «графіті» з «наркоадресами».

Широку інформаційну підтримку щодо поширення серед населення інформації про чат-бот та його можливості здійснюють МВС України, у тому числі Управління забезпечення формування державної політики у сфері протидії наркозлочинності; Департамент протидії наркозлочинності Національної поліції України та його територіальні підрозділи; ГУНП в областях, у тому числі в Донецькій області; Київська обласна рада; Харківська міська рада; Кременчуцька міська рада.

На теперішній час до користувачів чат-боту долучилися понад 30 тис. осіб, у тому числі мешканці тимчасово окупованих територій України. Небайдужі громадяни допомогли заблокувати понад 1500 електронних адрес у Telegram, що використовувались для незаконного збуту наркотиків через мережу Інтернет, у тому числі 10 «наркокрамниць» на тимчасово окупованих територіях Донецької та Луганської областей та 3 «наркокрамниці» в Автономній Республіці Крим. За час роботи чат-боту користувачі надіслали на перевірку більше 20 тис. зображень з «рекламою» електронних адрес «інтернет-наркокрамниць»; майже 30 тис. електронних адрес у месенджері Telegram; 2320 гіперпосилань на вебсайти [11].

Чат-бот «ДійПротиНаркотиків» у Telegram розроблено співробітниками управління боротьби з наркозлочинністю в Донецькій області ДБН Нацполіції України в рамках Програми ООН із відновлення та розбудови миру за фінансової підтримки урядів Данії, Швейцарії та Швеції. Чат-бот діє на всій території Донецької області. Громадяни можуть анонімно надати інформацію про відомі факти наркозлочинів: обрати населений пункт, район та надати детальну інформацію щодо осіб, причетних до наркообігу, та фізичні адреси, де здійснюється продаж, виготовлення чи вживання незаконних речовин. Інформація всебічно аналізується та перевіряється працівниками кримінальної поліції територіальних підрозділів з метою викриття розповсюджувачів, постачальників та організаторів каналів збуту наркотиків тощо. Про ефективність свідчать вже заблоковані 2200 наркоадрес, про які громадяни повідомили до поліції за допомоги чат-боту «СтопНаркотик» [12].

Чат-бот @StopDangerBot в «Telegram» було презентовано 22.03.2021 у Харківській міській раді. Чат-бот працює таким чином: людина фіксує на відео або фото поширення наркотиків (продаж або закладка), відзначає геолокацію і записує аудіоповідомлення про подію, натискає кнопку «Швидке реагування» і відправляє інформацію. Розробники чат-бота, представники громадської організації «Hunters Kharkov», зазначили, що анонімність звернень гарантується, а інформація надходить правоохоронцям протягом хвилини. Начальник ГУНП в Харківській області Андрій Рубель зазначив, що особисто перевірив роботу чат-бота – після того, як відправив фото, де ймовірно були залишені наркотики, патрульні приїхали через 7 хвилин [13].

У м. Бахмут діє чат-бот для протидії продажу наркотиків «Стопнаркотик» (https://t.me/StopDrugsBot) в «Telegram». Користувачі анонімно відправляють в чат-бот нарко-адресу в «Telegram», внаслідок чого робота інтернет-магазинів, які здійснюють продаж наркотичних речовин, блокується [14].

Чат-бот AntiDrugKropBot із протидії наркозлочинності впроваджено за ініціативою Головного управління Національної поліції в Кіровоградській області та управлінням боротьби з наркозлочинністю в Кіровоградській області ДБН Нацполіції України. Скориставшись програмою, громадяни можуть анонімно

надати відому їм інформацію (текст, фото, відео) про наркозлочини, а також отримати консультацію спеціалістів та контакти «телефону довіри» [15].

МВС України розробило чат-бот «СтопНаркотик» в Telegram для боротьби із «закладками». За час роботи чат-боту 3,6 тисячі користувачів надіслали на перевірку 4769 зображень з адресами «закладок», 7318 адрес у Telegram, 811 адрес веб-сайтів. Вже заблоковано 214 адрес у Telegram, що використовувалися зловмисниками для незаконного розповсюдження наркотиків, у тому числі 6 «наркокрамниць», на тимчасово окупованій території Донецької та Луганської областей [16].

І, нарешті, створено загальноукраїнський чат-бот DrugHunters («Мисливці за наркотиками») – офіційний чат-бот від патрульної поліції у Telegram. Скористатись чат-ботом можуть анонімно усі громадяни у тих містах, де працює патрульна поліція. Щоб залишити заявку про можливе місце закладки чи закладника, достатньо розпочати діалог у Telegram, вказавши населений пункт та адресу, за якою побачили потенційного зловмисника, а також опис місця, де на думку заявника може бути закладка. Для того, щоб правоохоронці швидше виявили закладку, потрібно надіслати геолокацію й додати фото чи відео з місця наркозлочину. Після отримання повідомлення про знахідку або ймовірного закладника, патрульні виїжджатимуть на місце і перевірятимуть інформацію [17].

Перший заступник начальника Департаменту патрульної поліції Олексій Білошицький повідомив, що за першу добу на чат-бот DrugHunters надійшло 52 звернення від громадян. За словами Білошицького, пілотні версії чат-боту працювали у Львові й Одесі та довели свою ефективність. За допомогою цієї програми правоохоронці виявили сотні місць із закладками, а також затримували осіб, які їх розповсюджують [18].

Отже, ми бачимо, що з кожним днем зростає кількість чат-ботів, які використовує Національна поліція України. Вони допомагають збільшити ефективність протидії злочинності. У перспективі їх кількість буде збільшуватись. Основною проблемою, яка потребуватиме вирішення, є відсутність нормативно-правового регулювання використання чат-ботів Національною поліцією.

Література:

1. Рижкова С.А. Використання чат-ботів в діяльності Національної поліції як інструмент побудови партнерських відносин з населенням / С.А. Рижкова // Використання сучасних інформаційних технологій в діяльності Національної поліції України: матеріали Всеукр. наук.-практ. семінару (м. Дніпро, 28 листопада 2019 р.). Дніпро: ДДУВС, 2019. С. 59-62. URL: https://er.dduvs.in.ua/handle/123456789/4989.
2. Рижкова С.А. Використання чат-ботів в діяльності національної поліції як інструмент побудови партнерських відносин з населенням. // URL: http://er.dduvs.in.ua/bitstream/123456789/4989/1/8%D1%80.pdf.
3. Поліція запровадила для дітей чат-бот «KidsPolice» // Рівне вечірне від 23.10.2021. URL: https://rivnepost.rv.ua/news/ politsiya-zaprovadila-dlya-ditey-chatbot-kidspolice.
4. Миколаївські ювенали запустили чат-бот задля дієвої комунікації громадян із поліцією // Портал МВС від 7-го червня 2021 URL: https://mvs.gov.ua/uk/press-center/news/ mikolayivski-yuvenali-zapustili-cat-bot-zadlya-dijevoyi-komunikaciyi-gromadyan-iz-policijeyu.
5. МВС запустило чат-бот «Вибори-2020» для забезпечення прозорого виборчого процессу. // Урядовий портал від 13 жовтня 2020 року. URL: https://www.kmu.gov.ua/news/mvs-zapustilo-chat-bot-vibori-2020-dlya-zabezpechennya-prozorogo-viborchogo-procesu.
6. МВС запустило у Telegram чат-бот для протидії домашньому насильству // Укрінформа від 05.11.2021. URL: https://www.ukrinform.ua/rubric-technology/3002636-mvs-zapustilo-u-telegram-catbot-dla-protidii-domasnomu-nasilstvu.html.
7. МВС у співпраці з Міністерством у справах ветеранів випустило оновлення чат-боту #ДійПротиНасильства. // Урядовий портал від 16.11.2020. URL: https://www.kmu. gov.ua/news/mvs-u-spivpraci-z-ministerstvom-u-spravah-veteraniv-vipustilo-onovlennya-chat-botu-dijprotinasilstva.
8. Миколаївські поліцейські запустили чат-бот із протидії домашньому насильству. // Legalaid від 03.04.2020. URL: https://www.legalaid.gov.ua/novyny/mykolayivski-politsejski-zapustyly-chat-bot-iz-protydiyi-domashnomu-nasylstvu.

9. Для Ніжинської поліції та Муніципальної варти створено анонімного чат-бота для повідомлень. // mynizhyn.com від 2 Квітня 2021. URL: https://mynizhyn.com/news/misto-i-region/18920-dlja-nizhinskoyi-policiyi-ta-municipalnoyi-varti-stvoreno-anonimnogo-chat-bota-dlja-povidomlen.html.
10. Чат-бот допомагає кропивницьким поліцейським протидіяти злочинам на ґрунті ненависті. // «3 перших уст» від 26.02.2021. URL: https://zpu.kr.ua/suspilstvo/21556-yak-chat-bot-dopomahaie-kropyvnytskym-politseiskym-protydiiaty-zlochynam-na-hrunti-nenavysti.
11. Користувачі чат-боту «СтопНаркотик» допомогли заблокувати 1500 наркоадрес. // Портал МВС від 26-го серпня 2020. URL: https://mvs.gov.ua/uk/press-center/news/ Koristuvachi_chat_botu_StopNarkotik_dopomogli_zablokuvati_1500_narkoadres_33548.
12. На Донеччині запрацював поліцейський чат-бот щодо протидії наркозлочинності. // Поліція Донеччини від 02.06.2021. URL: https://police.dn.ua/news/view/na-donechchini-zapratsyuvav-politsejskij-chat-bot-shhodo-protidii-narkozlochinnosti.
13. Харків'яни можуть анонімно повідомляти про розповсюдження наркотиків. // Офіційний сайт Харківської міської ради, міського голови, виконавчого комітету від 22.03.2021. URL: https://www.city.kharkov.ua/uk/news/ kharkivyani-mozhut-anonimno-povidomlyati-pro-rozpovsyudzhennya-narkotikiv--46937.html.
14. Поліцейські Бахмута запрошують громадськість приєднатися до чат-ботів з протидії незаконному розповсюдженню наркотиків. // Сайт Бахмутського районного відділу поліції від 03.11.2021. URL: http://bahmut-police.dn.ua/news/view/8389.
15. Чат-бот AntiDrugKropBot із протидії наркозлочинності. // Сайт ГУНП Кіровоградської області. URL: https://kg.npu.gov.ua/gromadyanam/zvernennya/chat-bot-antidrugkropbot-iz-protidiji-narkozlochinnosti.html.
16. Чат-бот в Telegram допоміг МВС заблокувати понад 200 наркокрамниць: подробиці // «Судебно-юридическая газета в Украине» від 23.01.2020. URL: https://sud.ua/ru/news/ ukraine/158677-chat-bot-v-telegram-dopomig-mvs-zablokuvati-ponad-200-narkokramnits-podrobitsi.
17. Белей Аліса. Чат-бот «Мисливці за наркотиками»: як анонімно повідомити поліції про закладчика // Львівський портал від 09.11.2021. URL: https://portal.lviv.ua/ news/2021/11/09/chat-bot-myslyvtsi-za-narkotykamy-iak-anonimno-povidomyty-politsii-pro-narkozlochyn.
18. «Мисливці за наркотиками»: на чат-бот вже надійшло понад 50 звернень // Укрінформ від 10.11.2021. URL: https://www.ukrinform.ua/rubric-society/3347937-mislivci-za-narkotikami-na-catbot-vze-nadijslo-ponad-50-zvernen.html.

Зачко О. Б.,
професор кафедри права та менеджменту у сфері цивільного захисту Львівського державного університету безпеки життєдіяльності, доктор технічних наук, професор, Заслужений діяч науки і техніки України

Кобилкін Д. С.,
доцент кафедри права та менеджменту у сфері цивільного захисту Львівського державного університету безпеки життєдіяльності, кандидат технічних наук

Зачко І. Г.,
фахівець відділу Філії Товариства з Обмеженою Відповідальністю «Нестле Україна» Нестле Бізнес сервіс в Європі, кандидат технічних наук

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ У МЕНЕДЖМЕНТІ БЕЗПЕКИ ТРАНСКОРДОННИХ ТЕРИТОРІАЛЬНИХ СИСТЕМ

На сьогодні Україна є найбільшим критичним регіоном Європи з техногенного навантаження та потенційної небезпеки шкідливих виробників для населення і навколишнього природного середовища. Екологічна небезпека поглиблюється соціально-політичною напруженістю, викликаною екологічною та фінансовою нестабільністю, зростанням кількості надзвичайних ситуацій. Усе це створює об'єктивні передумови зростання кількості техногенних аварій, катастроф, посилення наслідків стихійних лих та інших надзвичайних ситуацій, що, як результат, створює низькі умови безпеки людини в цілому.

Незважаючи на постійне удосконалення методів, технічних та організаційних заходів направлених на ліквідації надзвичайних ситуацій, зусилля в цьому напрямку є усе менш ефективними. Економіка навіть високо розвинутих країн не в змозі збільшувати фінансування робіт з ліквідацій наслідків надзвичайних ситуацій та компенсувати витрати від них.

Впровадження інструментів та підходів менеджменту безпеки у транскордонних територіальних системах на сьогодні лежить у площині застосування інформаційних технологій, шляхом розробки та впровадження комплексу комп'ютерних моделей, методів, алгоритмів і програмних засобів оцінки ризиків виникнення надзвичайних ситуацій, прогнозування їх розвитку, оптимізації розподілу матеріальних і фінансових ресурсів та створення методики комплексної оцінки і управління ризиками виникнення надзвичайних ситуацій при формуванні регіональних проектів розвитку транскордонних територіальних систем.

Застосування інформаційних технологій у менеджменті безпеки транскордонних територіальних систем передбачає розв'язання наступних категорій взаємопов'язаних задач:

- ідентифікацію загроз техногенній та природній безпеці України і прикордонних територій;
- на основі визначення пріоритетів, елементів системи техногенної та природної безпеки проведення розрахунків комплексного показника потенційної небезпеки транскордонних регіонів України щодо виникнення надзвичайної ситуації;
- прогнозування максимальною збитку від катастрофи на територій транскордонних регіонів.
- методи і алгоритми вирішення оптимізаційних задач розподілу матеріальних і фінансових ресурсів.

Результат розв'язку поставлених завдань дозволить створити:

- методику прогнозування максимального збитку від катастроф за допомогою розподілу Парето;
- методи і алгоритми вирішення оптимізаційних задач розподілу матеріальних ресурсів.

Всі вище перераховані заходи забезпечать в перспективі досягнення кінцевої мети – забезпечення безпечного функціонувння транскордонних територіальних систем засобами інформаційних технологій.

Суттєвою перевагою запропонованих методик, методів та підходів є розробка методики комплексної оцінки і управління ризиками виникнення надзвичайних ситуацій при формуванні регіональних проектів удосконалення системи безпеки транскордонних територіальних систем засобами інформаційних технологій, що є складовою програми регіонального розвитку.

Основною робочою концепцією застосування інформаційних технологій у менеджменті безпеки транскордонних територіальних систем є розробка системного і наукового підходу до вивчення

надзвичайних ситуацій, моделювання та оцінки ризику їх виникнення, прогнозування аварій техногенного характеру та оперативне реагування на них, зниження ризиків виникнення аварій та катастроф, що є основою національної стратегії забезпечення захисту населення і територій від надзвичайних ситуацій.

Успішне виконання комплексу заходів можливе завдяки подальшому дослідженню причинно-наслідкових зв'язків від виникнення надзвичайних ситуацій, залучення допоміжних науково-технологічних засобів. А розроблений в процесі дослідження комплекс комп'ютерних моделей, методів і алгоритмів знайде практичне використання в Управлінні прогнозування ДСНС України, головних управліннях ДСНС України, інших підрозділах, які відповідають за ліквідацію наслідків НС, на потенційно небезпечних об'єктах в якості інструменту для отримання чисельних оцінок ризику і проведення на цій основі декларування безпеки підприємств, територій, зон, регіонів тощо.

Література:

1. Rak Y. Model of resource management in projects of the conditions improvement of implementation of System 112 / Y. Rak, D. Kobylkin. // Technology, Computer science, Safety Engineering: Scientific issues Jan Długosz University in Czestochowa. – 2014. – Tom№ 2. – P. 297-301.
2. Зачко О. Б. Теоретичні підходи до управління безпекою в проектах розвитку складних систем / О. Б. Зачко // Управління розвитком складних систем. – 2015.– № 22. – С. 48-53.
3. Зачко О. Б., Головатий Р. Р. Імітаційне моделювання потоку відвідувачів торгово-розважального центру. Управління проектами: стан та перспективи: матер. XII міжнар. наук.-прак. конф. Миколаїв: МНУК, 2016. С. 96-98.
4. Зачко О. Б., Кобилкін Д. С. Управління освітніми проектами в безпеко-орієнтованих системах засобами віртуального ситуаційного центру. Електронне наукове фахове видання "Інформаційні технології і засоби навчання". Київ, 2018. № 65. С. 12-24.
5. Зачко О. Б., Кобилкін Д. С., Головатий Р. Р. Structural model of projects management of safety providing at objects with mass stay of people. Проблеми та перспективи розвитку системи безпеки життєдіяльності: Зб. наук. праць XII Міжнар. наук.-практ. конф. молодих вчених, курсантів та студентів: [в 2 ч.]. Ч. 2. Львів: ЛДУ БЖД, 2017. С. 100-101.
6. Зачко О.Б. Інтелектуальне моделювання параметрів продукту інфраструктурного проекту (на прикладі аеропорту «Львів»). Східно-Європейський журнал передових технологій. 2013. № 1/10(61). С. 92-94.
7. Кобилкін Д.С., Устіловський Я.В. Офісне проектно-орієнтоване управління Системою 112 для забезпечення стану екологічної безпеки. Сталий розвиток 2013 – науковий дебют: зб. статей. Варшава: Вища школа менеджменту, 2014. С. 117-128.
8. Рак Ю.П. Методи аналізу та оцінки рівня безпеки життєдіяльності регіонів України в умовах реалізації проектів регіонального розвитку / Рак Ю.П., Зачко О.Б. // Управління проектами та розвиток виробництва, 2008. – № 2(26). – С. 29-39.

Карелін Є. І.,
здобувач вищої освіти Дніпропетровського державного університету внутрішніх справ

Прокопов С. О.,
старший викладач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ

ДОСВІД РОБОТИ СИТУАЦІЙНОГО ЦЕНТРУ ГУНП В ДНІПРОПЕТРОВСЬКІЙ ОБЛАСТІ.

Боротьба з правопорушеннями, і перш за все з кримінальними, в значній мірі залежить від інформаційного забезпечення діяльності правоохоронних органів. В умовах стрімкого зростання інформаційних потоків і недостатність часу для прийняття необхідних управлінських заходів важливим стає створення сучасного науково-технологічного підрозділу, який сприяє оперативному інформаційно-аналітичному забезпеченню діяльності правоохоронних органів і прийняттю своєчасних ефективних управлінських рішень.

Такими підрозділами є Ситуаційні центри управлінь національної поліції. Основою цих центрів є не лише спеціально обладнане приміщення, але і відповідні інформаційні, телекомунікаційні, програмні та методичні засоби з метою вироблення відповідних управлінських рішень. Співробітники правоохоронних органів у своїй роботі постійно використовують сучасні технології. І чим більше цих технологій, тим складнішим стає процес їх об'єднання і інтеграції [1]. Тому рішенням цієї проблеми стає об'єднання існуючих потоків інформації і інструментів управління в єдиний інформаційний візуальний простір на базі геоінформаційних систем. Подібні рішення дозволяють повноцінно організувати збір необхідної інформації, її обробку, аналіз і надання доступу до результатів обробки. Впроваджуючи геоінформаційні системи в роботу ситуаційних центрів, поліція отримує програмну платформу для реалізації ефективного управління та реагування в справі охорони громадського порядку та боротьби з правопорушеннями. Геоінформаційні системи з самого початку створювалися для збору, аналізу і відображення даних в найбільш зрозумілому людині вигляді: шляхом нанесення на карту.

Ситуаційні центри надають наступні можливості. як оперативний доступ до легкої для розуміння карти з виводом необхідної інформації, з використанням різних каналів передачі даних. збір, зберігання і обробка даних про злочини, правопорушників, підозрюваних, місцях підвищеної небезпеки і будь-яких інших типах об'єктів, надання результатів аналітичної роботи для виявлення залежності між кримінально значущою інформацією і прогнозованими ризиками при плануванні оперативно-розшукових заходів. А також підвищення ефективності планування і прийняття управлінських рішень. Ситуаційний центр, як правило, розміщується на базі окремого підрозділу, в якому є прямий доступ не тільки до різних джерел інформації, але і до всіх ключових співробітників, включаючи керівництво і конкретних виконавців. Ситуаційний центр, перш за все, побудований на аналізі ситуації.

За словами начальника Департаменту організаційно-аналітичного забезпечення та оперативного реагування МВС України полковника поліції Сергєєва О.О. у Національній поліції України використовують три види аналізу [2].

Стратегічний (кримінологічний) – аналіз злочинності, її рівня, поширеності, динаміки, структури загалом. Проводиться аналіз стану злочинності в країні, визначається, в яких регіонах складна криміногенна ситуація, і що потрібно робити, щоб стабілізувати обстановку.

Другий рівень – тактичний аналіз. Це ситуація впродовж доби, тижня щодо конкретних регіонів, конкретних видів злочинів. Саме цим і займаються ситуаційні аналітики.

Третій рівень (один із найскладніших) – практичний. Це оперативний кримінальний аналіз. Це робота щодо кожного конкретного тяжкого та особливо тяжкого злочину.

Більш детально розглянемо практичний вид тактичного аналізу на прикладі Ситуаційного центру ГУНП в Дніпропетровській області.

Особа, яка здійснює моніторинг оперативної обстановки, аналіз інформації, моделює можливий розвиток ситуації, обробляє інформацію загального характеру та підготовку проектів управлінських рішень є ситуаційний аналітик

При отриманні інформації про гучний злочин, ситуаційний аналітик з використовуючи системи відеонагляду, відомчі бази даних та відкриті джерела інформації, передає отриману інтерактивну

інформацію нарядам поліції. Вказана інформація дуже важлива при реагуванні та розкритті кримінальних правопорушень по «гарячих слідах».

У 2018 році СЦ ГУНП надана інформація, що сприяли затриманню по «гарячих слідах» 69 осіб, із них 20 пограбувань, 1 умисне вбивство, 1 погроза вбивством, 1 зґвалтування, 1 насильницьке задоволення статевої пристрасті, 13 фактів спричинення тілесних ушкоджень, 13 крадіжок, 6 хуліганств, 30 водіїв транспортних засобів, які втекли з місць вчинення ДТП, 2 факти незаконного позбавлення волі, 1 шахрайство, 1 неправдиве повідомлення про загрозу вибуху, а також встановлено місце знаходження 3 безвісно зниклих дітей, 18 автомобілів, що знаходились в розшуку та інші.

Приведу приклад реагування на повідомлення про незаконне заволодіння транспортним засобом.

Так, 8 квітня цього року о 21.43 по спецлінії «102» надійшло повідомлення від громадянина Чорного про те, що по вулиці Льоні Голікова м. Дніпро троє невідомих осіб під погрозою зброї побили заявника, забрали гроші, мобільні телефони та незаконно заволоділи його автомобілем «Део Ланос», (д.з. АЕ4009НН) на якому зникли з місця вчинення злочину.

Відразу було введено в дію відповідну поліцейську операцію, забезпечено виставлення постів та заслонів, згідно з розробленим розрахунком.

Разом з цим, після надходження вказаного повідомлення ситуаційним аналітиком невідкладно було проаналізовано інформацію з камер відеоспостереження системи «Безпечне місто», за результатами якого в режимі он-лайн було визначено маршрут руху правопорушників на викраденому автомобілі та диспетчером негайно було орієнтовано найближчі автопатрулі УПП в Дніпропетровській області.

У результаті розшукуваний автомобіль та трьох зловмисників було затримано по «гарячих слідах» (по вулиці Універсальній) (Таранова 20 років, Станаєва 22 роки та Коробчана 31 рік, ЄРДР Індустріального ВП за ч.2 ст. 289 ККУ).

Таким чином, доцільно зробити висновок, що Ситуаційні центри Національної поліції України є важливою складовою для реалізації і забезпеченні взаємодії підрозділів поліції щодо підвищення ефективності боротьби з правопорушеннями. Також слід зазначити про необхідність збільшення штату ситуаційних аналітиків, які в свою чергу показали як їх праця облегшує роботу підрозділів Національної поліції. Це можна спостерігати на прикладі розкриття правопорушень по «горячих слідах» , що не було б забезпечено в повній мірі без інформаційно-аналітичної діяльності яку виконують Ситуаційні центри.

Література:

1. МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ НАКАЗ 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. URL: https://zakon.rada.gov.ua/laws/show/z0028-19#Text (Дата звернення: 07.12.2021)
2. Ситуаційний центр працює вже рік. Що це, навіщо він потрібен і як впливає на розкриття злочинів. URL: https://ua.112ua.tv/statji/sytuatsiinyi-tsentr-natspolytsyy-analiz-zlochynnostioperatyvnoi-obstanovky-ta-koordynatsiia-pidrozdiliv-431302.html (Дата звернення: 07.12.2021)

Католик Г. В.,
професор кафедри практичної психології Інституту управління, психології та безпеки Львівського державного університету внутрішніх справ, доктор психологічних наук, доцент

Калька Н. М.,
старший викладач кафедри практичної психології Інституту управління, психології та безпеки Львівського державного університету внутрішніх справ

Перун А.,
здобувач вищої освіти Львівського державного університету внутрішніх справ

ЕКЗИСТЕНЦІЯ ТА СЕНС ЖИТТЯ ОСОБИСТОСТІ В УМОВАХ КОВІДНОЇ РЕАЛЬНОСТІ

В умовах сучасної реальності, наповненої «вірусом паніки» та підсиленою панікою військового втручання, внаслідок тривалого перебування в карантинних обмеженнях через пандемію корона вірусу, особистість все частіше переживає негативні емоції, тривогу, агресію та депресивні стани різного формату. Нездатність планувати майбутнє, переживання за власне здоров'я та здоров'я і життя своїх рідних, інтенсивні та загрозливі інформаційні потоки, порушення звичного ритму життя породжують зростання нестабільності та «розхитують» особистісні сенси.

Дослідниця Волошина Л. та її колеги акцентують увагу на трьох особистісних вимірах, у яких перебуває особистість в умовах пандемії Covid -19 :

- соматичний вимір (стан фізичного здоров'я та стан організму при Covid- 19);
- психологічний вимір (психічна матерія в стані фізичної хвороби та постхворобливий стан);
- екзистенційний вимір (питання сенсу життя та благопполуччя в актульній ситуації повязаній з пандемією).

Екзистенційний вимір представлений четвіркою феноменів: перший вимір – фізичний (Umwelt), другий вимір - соціальний (Mitwelt) третій вимір – особистісний (Eidenwelt) і духовний (Uberwelt). Саме духовний вимір відповідає за цінності, принципи та віру, які забезпечують важливу опору у визначенні сенсу та усвідомленні цінності життя та самоцінності в ньому [1].

Фокусування на важливі моменти екзистенції: сенсу життя та свободу є надважливим в умовах тотального стресу, травматичних подій та гіперплинності нашого існування. Саме пошук сенсу є порятунком, що вселяє надію та підтримку, є рятувальним колом, що дає опору та відчуття перспективи. Ще свого часу В. Франкл наголошував, що життя людини не може позбутися сенсу ні за яких обставин; сенс життя завжди повинен бути у стані пошуку [3].

Відтак у реаліях сучасних соціальних умов (загроз пандемії та ймовірного зовнішнього військового втручання) важливим особистісним завдання є знайти нові, перспективно актуальні життєві сенси. Тому у сучасних реаліям актуальною стає формування сенсу життя через так звану «інтелектуальну вакцинацію», як спробу вприснути у свідомість людини сенс життя, на підставі якої вже не біологічний організм, а розум людини продукує свою «інтелектуальну вакцину» і з нею, постійно оновлюючись, торує життєву дорогу [1]. Інтелектуальна вакцинація передбачає рух від панівних станів страхів і тривожності до компенсаторних станів надії і пошуку сенсу життя. Завдяки цьому особистість набуває змісту і сенс життя, що є важливим кроком до одужання, життя і здоров'я.

ВІднайдення сенсу в умовах коронавірусної реальності га військових загроз забезпечить зменшення інтенсивності переживання стресу, депресії, тривоги, паніки і активує позитивні ресурси особистості, її розвиток, діяльність та творчість.

Літераптура:

1. Волошина Л., Леко Б., Кушніра Л. Сенс життя, екзистенційна психотерапія і COVID-19. Психосоматична медицина та загальна практика. №4. 2020. Режим доступу: URL: https://uk.e-medjournal.com/index.php/psp/article/view/269#title-0
2. Психологія і педагогіка у протидії пандемії COVID-19: Інтернет-посібник / за наук. ред. В.Г. Кременя ; [координатор інтернет-посібника В.В. Рибалка колектив авторів]. Київ : ТОВ «Юрка Любченка», 2020. 243 с.
3. Франкл В. Людина в пошуках справжнього сенсу. Харків: Клуб сімейного дозвілля, 2016. 160с.

Ковалів М. В.,
завідувач кафедри адміністративно-правових дисциплін Інституту права Львівського державного університету внутрішніх справ, кандидат юридичних наук, професор

Татусько Д. Р.,
здобувач вищої освіти Львівського державного університету внутрішніх справ

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ УКРАЇНИ

Інформаційне забезпечення органів державної влади України є основною умовою для сталого розвитку та ефективного функціонування державних механізмів, проведення процесу державного управління, яке відповідає сучасним міжнародним реаліям, внутрішньодержавним потребам. Реалізація зазначеного забезпечується проведенням єдиних організаційно-технічних заходів на території України органами влади центрального та регіонального рівнів, організаціями та підприємствами щодо забезпечення інформаційної безпеки від внутрішніх і зовнішніх загроз.

В результаті глобального соціально-економічного розвитку світу роль інформаційної безпеки неухильно зростає, тому можна говорити, що забезпечення інформаційної безпеки стало одним з важливих компонентів забезпечення національної безпеки.

Забезпечення інформаційної безпеки визначає наступні компоненти державної політики:

- нормативно-правовий компонент, розробка законодавства в інформаційній сфері, формування принципів проведення державної політики у сфері захисту інформації, інформаційних ресурсів, інформаційної інфраструктури;
- організаційно-технологічний компонент має на увазі функціонування інформаційно-комунікаційної інфраструктури;
- техніко-економічний компонент передбачає розробку та виробництво інформаційно-комунікаційних технологій;
- соціальний компонент – підготовка фахівців, ефективне використання технічних засобів та інформаційних систем.

Державна політика у сфері забезпечення інформаційної безпеки України проводиться і здійснюється у вигляді прийняття управлінських рішень, які ґрунтуються на законодавстві України, є основним обов'язком органів державної влади та уповноважених посадових осіб. Для здійснення та проведення державної політики, яка повинна бути спрямована на реалізацію національних інтересів України в інформаційній сфері, державною владою формуються:

- концептуальні документи, які визначають перспективи розвитку інформаційної сфери в Україні, в сфері забезпечення інформаційної безпеки – розробляються та приймаються відповідно до положень, закріпленими в Конституції України;
- законодавство в інформаційній сфері, що визначає правила та обмеження в галузі регулювання суспільних відносин в інформаційній сфері;
- організаційне та технологічне забезпечення діяльності держави в інформаційній сфері, організація державного нагляду та контролю, як об'єкта державного управління.

Забезпечення інформаційної безпеки здійснюється регламентуючими документами та нормативно-правовими актами, що визначають вимоги та критерії, загальну організацію робіт із забезпечення інформаційної безпеки, з виробництва та експлуатації систем захисту інформації; порядок виробництва, зберігання, продажі, передачі, розповсюдження та споживання інформації в різних галузях діяльності (наприклад, політичної, економічної, військової, ліцензійної).

М. Т. Гаврильців зазначає, що загалом політика інформаційної безпеки як суспільне явище має комплексний характер, включаючи внутрішньо та зовнішньополітичні, економічні, технологічні, військові та інші елементи, тому вимагає комплексного підходу. Діяльність органів державної влади повинна спрямовуватися на виконання конкретних завдань у цій сфері й об'єднуватися єдиною метою – надання належних умов для реалізації забезпечення інформаційної безпеки України [1, с. 203].

Державна інформаційна політика України реалізується за допомогою формування державними органами влади необхідних правових, економічних, організаційних та інших умов, що сприяють охороні та захисту інформаційної інфраструктури, а особливо критичної інформаційної інфраструктури [2].

Під критичною інформаційною інфраструктурою розуміються об'єкти припинення роботи яких призведе до значних наслідків і втрат для функціонування держави, наприклад, втрата управління державою і економікою, незворотні зміни в державному управлінні, загрози національній безпеці.

У даний час в Україні тільки почалася розробка нормативно-методичних документів, що регламентують забезпечення безпеки критичної інформаційної інфраструктури, в тому числі в галузі забезпечення інформаційної безпеки критичної інформаційної інфраструктури, що передбачено статтею 6 закону України «Про основні засади забезпечення кібербезпеки України» [3].

Незважаючи на те, що критична інформаційна інфраструктура не часто піддається атакам, варто відзначити, що порушення функціонування критичної інформаційної інфраструктури може спричинити серйозні наслідки, наприклад, видалення файлів з системи, яка відповідальна за моніторинг і подачу води чи електрики на гідротехнічній споруді, або збій в роботі комп'ютерної мережі управління в аеропорту.

З огляду на уповільнених процесів інформатизації в Україні і застарілого вітчизняного програмного забезпечення, засобів інформатизації, засобів захисту безпеки органи влади, організації та підприємства при розробці і функціонуванні систем захисту інформації використовують обладнання і програмне забезпечення іноземного виробництва, не завжди при цьому організовуючи для таких технічних засобів спеціальні перевірки і атестацію технічних засобів обробки інформації, автоматизованих робочих місць, що збільшує ризики несанкціонованого доступу до оброблюваної інформації.

Стратегія національної безпеки України передбачає завершення створення національної системи кібербезпеки, сформує сучасні спроможності суб'єктів забезпечення кібербезпеки і кібероборони та зміцнить систему їх координації [4].

Література:

1. Гаврильців М. Т. Інформаційна безпека держави в системі національної безпеки України. Юридичний науковий електронний журнал. 2020. № 2. С. 200-203.
2. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури : Постанова Кабінету Міністрів України від19.06.2019 р. № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text
3. Про правові засади забезпечення кібербезпеки України, 5 жовтня 2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
4. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» : Указ Президента України від 14.09.2020 р. № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text

Корнейко О. В.,
завідувач кафедри інформаційних технологій та кібербезпеки Національної академії внутрішніх справ, кандидат технічних наук, професор

Школьніков В. І.,
старший викладач кафедри інформаційних технологій та кібербезпеки Національної академії внутрішніх справ

ПІДГОТОВКА НОВОЇ ГЕНЕРАЦІЇ «ЦИФРОВИХ ОПЕРАТИВНИКІВ» В НАЦІОНАЛЬНІЙ АКАДЕМІЇ ВНУТРІШНІХ СПРАВ

На даний час вивчення та розвиток новітніх технологій та методик здійснення кримінального аналізу (КА), інформаційно-пошукової та аналітичної роботи є одним із важливих напрямів освітньої та наукової діяльності Національної академії внутрішніх справ (НАВС) при підготовці, перепідготовці та підвищенні кваліфікації оперативних працівників НП України.

Вперше планова підготовка в НАВС оперативників, які опановували кримінальний аналіз (КА) розпочалась у 2017 році на базі кафедри фінансової безпеки та фінансових розслідувань, де вивчалась теоретичні основи та загальна методологія ведення КА, особливості здійснення оперативного, тактичного та стратегічного аналізу при розслідуванні кримінальних правопорушень. І сьогодні кафедра продовжує надавати такі знання всім здобувачам вищої освіти, що навчаються в НАВС і здобувають освітній рівень бакалавра та магістра.

Починаючи з 2018 року, з метою надання здобувачам вищої освіти НАВС практичних навичок застосування сучасних інформаційних технологій (ІТ) та програмних засобів при здійснення інформаційно-пошукової та аналітичної роботи, до підготовки фахівців у сфері КА приєдналась і кафедра інформаційних технологій та кібербезпеки НАВС. Для цього кафедрою були розгорнути сучасні комп'ютерні класи, розроблені нові авторські курси та методики у сфері технологій КА, в тому числі для ведення оперативно-розшукової діяльності (ОРД) в кіберпросторі.

У 2018-2019 та 2019-2020 навчальних роках на кафедрі проводилась планова підготовка курсантів, які навчались в НАВС для комплектування органів досудового розслідування НП України, з розширенням їх фахових компетенцій у сфері інформаційно-аналітичної підтримки слідчої діяльності. А починаючи з 2020-2021 навчального року підготовка фахівців у сфері сучасних технологій КА здійснюється на кафедрі вже для здобувачів НАВС, які навчаються для подальшого комплектування підрозділів кримінальної поліції.

Під час навчання на кафедрі інформаційних технологій та кібербезпеки НАВС, разом з опануванням традиційних дисциплін для майбутніх працівників аналітичних та оперативних підрозділів поліції, курсанти навчаються:

- особливостям організації та здійснення оперативно-розшукової, інформаційно-пошукової та аналітичної роботи в підрозділах кримінальної поліції за допомогою технологій ILP (англ. Intelligence Led Policing, поліцейська діяльність керована аналітикою) та OSINT (англ. – Open Source INTelligence, розвідка на основі відкритих джерел інформації);
- застосовувати при здійсненні ОРД спеціалізовані програмні засоби та сервіси для пошуку та аналізу за допомогою технологій OSINT оперативної інформації про фізичних та юридичних осіб, необхідні документи та зображення в поверхневій (Surface Web), глибинній (Deep Web) та темній (Dark Web) частинах мережі Інтернет, в соціальних мережах, в державних реєстрах та інформаційних системах, в системах електронного банкінгу тощо;
- здійснювати заходи із забезпечення анонімної ОРД в мережі Інтернет;
- використовувати технологію ILP та основні функції програмних засобів Microsoft Word, Excel, Power BI та IBM i2 Analyst's Notebook для обробки та кримінального аналізу здобутої оперативної інформації;
- застосовувати програмний засіб Belkasoft як інструментарій для збирання, обробки та аналізу електронних (цифрових) доказів з мережі Інтернет, персональних комп'ютерів, мобільних пристроїв тощо;
- використовувати основні функції програмного продукту ArcGIS для геоінформаційного відображення оперативної інформації на електронних картах місцевості;

- здійснювати візуалізацію великих об'ємів здобутої та проаналізованої оперативної інформації та інші заходи щодо інформаційно-аналітичної роботи тощо.

Для забезпечення цієї освітньої діяльності в НАВС є відповідна сучасна матеріально-технічна база. Так, академія зареєстрована на відповідних освітніх порталах (Octopus Cybercrime Community, «SPACE» – The Secure Platform for Accredited Cybercrime Experts) та приймає участь в навчальних програмах (Microsoft Office for Education, Gsuit for Education, IBM Academic Initiative), які дозволяють отримувати ліцензоване програмне забезпечення та проводити освітній процес на високому методологічному рівні.

Для підтримки цієї освітньої діяльності кафедри на підставі рішення Вченої ради НАВС від 07.07.2020 та за підтримки керівництва Департаменту кримінального аналізу НП України в НАВС як самостійний структурний підрозділ був створений відповідний Центр кримінальної аналітики. Основними завданнями цього Центру є здійснення науково-освітньої діяльності у сфері кримінального аналізу, впровадження разом з кафедрою новітніх ІТ в практичну діяльність НП України, підтримання курсантської молоді НАВС в задоволенні їхніх наукових інтересів у сфері КА та кіберрозвідки.

Хоча Центр тільки розпочав свою діяльність, але за час свого функціонування його співробітниками разом з науково-педагогічними працівниками кафедри інформаційних технологій та кібербезпеки:

- було проведено на платформі Google Classroom онлайн тренінги «MS Excel у кримінальному аналізі» та «Аналітичні програмні продукти в кримінальному аналізі (Microsoft Excel, IBM i2 Analyst's Notebook, Power BI, ArcGIS)» для співробітників підрозділів кримінального аналізу, внутрішньої безпеки, кіберполіції, карного розшуку, оперативно-технічних заходів, оперативної служби, протидії наркозлочинності та боротьби зі злочинами, пов'язаними з торгівлею людьми НП України;
- були організовані та проведені курси підвищення кваліфікації для працівників практичних підрозділів кримінального аналізу НП України, де розглядались новітні методики та технології здійснення КА із застосуванням сучасного програмного забезпечення;
- підготовлено ряд практичних посібників, що детально розкривають специфічні методики та технології проведення КА, серед яких, наприклад, такі: «Кластерний аналіз інформації про телефонний трафік»; «Обробка та аналіз за допомогою MS Excel та IBM i2 Analyst's Notebook інформації щодо одночасного перетину кордону декількома особами»; «Обробка та аналіз інформації з Державного реєстру нерухомого майна Міністерства юстиції України»; «Обробка та аналіз інформації з інформаційно-аналітичного комплексу "Безпечне місто"»; «Встановлення місцезнаходження та маршруту руху особи чи транспортного засобу за допомогою геоінформаційного програмного продукту ArcGIS»;
- здійснюється науково-аналітичне опрацювання результатів проведеного онлайн курсу з кібергігієни для працівників апарату МВС України (у межах спільного проєкту Консультативної місії Європейського Союзу й української компанії з кібербезпеки ISSP), а також підготовка відповідних методичних рекомендацій тощо.

Таким чином, можна стверджувати, що стрімкий розвиток сучасних інформаційно-аналітичних технологій зумовлює переосмислення змісту поліцейської діяльності, а теоретичні та практичні наробки науковців та викладачів НАВС у сфері кримінальної аналітики дозволяють підготувати нову генерацію працівників поліції, що здатні виконувати складні інформаційно-аналітичні завдання задля ефективного попередження, розслідування, розкриття та прогнозування кримінальних правопорушень.

Кулешник Я. Ф.,
доцент кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів Львівського державного університету внутрішніх справ, кандидат технічних наук, доцент

Сорокач О.В.,
начальник відділу режимно-секретного та документального забезпечення Львівського державного університету внутрішніх справ

КВАНТОВІ КОМП'ЮТЕРИ ТА КУБІТИ

Квантовий комп'ютер (КК) – це обчислювальний пристрій, який використовує явища квантової механіки для передачі й обробки даних, на який багато дослідників покладають великі надії, чекаючи, що він позитивно вплине на розвиток науки. Ідея квантових обчислень була незалежно запропонована Юрієм Маніним і Річардом Фейнманом на початку 80-х років минулого століття. З тих пір була пророблена колосальна робота з їх створення. Однак повноцінний універсальний квантовий комп'ютер усе ще є гіпотетичним пристроєм, можливість розробки якого пов'язана з серйозним розвитком квантової теорії. До теперішнього моменту були створені поодинокі експериментальні системи з алгоритмом невеликої складності.

Якщо наші класичні комп'ютери (такі як ПК, ноутбуки та смартфони) – це свічки, то квантові комп'ютери – це лампочки. Призначення обох однакове – для ламп розжарювання та свічок це випромінювання світла, а для комп'ютерів – проведення розрахунків. Однак в обох випадках мета досягається зовсім інакша і результат інший. Простими словами, квантовий комп'ютер – це не просто вдосконалена версія сучасних комп'ютерів, як і лампочка – це не просто більш велика свічка. Ви не можете створити лампочку, роблячи свічки все кращими і кращими. Лампочка – це інша технологія, заснована на більш глибокому науковому розумінні. Так само квантовий комп'ютер – це новий тип пристроїв, заснований на квантовій фізиці, і так само, як лампочка змінила суспільство, квантові комп'ютери можуть впливати на багато аспектів нашого життя, включаючи потреби в безпеці, охорону здоров'я та навіть Інтернет.

Ми знаємо деякі теоретичні основи роботи квантових комп'ютерів, але на їх розвитку існують величезні перешкоди, які ще чекають на своє вирішення. Найбільшою перешкодою у використанні квантових обчислень є велика кількість помилок, на які впливають навіть найменші зміни в середовищі квантових машин.

Дослідницькі центри та компанії з усього світу проводять подальші випробування та дослідження і фахівці у галузі квантової фізики сходяться на думці, що від створення повноцінно функціонуючих квантових машин, які ми зможемо використовувати для досягнення цілей, яких на даному етапі неможливо досягти, пройдуть, очевидно, десятки років.

Основна відмінність квантового комп'ютера від класичного полягає в поданні інформації. Відомо, що у класичних комп'ютерах, що працюють на основі транзисторів і кремнієвих чіпів, для обробки інформації використовується бінарний код. Біт, як відомо, має два базових стани – нуль та одиницю, і може перебувати тільки в одному з них для представлення символів (послідовність нулів та одиниць) та проведення обчислень. Така інформація сприймається та правильно інтерпретується сучасними телефонами, смарт-телевізорами та іншими застосуваннями. Наскільки неефективною є ця система, видно, коли ми доходимо до її фізичної межі. Уже зараз, зважаючи на швидкий розвиток інформаційних технологій, нам починає не вистарчати об'ємів пам'яті та швидкодії найсучасніших комп'ютерів. Інакше ми давно вже би вирішили питання онко захворювань чи будь-якої пандемії.

Якщо прийняти, що термін "квант" використовується для опису найменшої частинки будь-чого, то для опису квантового біта можна використати термін кубіт, тобто найменша і неподільна одиниця квантової інформації за допомогою якої будуть представлятись символи та проводитись обчислення у квантових комп'ютерах.

Хоч електрон ще давніми греками прийнято вважати точковим тілом, крім обертання навколо ядра він має ще одну властивість – обертання навколо своєї уявної осі (спін). Частині електронів приписують обертання за годинниковою стрілкою, а частині - проти. Умовно це позначають стрілками з протилежними напрямами ↑ **-** відповідає значенню одиниця та ↓ **-** відповідає значенню нуль **.**

Що ж стосується квантового комп'ютера, то його робота ґрунтується на принципі суперпозиції. У кубіта також є два основні стани: нуль та одиниця. Однак завдяки суперпозиції кубіт може приймати значення, отримані шляхом їх комбінування, і перебувати у всіх цих станах одночасно. Кубіт може приймати будь-яке значення від 0 до 1. Він має властивості всього спектра і може мати значення, наприклад, на 10 відсотків значення нуль і на 90 відсотків значення один. Теоретично це дозволяє зберегти набагато більше інформації, або пришвидшити обчислення.

У цьому полягає паралельність квантових обчислень, тобто відсутність необхідності перебирати всі можливі варіанти станів системи. Крім того, для опису точного стану системи квантовому комп'ютера не потрібні величезні обчислювальні потужності й обсяги оперативної пам'яті, оскільки для розрахунку системи з 100 частинок досить лише 100 кубітів, а не трильйон трильйонів біт. Відомо, що для перенесення одного біта інформації традиційними електричними кабелями використовується 1000000 електронів. При використанні кубітів (де кожен електрон завдяки спін-орбіталі може приймати значення 0-спін вниз, або 1 – спін вверх) об'єми обробленої інформації зростають у мільйони разів. Так, наприклад, слово "gubit", запис якого у двійковій системі числення буде: 1110001 1110101 11000010 1101001 1110100, при використанні процесора з тактовою частотою 3,3 МГц буде вимагати для використання $35*10^6$ електронів, а у квантовому комп'ютері – тільки 35 електронів.

При будь-якій зміні кубіта він змінює свій стан випадковим чином, а за рахунок наявності зв'язку між кубітами паралельно свій стан змінюють і пов'язані кубіти. Набір пов'язаних кубітів прийнято називати квантовим регістром, який за рахунок можливої безлічі комбінацій (суперпозицій) кубітів, що входять до нього, значно інформативніший від класичного бітового регістра, який займає 32 або 64 біти пам'яті. Безпосередньо спостерігати за станом кубіта або квантового регістра можна. У той же час кубіти можуть обмінюватися своїм станом і перетворювати його, що, власне, і дозволяє створити комп'ютер, який реалізує паралельні обчислення на фізичному рівні. Але при цьому також виникає маса проблем, які важко контролювати і навіть зрозуміти.

Ще однією особливістю квантових комп'ютерів, яка дозволяє додатково масштабувати обчислювальний приріст потужності, є використання квантового переплутування. Це стан, коли два кубіти з'єднані між собою, і кожного разу, коли ми спостерігаємо один з них, інший буде знаходитися у точно такому ж стані. Заплутаність дозволяє згрупувати кубіти в ще більш ефективні одиниці для запису та обробки інформації.

Квантове обладнання.

Квантовий комп'ютер складається з трьох основних частин: області для зберігання кубітів, методу передачі сигналів кубітам та класичного комп'ютера для запуску програми та надсилання інструкцій.

Квантовий матеріал, який утворює кубіти, є делікатним і надзвичайно чутливим до впливів навколишнього середовища. Для деяких методів зберігання кубітів одиниця, яка вміщує кубіти, тримається при температурі, близькій до абсолютного нуля, щоб максимізувати їх узгодженість. Інші типи кубітових сховищ використовують вакуумну камеру для мінімізації вібрації та стабілізації кубітів. Існують різні методи передачі сигналів кубітам, наприклад мікрохвилі, лазер та електрична напруга.

Щоб налагодити нормальну роботу квантових комп'ютерів, потрібно вирішити багато проблем. Суттєвою проблемою квантових комп'ютерів є виправлення помилок, а масштабування (додавання більшої кількості кубітів) ще більше збільшує частоту їх появи. Через ці обмеження квантовий персональний комп'ютер на нашому столі все ще є картиною з далекого майбутнього, але комерційні квантові комп'ютери можуть стати доступними вже найближчим часом.

Як працює квантовий комп'ютер?

Квантовий комп'ютер (КК) – це обчислювальний пристрій, який використовує явища квантової механіки для передачі й обробки даних. Ідея квантових обчислень була незалежно запропонована Юрієм Маніним і Річардом Фейнманом на початку 80-х років минулого століття. З тих пір була пророблена колосальна робота з їх створення. Однак повноцінний універсальний квантовий комп'ютер усе ще є гіпотетичним пристроєм, можливість розробки якого пов'язана з серйозним розвитком квантової теорії. До теперішнього моменту були створені поодинокі експериментальні системи з алгоритмом невеликої складності.

Звичайним чином (в життєвому розумінні) квантові частинки поводяться так як нам треба, тільки під нашим контролем, якщо ми не контролюємо їх, квантові частинки тут же переходять з певного стану відразу в кілька різних іпостасей. Тобто електрон (або будь-який інший квантовий об'єкт) частково буде

знаходитися в одній точці, частково в іншій, частково в третій і т. д. Такий стан електрона, коли він знаходиться відразу в декількох точках простору, називають суперпозицією квантових станів і описують зазвичай хвильовою функцією, введеною в 1926 році німецьким фізиком Е. Шредінгером.

Квантова суперпозиція говорить нам про те, що система з якоюсь ймовірністю є у всіх можливих для неї станах (при цьому сума всіх ймовірностей, зрозуміло, дорівнює 100% або 1).

Також варто відзначити, що зміна стану певного кубіта у квантовому комп'ютері веде до зміни стану інших часток, що є ще однією відмінністю від звичайного комп'ютера. І цією зміною можна керувати. Процес роботи КК був запропонований британським фізиком-теоретиком Девідом Дойчем у 1995 році, коли він створив ланцюжок, здатний виконувати будь-які обчислення на квантовому рівні. Згідно з його схемою, для початку береться набір кубітів і записуються їх основні параметри. Потім виконуються необхідні перетворення з використанням логічних операцій і записується отримане значення, яке і є результатом, що видаються комп'ютером. У ролі проводів виступають кубіти, а перетворення роблять логічні блоки.

Спрощено схему обчислень на квантовому комп'ютері можна представити таким чином. У якусь систему кубітів записується початковий стан, а потім над нею відбуваються унітарні перетворення, що виконують функцію потрібних нам логічних операцій. Таким чином, у квантових алгоритмах і описується послідовність унітарних операцій (названих гейтами або вентилями) із зазначенням – над якими саме кубітами їх треба здійснювати. Результатом роботи квантового алгоритму є підсумковий стан системи кубітів.

Результат роботи квантового комп'ютера.

Результат роботи квантового комп'ютера буде носити імовірнісний характер. Але, незалежно від реалізованого алгоритму, використання технологій квантових обчислень дозволяє ефективно вирішувати завдання, що вимагають серйозної обчислювальної потужності. Наприклад, квантовому комп'ютеру може виявитися під силу розшифрувати повідомлення, які захищені асиметричним криптографічним алгоритмом RSA (криптографічний алгоритм з відкритим ключем, що базується на обчислювальній складності задачі факторизації великих цілих чисел). Іншим можливим застосуванням КК можуть стати задачі моделювання фізичних процесів або обробка дуже великих обсягів даних.

Література:

1. Вакарчук І. О. Квантова механіка. – 4-е видання, доповнене. – Л. : ЛНУ ім. Івана Франка, 2012. – 872 с.
2. Ю. Світлик Квантові комп'ютери: що це, як працюють, які перспективи (https://root-nation.com/ua/author/yurisweetlik/).
3. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация = Quantum Computation and Quantum Information. – М. : Мир, 2006. – 824 с.

Кулешник Т. Я.,
завідуючий ІОЦ, викладач кафедри менеджменту Національної академії мистецтв

Кулешник О. І.,
старший викладач кафедри менеджменту Національної академії мистецтв

ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ВИКОРИСТАННЯ КВАНТОВИХ КОМП'ЮТЕРІВ

Для чого ми будемо використовувати квантові комп'ютери?

Сьогодні постає питання для чого можна використовувати квантові комп'ютери, подібно до того, як 20 років тому, для чого можна використовувати смартфон. Звичайно, вже є деякі плани та припущення, але найцікавіші напрямки для використання кубітів, мабуть, стануть зрозумілими, коли квантові комп'ютери набудуть широкого поширення.

Криптографія – це одна з найпопулярніших сфер, де найчастіше передбачають використання квантових обчислень. Річ у тім, що це буде метод передачі інформації дуже захищеним способом, і безпека базується не на складності обчислювальних процесів, а на законах фізики, що дасть упевненість в тому, що певні речі просто неможливі. І в цей момент неможливо буде прослуховувати, підглядати, зламувати.

Безпека в цьому випадку гарантується самими фізичними властивостями кубітів (найменша і неподільна одиниця квантової інформації за допомогою якої будуть представлятись символи та проводитись обчислення у квантових комп'ютерах), які перестають виявляти особливості суперпозиції, як тільки за ними починають «спостерігати». Тож будь-яка спроба перехопити або навіть скопіювати закодоване повідомлення просто знищить його.

Квантові комп'ютери також можуть дозволити нам краще зрозуміти природні процеси. "Хаос" суперпозиції набагато краще відображає спосіб, наприклад, мутацій в ДНК, а отже, розвиток хвороб та еволюцію. Квантові обчислення вже сьогодні використовуються для створення нових препаратів.

Можливо, є сенс говорити про використання квантових комп'ютерів для телепортації даних. Так, саме телепортації даних, а можливо і людини. Ми зможемо телепортувати інформацію з місця на місце, не передаючи її фізично. Це звучить як фантастика, хоча це можливо, оскільки ця плинність квантових частинок може заплутатися у часі та просторі, так що зміна однієї частинки може вплинути на іншу, і це створює канал для телепортації. Це вже було продемонстровано в лабораторіях, і це може бути частиною квантового Інтернету майбутнього. У нас такої мережі ще немає, але деякі вчені вже працюють над цими можливостями, моделюючи квантову мережу на квантовому комп'ютері. Вони вже розробили та впровадили нові цікаві протоколи, такі як телепортація між користувачами мережі та ефективна передача даних, і навіть безпечне голосування на виборах.

Також слід сказати, що квантові комп'ютери повинні використовуватися для моделювання різних ситуацій та пошуку рішень проблем, включаючи медикаменти і вакцини. Наприклад, під час пандемій, подібних коронавірусу, коли потрібне більш швидке обчислення і розрахунок варіантів. От тут можна задіяти можливість квантового моделювання, яке неможливо виконати на класичному комп'ютері. Коли виникає нове захворювання, процес пошуку ліків займає близько 15 років і може коштувати до 2,6 млрд доларів. При деяких захворюваннях необхідно фільтрувати мільйони молекул, щоб виявити лише сотні перспективних людей, які, ймовірно, можуть стати донорами. Потім під час випробувань приблизно 99% молекул відпадає через, серед іншого, неправильне передбачення поведінки та обмеження вибірки. Саме тут на перший план вийшли б квантові комп'ютери.

І це все ще лише деякі з чудових ідей щодо того, чого можна досягти, використовуючи квантову фізику. Наразі нам у деякій мірі вдається приборкати її примхливий характер, але всі розробки поки що на початковому рівні. До створення справжнього квантового комп'ютера і його масового застосування ще досить далеко, та прогрес не стоїть на місці. Тому, можливо, вже через якісь десять років ви читатимете цю статтю за допомогою квантового комп'ютера і будете поблажливо посміхатися.

Проблеми використання квантових комп'ютерів.

Втім, у квантових комп'ютерів є й системні недоліки, навіть якщо не брати до уваги складність фізичної реалізації. Результат квантових обчислень носить імовірнісний характер.

Однак у квантових комп'ютерів є одна величезна проблема. Тобто, вчені мають величезну проблему з їх використанням, оскільки, завдяки своїм особливим властивостям, кубіти потребують

достатньо спокійного середовища, щоб було можливо точно зчитувати будь-які дані з них. Кожне, навіть найменше порушення зробить неможливим точне зчитування інформації.

У випадку з класичними комп'ютерами подібна проблема також відігравала важливу роль у минулому, але сьогодні вона настільки незначна, що її часто не помічають навіть в академічній науці. Ми говоримо про частоту помилок. Вона є покажчиком, що визначає, яка частка бітів або кубітів інформації може бути пошкоджена. Це може статися, наприклад, у момент перенапруги або інших порушень.

Для класичних пристроїв ймовірність помилки становить приблизно один до 10^{17} біт. У випадку з квантовими комп'ютерами це все ще одна з кількох сотень. І це в ситуації, коли квантові комп'ютери працюють у максимально ізольованих умовах і при температурі -272 градуси Цельсія, тобто трохи вище абсолютного нуля. Будь-які коливання температури, зміна електромагнітного поля і навіть рух руйнують весь розрахунок.

Інша проблема – "нестабільність" квантових станів. Кожного разу, коли ми вимірюємо квантовий стан або хочемо його порушити, він повертається в одне з двох положень нуль-один. У такому випадку квантовий стан розпадеться. Цей процес називається квантовою декогеренцією.

Однак усі ці складнощі не лякають не тільки вчених, але й комерційні компанії, які все активніше цікавляться темою КК.

Перші спроби створення квантового комп'ютера.

Звичайно, реалізація повноцінного квантового комп'ютера вважається одним з фундаментальних завдань фізики XXI століття, але певні позитивні зрушення в цьому питанні вже є. У 1998 році вчені з Массачусетського технологічного інституту змогли розділити один кубіт між трьома ядерними спінами в кожній молекулі рідкого аланіну або молекули трихлороетілену (нагадаю, у квантових комп'ютерах носіями інформації можуть бути атоми, іони, фотони або електрони). У березні 2000 року вчені з Національної лабораторії у Лос Аламосі оголосили про успішне створення квантового комп'ютера з 7 кубітами. Роком пізніше, у 2001, фахівці IBM продемонстрували обчислення алгоритму Шора на 7-кубітному комп'ютері.

Запам'ятався 2005 рік досягненням – вченим з інституту квантової оптики та квантової інформації при Інсбрукському університеті вдалося створити кубайт (реєстр з 8 кубітів). У листопаді 2009 року фізикам з Національного інституту стандартів і технологій у США вдалося створити 2-кубітний програмований квантовий комп'ютер.

До речі, запропоноване Пашиним використання надпровідності для квантових комп'ютерів виявилося вельми перспективним. У лютому 2012 року фахівці компанії IBM заявили про серйозний прорив у справі створення кубітів на надпровідних елементах. Робоча температура подібних квантових комп'ютерів складає десятки мікрокельвін. Відповідно, йому потрібна вкрай ефективна система охолодження, що працює на спеціальній суміші ізотопів гелію-3 і гелію-4. Втім, технологічно отримання таких низьких температур відмінно опрацьоване вже зараз. У квітні 2012 групі дослідників з Південно-Каліфорнійського університету, нідерландського Технічного університету Делфта, університету штату Айова та Каліфорнійського університету Санта-Барбара, вдалося побудувати двохкубітний квантовий комп'ютер на кристалі алмаза (з домішками), який може працювати при кімнатній температурі й теоретично є масштабованим.

Розробки компанії D-Wave Systems.

На окрему увагу заслуговує компанія D-Wave Systems, яка у 2007 році продемонструвала 16-кубітний комп'ютер Orion, а в листопаді того ж року – 28-кубітний комп'ютер.

У травні 2011 року нею ж був показаний 128-кубітний комп'ютер D-Wave One, а наприкінці 2012 року – комп'ютер на 512 кубітів. При цьому D-Wave One є комерційно доступним продуктом, його ціна становить $11 млн. Втім, навіть якщо не звертати уваги на високу ціну, сфера застосування комп'ютерів D-Wave поки досить обмежена, в основному мова йде про завдання дискретної оптимізації.

Причому багато дослідників не вважають комп'ютери D-Wave справжніми квантовими обчислювальними машинами, заявляючи про зайве скромний приріст продуктивності щодо класичних систем і сумніваються в наявності в комп'ютерах D-Wave заплутаності кубітів, що є одним з фундаментальних принципів побудови квантових комп'ютерів. Втім, у січні 2014 року вчені D-Wave опублікували статтю, яка підтверджує наявність у комп'ютерах D-Wave квантової когерентності й заплутаності між окремими підгрупами кубітів (розміром 2 і 8 елементів) у процесорі під час проведення обчислень.

Основне застосування квантових обчислень – це штучний інтелект (ШІ). ШІ, заснований на принципах навчання в процесі здобуття досвіду, стає все точнішим в міру роботи зворотного зв'язку, поки, нарешті, не обзаводиться «інтелектом», нехай і комп'ютерним. Тобто самостійно навчається вирішенню завдань певного типу.

Наприклад, Lockheed Martin планує використовувати свій квантовий комп'ютер D-Wave для випробувань програмного забезпечення для автопілота, яке занадто складне для класичних комп'ютерів, а Google використовує квантовий комп'ютер для розробки ПЗ, яке зможе відрізняти автомобілі від дорожніх знаків. Ми вже досягли точки, за якою ШІ створює більше ШІ, і його сила й величина будуть тільки рости.

Інший приклад – це точне моделювання молекулярних взаємодій, пошук оптимальних конфігурацій для хімічних реакцій. Така «квантова хімія» настільки складна, що за допомогою сучасних цифрових комп'ютерів можна проаналізувати лише найпростіші молекули.

Квантові комп'ютери можуть виробляти такий факторинг експоненціально ефективніше за цифрові комп'ютери, роблячи сучасні методи захисту застарілими. Розробляються нові методи криптографії, які, втім, вимагають часу: у серпні 2015 року NSA почало збирати список стійких до квантових обчислень криптографічних методів, які могли б протистояти квантовим комп'ютерам, і у квітні 2016 Національний інститут стандартів і технологій почав публічний процес оцінки, який триватиме від чотирьох до шести років.

Хартмут Невен, директор з розробок у Google, зазначив, що квантові комп'ютери можуть також допомогти в створенні досконаліших кліматичних моделей, які могли б дати нам глибше уявлення про те, як люди впливають на навколишнє середовище. На основі цих моделей ми вибудовуємо наші уявлення про майбутнє потепління, і вони допомагають нам визначати кроки, які потрібні для запобігання стихійних лих.

Наскільки ми близькі до промислового створення КК?

Звичайно, сперечатися про істинність квантової суті комп'ютерів D-Wave можна скільки завгодно, але не можна не визнати, що інтерес до квантових комп'ютерів є як у вчених по всьому світу, так і великих корпорацій. У тому числі й у Google (команда проекту Google Quantum AI), яка збирається за допомогою квантових комп'ютерів вирішити завдання, які неможливо або недоцільно вирішувати за допомогою класичних обчислювальних пристроїв.

Гонка в самому розпалі. Провідні компанії світу намагаються створити перший квантовий комп'ютер, в основі якого лежить технологія, що давно обіцяє вченим допомогти в розробці чудових нових матеріалів, ідеальному шифруванні даних і точному прогнозуванні змін клімату Землі. Така машина напевно з'явиться не раніше ніж через десять років, але це не зупиняє IBM, Microsoft, Google, Intel та інших. Вони буквально штуками викладають квантові біти – або кубіти – на процесорному чіпі. Але шлях до квантових обчислень включає багато більше, ніж маніпуляції з субатомними частинками.

Застосування квантових комп'ютерів у мистецтві може привести до створення неймовірних і непередбачуваних шедеврів, нових напрямків у музиці, живописі та інших видах образотворчого мистецтва, але при цьому, звичайно, найважливішою буде залишатися обдарованість та талант особистості.

Зараз ця сфера активно розвивається, хоча поки й не має практичного застосування. Але через цю стадію пройшли багато технологій, які стали невід'ємною частиною нашого життя. Тим більше, що вчені дивляться в майбутнє з великим оптимізмом.

Література:

1. Вакарчук І. О. Квантова механіка. – 4-е видання, доповнене. – Л. : ЛНУ ім. Івана Франка, 2012. – 872 с.
2. Ю. Світлик. Квантові комп'ютери: що це, як працюють, які перспективи (https://root-nation.com/ua/author/yurisweetlik/).
3. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация = Quantum Computation and Quantum Information. – М. : Мир, 2006. – 824 с.
4. https://techno.nv.ua/ukr

Кулешник Я. Ф.,
доцент кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів Львівського державного університету внутрішніх справ, кандидат технічних наук, доцент

Дробіняк Х.Т.,
здобувач вищої освіти Львівського державного університету внутрішніх справ

КВАНТОВА ПЕРЕВАГА ТА КВАНТОВІ ШУМИ

Що таке квантова перевага? Очікування дива, передчуття швидкого прориву, який змінить все, змушує великі компанії вкладати величезні кошти в квантові комп'ютери.

Це чудо, якого всі чекають, називається квантовою перевагою. І коли (і якщо) воно дійсно трапиться, і квантові комп'ютери перевершать за продуктивністю звичайні обчислювальні системи, в навколишньому світі зміниться так багато всього, що навіть саме людство може перестати існувати.

Якщо говорити простою мовою, квантова перевага – це якийсь момент в майбутньому, коли квантові комп'ютери в усьому перевершать звичайні комп'ютери. Цей термін придумав в 2011 році фізик-теоретик Джон Прескіллу з Каліфорнійського технологічного інституту.

Наприклад, вони будуть здатні виконувати звичайні обчислювальні завдання швидше і ефективніше. І при цьому не будуть являти собою гігантські конструкції вартістю в мільярди доларів.

Зрозуміло, що суперкомп'ютери, котрі займають цілі будівлі, завжди будуть затребувані для вирішення найважливіших наукових завдань. Але квантові комп'ютери тільки тоді по справжньому змінять "все", коли будуть представляти собою такі ж ноутбуки та планшети, як і сучасні класичні обчислювальні пристрої і, зрозуміло, основним виграшем для всіх з моменту настання квантової переваги стануть безмежні можливості квантових обчислень.

У 2001 році три американських фізики отримали Нобелівську премію за відкриття конденсату Бозе-Ейнштейна – по суті, це п'ятий стан матерії після твердого, рідкого, газоподібного і плазми.

За температури близької до абсолютного нуля рух атомів сповільнюється настільки, що їхня кінетична енергія стає рівною їхній видимій енергії. У цьому стані стає можливим один із феноменів квантової фізики – квантова заплутаність. Атоми стають пов'язаними і перестають існувати як індивідуальні одиниці. Саме таким чином вдалося створити перші квантові комп'ютери, здатні здійснювати обчислення.

Таким ось чином, наприклад, був створений 72-кубітний квантовий комп'ютер Bristlecone від Google. Іншими словами, квантовий комп'ютер здійснює якісь обчислення, перевірити правильність яких ми просто не можемо.

В Google збираються провести експеримент, який полягатиме в наступному. Квантовому комп'ютеру поставлять завдання, яке під силу існуючим суперкомп'ютерам, але знаходиться на межі їхніх можливостей. Це дасть можливість з одного боку показати, наскільки квантові комп'ютери швидші, з іншого боку, можливість перевірити їхні обчислення на супер комп'ютері все ж збережеться.

Але все ж головною проблемою, пов'язаною з квантовими комп'ютерами, залишається не перевірка правильності обчислень, а квантовий шум.

Що таке квантовий шум? Джон Прескілл, автор терміну "квантова перевага", опублікував роботу, в якій пророкує, що головною проблемою квантових комп'ютерів стане загальна крихкість системи. Шум не є великою проблемою для сучасних комп'ютерів, оскільки їхні зв’язки можна зробити досить жорсткими для того, щоб протистояти зовнішньому впливу, відводячи його в формі тепла. Але квантові стани відрізняються надзвичайною крихкістю і можуть бути зруйновані шумом, тобто зовнішнім впливом.

Сама по собі суперпозиція – стан одночасного нуля і одиниці – триває наносекунди. І порушити цей стан дуже легко. Один дослідник навіть якось порівняв підтримку суперпозиції зі спробою поставити яйце на кінчик голки.

Якщо є такі перешкоди, можливо ніякого квантового переваги бути не може, а про квантові комп'ютери варто забути уже хоча б тому, що новий квантовий комп'ютер поки ще не довів свою спроможність, та й незрозуміло, які його експлуатаційні характеристики.

Вчені бачать відразу кілька потенційних рішень проблеми шуму. Серед них і тимчасові кристали (хоча ніхто до кінця не розуміє, що це таке) і, власне, конденсат Бозе-Ейнштейна і низка інших рішень. Однак, квантова перевага рано чи пізно станеться.

Якщо квантові комп'ютери настільки складні і дорогі, то чи не простіше обійтися без них?

Є ціла низка обчислювальних задач, з якими традиційні комп'ютери не здатні впоратися. Це розшифровка генів, рішення загадок Всесвіту, функціонування штучного інтелекту і врешті-решт повноцінна віртуальна реальність та телепортація. Квантова перевага стане революцією не тільки тому, що комп'ютери самі по собі будуть більш досконалими, а тому що перед людством відкриються деякі перспективи, про які не могли мріяти навіть найсміливіші фантасти.

Чого чекати звичайним людям? Можливо ви проживете років на двадцять довше, ніж ваші батьки завдяки медичним препаратам, які стануть можливими завдяки секвенуванню ДНК (метод визначення первинної структури нерозгалужених біополімерів) за допомогою квантових комп'ютерів.

Агентство національної безпеки США вже працює над своїм квантовим комп'ютером, який потрібен для злому існуючих систем комп'ютерного шифрування.

Уявіть собі ступінь ризику у сфері криптографії. Ваші банківські транзакції захищені кодом, який вважається безпечним тому, що звичайні комп'ютери будуть ламати його тисячі років. А тепер уявіть собі квантовий комп'ютер, який може розкрити цей код за хвилину.

Логічно припустити, що в епоху квантових комп'ютерів і криптографія стане квантовою, що дозволить забезпечити належний рівень захисту. Але що якщо технологія буде з'являтися не рівномірно по всьому світу, і спочатку буде доступна не всім.

Згадайте про шкільного вчителя однієї з африканських країн, який на уроках малював інтерфейс комп'ютера на дошці, тому що в школі просто немає комп'ютера. Що якщо настане момент, коли квантові комп'ютери вже будуть у деяких зловмисників, але ще не з'являться у звичайних людей?

Знову таки, багато експертів пророкують, що поява квантових комп'ютерів може внести хаос в існуючий фінансовий світ. Квантові комп'ютери зможуть передбачати коливання біржових курсів і курсів валют. Той, хто першим почне їх використовувати в цій сфері, багато заробить і може просто обрушити цілі ринки.

Блокчейн (книга обліку всіх операцій), який тільки-тільки завоював довіру у всьому світі і став базовою технологією для багатьох відповідальних операцій, теж опиниться під загрозою. Квантові комп'ютери зможуть зламувати ключі, якими захищені ланцюжки даних. Про яку конфіденційість тут може йтися? Ну а разом з блокчейном настане кінець і криптовалют. Хоча на їхнє місце найімовірніше прийдуть квантові валюти, але це вже буде зовсім інша історія.

І нарешті, ігри і віртуальна реальність. Потужність і швидкість обчислення, на які (теоретично) здатні квантові комп'ютери, в корені змінять ці індустрії.

Можливо, через 20 років можна буде подорожувати поверхнею Марса або спускатися на дно Маріанської западини, не виходячи з власного будинку і не ризикуючи скрутити собі шию саме завдяки квантовим комп'ютерам.

Чому ж ми не використовуємо ці комп’ютери? Проблема банальна – неможливість реалізувати квантову систему в звичайних домашніх умовах. Для того, щоб кубіт міг існувати в стані суперпозиції нескінченно довго, потрібні вкрай специфічні умови: це повний вакуум (відсутність інших частинок), температура, максимально близька до нуля за Кельвіном (для надпровідності), і повна відсутність електромагнітного випромінювання (для відсутності впливу на квантову систему). Погодьтеся, створити такі умови вдома м’яко кажучи важкувато, але ж найменше відхилення призведе до того, що стан суперпозиції зникне, і результати обчислень будуть невірними. Друга проблема – це змусити кубіти взаємодіяти один з одним – при взаємодії їх час життя катастрофічно зменшується. У підсумку самий максимум на даний день – це квантові комп’ютери з кількома десятками кубітів

Однак, є квантові комп’ютери від D-Wave, які мають 1000 кубітів, але, взагалі кажучи, справжніми квантовими комп’ютерами вони не є, бо не використовують принципи квантової заплутаності (тобто вони не взаємозв’язані). Тому вони не можуть працювати за класичними квантовим алгоритмами.

Але все ж такі пристрої виявляються відчутно (в сотні тисяч разів) могутніші звичайних ПК, що можна вважати проривом.

Література:

1. Ю. Світлик Квантові комп’ютери: що це, як працюють, які перспективи (https://root-nation.com/ua/author/yurisweetlik/).

Лукащук Ю. А.,
аспірант кафедри автоматизованих систем управління Національного університету «Львівська політехніка»

РОЗРАХУНОК ВАГОВИХ КОЕФІЦІЄНТІВ ДЛЯ КРИПТОГРАФІЧНОГО ЗАХИСТУ ПІД ЧАС ПЕРЕДАЧІ ДАНИХ У РЕАЛЬНОМУ ЧАСІ

Швидкий розвиток засобів обчислювальної та телекомунікаційної техніки і зв'язку дозволив збирати, акумулювати, обробляти та оперативно передавати інформацію у величезних обсягах. Завдяки інноваційним інформаційним технологіям діяльність людини, її повсякденна сфера спілкування розширюються за рахунок залучення досвіду та знань, вироблених світовою цивілізацією, і сама економіка в контексті глобалізаційних процесів все менше характеризується як виробництво матеріальних благ і все більше – як поширення інформаційного продукту (товарів та послуг).

Власне швидким розвитком інформаційних технологій і зумовлена актуальність вивчення проблем інформаційної безпеки: загроз для інформаційних ресурсів, різноманітних засобів та заходів захисту, бар'єрів для проникнення, а також уразливостей у системах захисту у т.ч. і військової та енергетичної галузей. Під інформаційною безпекою розуміють комплекс засобів, методів і процесів, які забезпечують захист інформаційних активів і гарантують збереження ефективності та практичної корисності технічної інфраструктури інформаційних систем і відомостей, які зберігаються і обробляються у таких системах.

Неухильно зростає різноманітність та складність проблем інформаційної безпеки, які виникають під час активного розвитку інформаційних технологій.

Існує чимало методів захисту інформації. Особливо актуальними є криптографічні методи, призначені для захисту від загроз шахрайства як інформації з обмеженим доступом, так і відкритої інформації. У всьому різноманітті проблем забезпечення інформаційної безпеки, що вирішуються за допомогою криптографічних методів та засобів, завдання забезпечення цілісності та достовірності переданої інформації є на сьогодні однією з найгостріших. З урахуванням сучасних вимог до інформаційно-телекомунікаційних систем це завдання дедалі частіше перетворюється на серйозну проблему. Особливо актуальна вона у фінансовій, військовій та енергетичній сферах, оскільки для їх надійного функціонування необхідною умовою є збереження всіх документів в цілісності та достовірності.

Криптографічний захист інформації – вид захисту, що реалізується за допомогою перетворень інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо.

Забезпечення криптографічного захисту при передачі важливої інформації, дистанційному управлінні безпілотними літальними апаратами, мобільними інтелектуальними роботами, мікросупутниками і т.п. вимагає розроблення нових методів та алгоритмів криптографічного захисту, орієнтованих на ефективну програмно-апаратну реалізацію у реальному часі з забезпеченням обмежень щодо габаритів, енергоспоживання та вартості. Одним із шляхів забезпечення таких вимог є використання автоасоціативної нейромережі прямого поширення, яка навчається на основі методу головних компонент. Особливістю таких нейромереж є можливість наперед обчислити вагові коефіцієнти та використати таблично-алгоритмічний метод для реалізації криптографічних засобів нейроподібного шифрування та дешифрування даних. Ключами при нейроподібному шифруванні та дешифруванні даних є структури нейроподібної мережі та матриці вагових коефіцієнтів. Актуальною проблемою є обчислення такої матриці для заданої архітектури нейроподібної мережі. Для цього слід розробити імітаційну модель, яка ґрунтується на вдосконаленому методі сингулярного розкладу матриці та забезпечує обчислення матриці вагових коефіцієнтів при заданих параметрах. Параметрами для розрахунку такої матриці слугують – розрядність самого повідомлення та розрядності входів. Практичною цінністю є те, що імітаційна модель забезпечує швидке обчислення коефіцієнтів для заданої архітектури нейромережі.

Для прикладу, нехай вхідне повідомлення із розрядністю – n = 16 та розрядністю входу – m = 2. Отже, вхідна матриця буде розмірністю 8x2. Опираючись на ці дані результуюча матриця вагових коефіцієнтів буде розмірністю 2x2. Далі ця матриця буде використовуватись як ключ для шифрування вхідного повідомлення. Однак, не для будь-якого. Для пакету даних, які плануються передаватись, є вимоги, а саме це те що розрядність самого повідомлення, а також розрядність входів має бути такими

ж, як при знаходженні матриці вагових коефіцієнтів. Також для дешифрування даних, щоб отримати оригінальне повідомлення, треба використовувати знайдену матрицю.

Сфера інформаційної безпеки – найбільш динамічна галузь розвитку національної безпеки загалом. Вона залежить від усього комплексу заходів та інноваційних технологій, керування якими відбувається із застосуванням різноманітних інформаційних систем, та постійно потребує нових рішень з урахуванням викликів сьогодення.

Література:

1. Указ Президента «Про Положення про порядок здійснення криптографічного захисту інформації в Україні» від 22 травня 1998 року № 505/98. Електронний ресурс. URL: https://zakon.rada.gov.ua/laws/show/505/98#Text (дата звернення: 03.12.2021).
2. Цмоць І. Г., Рабик В. Г., Лукащук Ю. А. Розроблення мобільних засобів нейроподібного криптографічного шифрування та дешифрування даних у реальному часі. Вісник Національного університету «Львівська політехніка». Серія: Інформаційні системи та мережі. 2021. № 9. С. 84-95.
3. Цимбал Ю. В. Нейромережевий метод симетричного шифрування даних. Вісник Національного університету «Львівська політехніка». Серія: Інформаційні системи та мережі. 2018. № 901. С. 118-122.

Лялюк Г. М.,
доцент кафедри теоретичної психології Інституту управління, психології та безпеки Львівського державного університету внутрішніх справ, доктор педагогічних наук, доцент

НАСИЛЬСТВО В КІБЕРПРОСТОРІ: СОЦІАЛЬНО-ПСИХОЛОГІЧНИЙ АСПЕКТ

Сьогодні наша країна переживає негативні соціальні процеси, які супроводжуються значними кризовими змінами у суспільстві. Одним із таких явищ є насильство. Насильством наповнені різні сфери людського буття: політичне, економічне, духовне та сімейно-побутове. Воно має вираження у пануванні таких явищ як знецінення життя, антигуманність, агресія, жорстокість. За соціально-предметними характеристиками домінуючих типів застосовуваного насильства розрізняють передусім фізичне та психологічне (психоемоційне, від бойкоту до т. зв. «газлайтінгу»), а також проміжні та суміжні його прояви та виміри: насильство вербальне, сексуальне (від зґвалтування [3] до ексгібіціонізму або вуайєризму), фінансове і т. п. Відповідно, за своїми праксеологічними проявами соціальне насильство може бути прямим/безпосереднім (передусім фізичне та суміжне із ними) та опосередкованим (фінансове, гендерне та ін.).

Окреме місце в цьому контексті займає проблематика «насильства у кібер-просторі» або «віртуального насильства», зокрема явища «кібербулінгу» («cyberbullying») та/або «кіберпереслідування» («cyberstalking»).

Надшвидкі темпи процесів інформатизації сучасного суспільства зробили інформаційні, комп'ютерні, мультимедійні технології ключовим об'єктом у житті людини. На сьогодні майже кожна людина не може уявити своє життя без смартфону, комп'ютера та будь-яких інших гаджетів, що забезпечують вихід в мережу Інтернет.

Суспільні відносини, які виникають у віртуальному середовищі, крім позитивних сторін (швидкість обробки і передачі інформації, швидке вирішення професійних та освітніх задач за допомогою прикладних комп'ютерних програм, мобільних додатків у телефоні та ін.), мають також і різко негативний, суспільно небезпечний характер: спостерігається поглиблення тенденції розширення ризиків і загроз впливу на психологічну і соціальну безпеку особисті з боку віртуального інформаційного простору. Зокрема, спілкування у соціальних мережах охоплює широке коло негативних дій – від знущань, залякувань, цькувань у кіберпросторі (кібербулінгу) до більш небезпечних наслідків (самогубства тощо) та стає глобальною проблемою педагогів, психологів, правоохоронних органів.

Сьогоднішнє цифрове середовище – це новий ризик (від кібербулінгу та продажу наркотичних речовин до дитячої порнографії, торгівлі людьми). З метою вербування потенційних жертв злочинці вибирають такі методи вербування, які не привертають уваги компетентних органів, діючи методом індивідуального підбору. З цією метою вербувальники часто знайомляться з жертвами в кіберпросторі. Незалежно від того, з якою метою здійснюється вербування жертв, останні часто стають при цьому об'єктами фізичних та психологічних катувань, зґвалтувань, переслідування [3].

При цьому в зону ризику перш за все потрапляють учнівська і студентська молодь, адже вона не має сформованої психологічної стійкості та перебуває на початку власної соціалізації в суспільстві. На сьогодні чинне законодавство не досконале, тому вести статистику та юридично кваліфікувати вияви кібернасильства дуже важко. Обліковуються лише випадки, коли такі дії призвели до серйозних наслідків відповідальність за які передбачена Кримінальним Кодексом України або Кодексом законів про адміністративні правопорушення України [1, с.181]. З прийняттям Закону України «Про внесення змін до деяких законодавчих актів України щодо протидії булінгу (цькуванню)» від 18 грудня 2018 року термін «булінг (цькування) учасників освітнього процесу» (…у тому числі із застосуванням засобів електронних комунікацій) введено до Кодексу України про адміністративні правопорушення (стаття 173-4) та ЗаконуУкраїни «Про освіту».

За результатами дослідження Дитячого фонду ООН (ЮНІСЕФ), близько третини українських підлітків (29%) ставали жертвами цькування в Інтернеті. В Україні долучилися до опитування 6791 респондент через SMS та сервіси миттєвих повідомлень і виявилося, що 29% опитаних підлітків були жертвами онлайн-булінгу [1]. Національна дитяча гаряча лінія ГО «Ла Страда-Україна» задокументувала 17 847 звернень отриманих в 2019 році. З них 979 стосувалось небезпек, з якими зіштовхуються діти в інтернеті. 684 звернення надійшло від дітей і 295 від дорослих, 322 звернень стосувались питань кібербулінгу, що складає третину від пов'язаних з інтернетом звернень.

Хоча тема кібербулінгу у більшості асоціюється з дітьми чи підлітками, проте постраждати від знущань в Інтернеті може будь-хто та в будь-якому віці. Статистика свідчить, що кібержорстокість продовжує набирати обертів, незважаючи на протидію держави та запровадження різних програм проти знущань. Хоча адміністративна відповідальність за булінг, в тому числі в кіберпросторі, в Україні була введена не так давно, говорити про позитивну динаміку поки рано.

Проблема кібербулінгу розглядається у наукових розвідках зарубіжних (P. Bocij, M. Gottfredson, L. McFarlane, J. Petrocelli) та вітчизняних вчених (Н. Лесько, І. Лубенець, Т. Миронюк, О. Міхєєва, Л. Найдьонової та ін.).

Більшість вчених трактують «кібербулінг», як психологічний вплив однієї особистості на свідомість іншої в інформаційному просторі (умисний, систематичний, спрямований проти особистості, всупереч його волі), який вчиняється з використанням інформаційно-комунікаційних засобів і виражаються у формі передавання невизначеному колу інших осіб повідомлень, фото-, відеоматеріалів, відеозаписів з метою зганьбити, принизити, залякати, образити, зацькувати її [2].

«Кібернасильство» загалом та «кібербулінг»/«кіберпереслідування» зокрема мають певні характерні ознаки, що претендують на принципову соціальну значущість. Передусім «кібернасильство» є не фізичним (адже здійснюється передусім у «кіберпросторі»), а переважно вербальним, психологічним та/або психоемоційним, а також сексуальним (зокрема у вигладі т. зв. «порно-помсти» (revenge porn) тощо) [3]. Засоби кібербулінгу можна ідентифікувати як інформаційну зброю за напрямом і ступенем інформаційного характеру психологічного тиску.

Завдяки сучасним технологіям насильство у кіберпросторі може реалізовуватися цілодобово та анонімно. Похідним чинником «анонімності» є проблема ускладнення визначення пошуку його джерел та ідентифікації осіб, залучених в цей процес.

Додаткову глибину та проблемність цьому явищу надає та обставина, що викладені в глобальну мережу фіксації проявів насильства (тексти, зображення, відео тощо) легкодоступні якнайширшій аудиторії, причому їх зазвичай дуже важко позбутися (адже видалити поширювані в мережі «вірусні» сюжети майже неможливо). Відповідно, принципово ускладнюється похідна проблема соціально-психологічної реабілітації та соціально-середовищної адаптації жертв кібернасильства.

Кібербулінг має власну типологію, де класифікаційною ознакою є форма поведінки, відповідно до якої виокремлюють вісім типів кібербулінгу (*табл. 1*) [2].

Таблиця 1

Загальна типологізація кібербулінгу як загрози психологічній та соціальній безпеці особистості

Тип кібербулінгу	Характеристичний опис	Загроза безпеки
Флеймінг (flaming)	обмін короткими гнівними та запальними репліками, використовуючи комунікаційні технології, яка може перетворитися в затяжну війну	нерівноправний психологічний терор, що призводить до сильних емоційних переживань
Харассмент або нападки, постійні виснажливі атаки (harassment)	повторення образливих повідомлень, із перевантаженням персональних каналів комунікації, тривалі й односторонні	характерно для онлайн-ігор, руйнація ігрового досвіду
Обмовлення, зведення наклепів (denigration)	розповсюдження принизливої неправдивої інформації з використанням комп'ютерних технологій, тренування власної злоби, зливання роздратування, перенесення агресії тощо	психологічний терор, що призводить до сильних емоційних переживань, підвищує репутаційні ризики (руйнування іміджу і репутації)
Самозванство, втілення в певну особу (impersonation)	позиціонування онлайн-агресора як жертви, використовуючи її пароль	імперсоналізації проти людей, включених до

	доступу до її аккаунту в соціальних мережах, блогу, пошти, системи миттєвих повідомлень тощо, для подальшого здійснення негативної комунікації	«списку груп ненависті», наражає на реальну небезпеку їхнє життя
Ошукування, видурювання конфіденційної інформації та її розповсюдження (outing&trickery)	отримання персональної інформації в міжособовій комунікації та оприлюднення її у віртуальному середовищі	підвищує репутаційні ризики (руйнування іміджу і репутації)
Відчуження (остракізм), ізоляція	виключення із соціуму, обмеження можливості власного позиціонування та взаємодії у групі	падіння самооцінки, серйозні емоційні негаразди, аж до повного емоційного руйнування, соціальна смерть
Кіберпереслідування (cyberstalking)	приховане, анонімне вистежування необережних користувачів через Інтернет для отримання інформації про час, місце і всі необхідні умови здійснення майбутнього нападу	злочинні дії, фізичне насильство, побиття
Хепіслеппінг або щасливе ляскання (happyslapping)	зняття відеороліків реальних нападів (хепіслеппінг), ґвалтування чи його імітації (хоппінг) із подальшим розміщенням в Інтернеті без згоди жертви	може призвести до трагічних наслідків

За даними моніторингу дослідницького центру Cyberbullying (2018), протягом останніх років спостерігається тенденції зростання кібербулінгу. Стійкими тенденціями є:

- зростання уваги до теми залякування серед комп'ютерних розповсюджувачів;
- стосовно гендерного аспекту онлайн-агресорів спостерігається тенденція більшої схильності дівчат (жінок) до кібербулінгу, адже серед них був виявлений більш високий рівень явної агресії за всіма видами поведінки, тому їх можна ідентифікувати як активних комбінованих кібербулерів;
- стосовно наслідків кібербулінгу — зростає кількість спроб самогубства або думок про нього [2].

Психологічну небезпеку з боку кібербулінгу потрібно розглядати на рівні особистості та системи відносин у суспільстві. Захистити користувачів он-лайн стає складним завданням сьогодення. Особливої уваги науковців та правоохоронних органів потребує проблема профілактики кіберсталкінгу, який може змінюватися від небезпечних електронних повідомлень до потенційно смертельної зустрічі між зловмисником та жертвою [8].

Серед типологій кіберпереслідувань однією з популярних вважається типологія L. McFarlane та P. Bocij (2005), які провели одне з найбільш вичерпних досліджень з питання онлайн-переслідувань, в результаті яких з'явилися чотири типи кіберсталкерів [6]. На думку вчених, до них відносяться мстивий кіберсталкер, стриманий кіберсталкер, інтимний кіберсталкер та колективний кіберсталкер [6].

Мотивацію онлайн-переслідувачів можна поділити на 4 основні групи:

- мотивація до задоволення своєї психологічної потреби, бажання або тяги до іншої людини (наприклад, нав'язлива зацікавленість до когось, бажання висміювати когось, дражнити когось задарма);
- мотивація вселити страх жертві або встановити над нею контроль;
- мотивація, яка стосується бажання помститися або покарати жертву (зазвичай в результаті негативних емоцій по відношенню до жертви, таких як гнів або ревнощі);
- мотивація до встановлення стосунків з жертвою (включаючи сексуальні відносини) [8].

Вчені зазнають, що кіберсталкери можуть мати одночасно декілька мотивів, що визначають й керують поведінкою.

Психологічне пояснення кіберсталкінгу полягає в тому, що кіберсталкери здійснюють злочини маючи психічні відхилення [4]. Дослідники вказують на те, що переслідування не є результатом психічного розладу, а скоріше розладом поведінки, таким чином кіберсталкери схильні бути емоційно віддаленими одинаками [7], які просто хочуть шукати уваги і товариства в іншим [5]. Проблема полягає в тому, що переслідувачі часто стають одержимими й захоплюються жертвами, які не відповідають взаємністю на почуття і, відтак, уявлення про них деформується, що й детермінує специфічний тип переслідування [8].

Аналіз результатів емпіричних досліджень дозволяє виокремити такі особливості кіберсталкерів: схильність до дій, які детерміновані потягом до влади та контролю, високий рівень тривожності, високий рівень нейротизму, маячні ідеї або параноїдальні схильності, знижена стресостійкість, занижена самооцінка та образливість. Особи, схильні до кіберсталкінгу, не здатні контролювати власні емоції та імпульсивні потяги. Їхня поведінка характеризується зниженим відчуттям відповідальності за власні дії. Як правило для них характерні прояви ескапізму, такі люди відчувають, що нездатні витримувати життєві труднощі, їхні дії підпорядковані ситуативним чинникам, при цьому почуття тривоги й розгубленості, ймовірно, переважають у разі неприємностей, отже, люди легко піддаються відчаю. Кіберсталкерам притаманний середній або вище показники IQ, розвинуті навички роботи з комп'ютером [8]. Особистісні чинники можуть виступати превалюючими предикторами у формуванні та визначенні рівня схильності до кіберсталкінгу.

Знання про існування зв'язку та особистісних чинників даного феномену дає змогу прогнозування можливої особистісної моделі кіберсталкерів із метою подальшого аналізу причин виникнення схильностей до кіберпереслідування, розроблення програм попередження противоправних дій, корекційних програм тощо. Поглиблене систематичне дослідження цього феномену і випадків його прояву забезпечить методи для підтримки більш ефективної профілактики онлайн-переслідувань та діагностики кібер-сталкерів.

Висновки. Поширення насильства у кіберпросторі вимагає побудови ефективної системи профілактики і протидії, яка спирається на принципи соціальної безпеки особистості, саморегуляції, психологічного самозахисту і взаємодопомоги. Кібербулінг є проблемою, що потребує комплексного підходу і застосування всіх методик для профілактики і подолання проявів його впливу. Особливого значення має набути фахова робота щодо розробки ефективних способів превенції кібернасильства і доказових методів втручання для зменшення негативних наслідків цього явища, апробація та застосування програм профілактики кібербулінгу в Інтернет середовищі.

Літераптура:

1. Лубенець Ірина. Кібернасильство (кібербулінг) серед учнів загальноосвітніх навчальних закладів. Национальный юридический журнал: теория и практика. 2016. № 3. С. 178–182
2. Пантелєєва Н.М., Кабенгеле Г. Кібербулінг як загроза психологічній і соціальній безпеці життєдіяльності особистості та суспільства. Фінансовий простір 2018 № 4 (32) С.125-131.
3. Полтораков О. Ю. Сучасні соціокультурні виміри насильства: соціологічний підхід. Габітус. 2019. № 8. С. 25-28.
4. Bocij P. Seven fallacies about cyber stalking / P. Bocij, L. McFarlane // Prison Service Journal. – 2003. – № 149. – pp. 37-42.
5. Gottfredson M.R. A General Theory of Crime / M.R. Gottfredson, T. Hirschi. – Stanford: Stanford University Press, 1990. – 297 p.
6. McFarlane L. An exploration of predatory behaviour in cyberspace: Towards a typology of cyberstalkers/ L. McFarlane, P. Bocij // First Monday. –
7. 2003.URL:https://www.researchgate.net/publication220167750_An_exploratio
8. n_of_predatory_behaviour_in_cyberspace_Towards_a_typology_of_cyberstaer
9. Petrocelli J. Cyber stalking / J. Petrocelli // Law & Order. – 2005. – № 53. – pp. 56-58.
10. Understanding and Predicting Cyberstalking in Social Media: Integrating Theoretical Perspectives on Shame, Neutralization, Self-Control, Rational Choice, and Social Learning / P.B. Lowry, J. Zhang, C. Wang та ін. // International Conference on Systems Sciences. – 2013. URL: https://www.researchgate.net/publication/268597303_Understanding_and_predicting_cyberstalking_in_social_media_Integrating_theoretical_perspectives_on_shame_neutralization_self-control_rational_choice_and_social_learning

Магеровська Т. В.,
доцент кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів Львівського державного університету внутрішніх справ, доцент кафедри обчислювальної математики та програмування Національного університету «Львівська політехніка», кандидат фізико-математичних наук, доцент

Філь Б. М.,
доцент кафедри обчислювальної математики та програмування Національного університету «Львівська політехніка», кандидат фізико-математичних наук, доцент

Шостак К.,
здобувач вищої освіти Львівського державного університету внутрішніх справ

АНАЛІЗ СПОСОБІВ ВПРОВАДЖЕННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ОСВІТНИЙ ПРОЦЕС

Використання штучного інтелекту в освіті призвело до підвищення ефективності навчання, глобалізації навчання, персоналізації навчання, збільшення інтелектуального контенту, підвищення ефективності та результативності управління освітою. Штучний інтелект продовжує активно розвиватися і, як наслідок, з'являються нові способи його застосування в освіті.

Інтерес до використання алгоритмів і систем штучного інтелекту в освіті з кожним роком зростає. Помітне значне зростання числа статей, що були опубліковані за темою «Штучний інтелект» та «Освіта» починаючи з 2012 року (Рис. 1). По мірі розвитку освіти дослідники намагаються застосовувати інтелектуальний аналіз даних для вирішення складних задач та адаптації методів навчання для окремого студента.

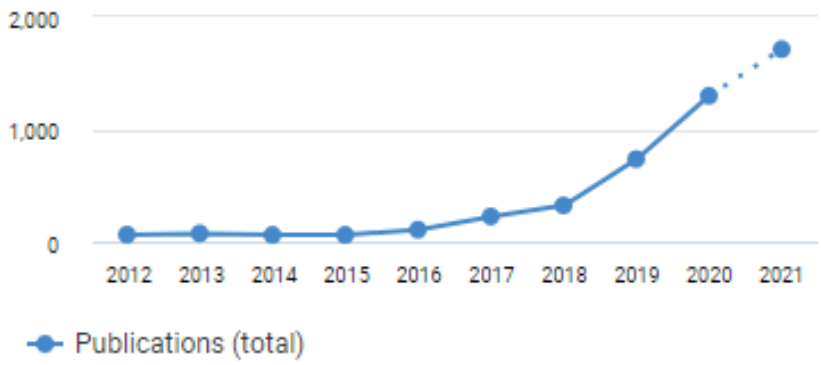

Рис. 1. Кількість статей з ключовими словами «Artificial Intelligence» та «Education» за 2012-2021 гг. (по даним https://app.dimensions.ai)

Існує безліч можливих варіантів впровадження елементів штучного інтелекту до системи освіти, наприклад:

- виконання адміністративних задач, які віднімають багато часу;
- адаптація навчальних програм до потреб користувачів;
- виявлення елементів курсу, зміст яких потрібно покращити;
- аналіз навчальної програми та матеріалів курсу для створення індивідуального контенту;
- індивідуальний метод навчання для кожного студента на основі персональних даних;
- виявлення недоліків в навчанні студентів та їх ліквідацію на ранніх етапах;
- зворотній звязок через додатки зі штучним інтелектом;
- зміна ролі викладачів;
- спрощення навчання методом спроб і помилок;
- зміна пошуку, навчання та підтримки студентів;
- зміна місця та методів навчання;
- прогнозування кар'єрного шляху для кожного студента на основі даних про навчання.

Очікується, що незабаром освіту неможливо буде уявити без участі штучного інтелекту, який буде контролювати освітній процес від початку до кінця. Наразі алгоритми залучають до освітнього процесу фрагментарно.

Можливі наступні варіанти інтеграції штучного інтелекту в освітній процес:

- репетиторство;
- автоматизація оцінки знань;
- аналіз поведінки студентів;
- дистанційно-очна освіта.

Вже існують програми-репетитори (наприклад, YiXue Inc), завдяки яким можна додатково вивчити незрозумілу тему. Штучний інтелект може також проаналізувати виконані роботи, визначити проблемні ділянки та створити індивідуальні заняття для заповнення прогалин у знаннях.

Очікується, що незабаром штучний інтелект навчиться перевіряти письмові роботи та екзаменаційні завдання за допомогою встановлених правил, які виключатимуть упередженість та некомпетентність викладачів.

Використовуючи камери, штучний інтелект може аналізувати поведінку здобувачів освіти, як вони реагують на різні теми та завдання, їх емоційний та фізичний стан, причини прогулів, професійні навички вчителів.

Однією з альтернативних можливостей застосування штучного інтелекту в освіті є впровадження його у процес дистанційно-очного навчання яке полягає у наступному:

- видача завдань різної складності групам студентів з подальшою перевіркою виконання та оцінюванням;
- перевірка присутності;
- аналіз змісту курсу та повідомлення викладача про можливість недостатнього засвоєння студентами окремих тем;
- складання та оцінювання завдань для контролю засвоєння знань;
- порівняння фотографії студента, яка є в базі, із зображенням з веб-камери пристрою, на якому студент проходить тестування. Система має реєструвати спроби студента порушити правила академічної чесності при складанні іспиту (спроби скласти іспит сторонніми людьми, використання шпаргалок, смартфонів, наявність у приміщенні сторонніх тощо).

Основні методи створення сценаріїв навчання зі штучним інтелектом наведені в таблиці 1.

Таблиця 1

Сценарії	Методи
Оцінка здобувачів освіти та навчальних закладів	Метод адаптивного навчання, персоналізований підхід до навчання, аналітика навчання
Оцінка робіт та іспитів	Розпізнавання зображень, система прогнозу
Персоналізоване інтелектуальне навчання	Data mining, інтелектуальні освітні системи, аналітика навчання
Розумні навчальні заклади	Розпізнавання обличчя, розпізнавання мови, доповнена та віртуальна реальність (AR, VR)
Онлайн і мобільна дистанційна освіта	Граничні обчислення, віртуальний персональний асистент, аналіз у режимі реального часу

Таким чином при впровадженні штучного інтелекту, навіть частковому, в освітньому процесі можна досягнути зменшення об'єму рутинної та монотонної роботи, прискорення темпів виконання завдань, спрощення розв'язання складних проблем.

Але жодна технологія не обходиться без несприятливих наслідків. І хоча штучний інтелект дійсно створює ажіотаж в індустрії освіти завдяки удосконаленим та ефективним засобам навчання та викладання, не потрібно ігнорувати те, що цей прогрес може призвести до збоїв.

Для визначення раціональності впровадження штучного інтелекту в освіту проведемо наступний аналіз (табл.2).

Таблиця 2

Корисно	Шкідливо
Сильні сторони: – Покрокові системи STEM – Ефективне навчання за допомогою комп'ютерів – Навчальні агенти для вивчення природної мови – Екосистеми засобів навчання – Оцінка моделей навчання	Слабкі сторони: – «Дурні» системи навчання – Упередженість даних та алгоритмів – Налаштування штучного інтелекту заважає стандартизації
Можливості: – Зміни у ролі викладача – від «мудреця на сцені» до «помічника» – Допомога викладачам та звільнення викладачів від стомлюючої рутинної роботи – Допомога викладачам у будь-який час та в будь-якому місці – Персоналізоване навчання	Загрози: – Зміни у ролі викладача - викладач як спеціаліст з обслуговування системи – Страх ризику зникнення / страх заміни – Недостатня підготовка в освіті для використання ШІ-освіти – Штучний інтелект заважає студентам, що розвивають навички самостійного навчання – Шумиха може призвести до незаперечної «панацеї»

Цей аналіз показує, що необхідно з обережністю підходити до впровадження штучний інтелект в освітній процес, проте під час виконання певних умов можна уникнути неприємних результатів.

Наприклад, необхідно поступово вводити елементи штучного інтелекту, щоб за потреби можна було повернутися до старих методів у разі відмови системи. Також необхідна попередня підготовка та додаткове навчання як викладачам, так і студентам для того, щоб уникнути нерозуміння роботи системи та відчуття "незручності" користування або "непотрібності" керівника.

При цьому в разі успішного впровадження у студентів з'являться нові методи для вивчення різних матеріалів, а у викладачів буде більше часу для роботи зі студентами, а не з документацією. До того ж штучний інтелект дозволить персоналізувати процес навчання кожного студента, виходячи з їхнього рівня підготовки та наявних знань.

Література:

1. https://app.dimensions.ai/discover/publication
2. Disrupting clinical education: Using artificial intelligence to create training material. The Clinical Teacher, 17(4), 357-359 - June 2020
3. Artificial Intelligence in Education (AIEd): a high-level academic and industry note 2021. AI and Ethics, 1-9 - July 2021
4. Artificial intelligence in education: Addressing ethical challenges in K-12 settings. AI and Ethics, 1-10 - September 2021
5. Пути к общему искусственному интеллекту: краткий обзор разработок и этических проблем с помощью искусственного интеллекта, машинного обучения, глубокого обучения и науки о данных Мохаммадреза Иман, Хамид Р. Арабния, Роберт Марибе Бранчинст 2021 г. , Advances in Artificial Intelligence and Applied Cognitive Computing Transactions on Computational Science and Computational Intelligence, 73-87 - October 2021

Мовчан А. В.,
професор кафедри оперативно-розшукової діяльності Львівського державного університету внутрішніх справ, доктор юридичних наук, професор

Жуковський І. В,
аспірант кафедри оперативно-розшукової діяльності Львівського державного університету внутрішніх справ

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ ІНТЕРПОЛУ ТА ЄВРОПОЛУ У ПРОТИДІЇ ЗЛОЧИНАМ, ПОВ'ЯЗАНИМ З ТОРГІВЛЕЮ ЛЮДЬМИ

Важливе значення для підвищення ефективності діяльності правоохоронних органів України у протидії злочинам, пов'язаним з торгівлею людьми, має взаємодія з міжнародними правоохоронними, поліцейськими та безпековими організаціями, зокрема Інтерполом та Європолом.

Основними завданнями Генерального Секретаріату Інтерполу щодо протидії злочинам, пов'язаним з торгівлею людьми, є:

- координація співробітництва правоохоронних органів держав-членів Інтерполу у справах щодо злочинів, пов'язаних з торгівлею людьми та незаконною міграцією;
- створення та формування спеціалізованих банків даних щодо осіб, причетних до торгівлі людьми;
- ведення банку даних порнографічних зображень неповнолітніх;
- ідентифікація потерпілих у справах про транснаціональні злочини, пов'язані із створенням та розповсюдженням дитячої порнографії;
- запровадження та реалізація аналітичних проєктів у сфері протидії торгівлі людьми;
- організація та проведення міжнародних науково-практичних заходів з проблем протидії торгівлі людьми (конференцій, тренінгів, оперативних зустрічей тощо) [1].

Однією із основних форм міжнародного поліцейського співробітництва є використання банків даних Генерального секретаріату Інтерполу, які мають за мету забезпечення всебічної взаємодії правоохоронних органів держав-членів Інтерполу. Банки даних Інтерполу є складовою інформаційної системи Інтерполу, в якій зберігаються дані щодо осіб, предметів та подій, що обробляються Генеральним секретаріатом Інтерполу з метою забезпечення міжнародного співробітництва правоохоронних органів.

В інформаційній системі Інтерполу використовується 19 банків даних з інформацією про злочини та злочинців, які доступні в реальному часі країнам-членам Європолу. Формування цих банків даних здійснюється за рахунок інформації, яку надають правоохоронні органи держав-членів Інтерполу на добровільних засадах. Право власності на цю інформацію належить виключно тим державам, які її надали [1].

Міжнародне співробітництво правоохоронних органів України з органами Інтерполу, компетентними органами іноземних держав та міжнародними установами з використанням інформаційної системи Інтерполу здійснюється згідно з Правилами Інтерполу. Цілями міжнародного співробітництва з використанням інформаційної системи Інтерполу є:

- установлення місцезнаходження осіб, які розшукуються, з метою їх затримання, арешту, обмеження свободи пересування та подальшої видачі (екстрадиції);
- установлення місцезнаходження осіб чи об'єктів, що становлять інтерес для правоохоронних органів України чи інших держав-членів Інтерполу;
- надання чи отримання інформації, що стосується розслідування злочинів, кримінального минулого або злочинної діяльності осіб;
- надання чи отримання інформації з метою попередження про осіб, події, об'єкти, способи вчинення злочинів, що становлять реальну загрозу публічній безпеці та порядку й можуть завдати істотної шкоди майну чи громадянам;
- ідентифікація осіб чи невпізнаних трупів та проведення криміналістичних досліджень;
- надання чи отримання інформації з питань публічної безпеки і порядку;
- ідентифікація загроз, організованих груп та злочинних організацій, тенденцій розвитку злочинності;
- обмін досвідом з питань боротьби із злочинністю та правоохоронної діяльності [2].

Генеральний секретаріат також надає доступ до банку даних циркулярних повідомлень Інтерполу за допомогою системи I-24/7. У зазначеному банку даних зберігається інформація про усі циркулярні повідомлення в електронному вигляді.

Використання інформаційної системи Інтерполу правоохоронними органами України здійснюється відповідно до порядку, встановленого Інструкцією про порядок використання правоохоронними органами України інформаційної системи Міжнародної організації кримінальної поліції – Інтерпол, затвердженої наказом МВС, Офісу Генерального прокурора, НАБУ, СБУ, ДБР, Мінфіна, Мінюста від 17 серпня 2020 р. № 613/380/93/228/414/510/2801/5, у формі надсилання запиту/звернення до уповноваженого підрозділу або у формі прямого доступу [2].

Національна поліція України в діяльності з розслідування транснаціональних злочинів взаємодіє також із установами Євросоюзу (EUROPOL, EUROJUST, FRONTEX). Зокрема, Європейський поліцейський офіс (Європол) є міжнародною правоохоронною організацією, що бере активну участь у протидії злочинності в рамках Європейського Союзу.

Європол підтримує правоохоронну діяльність держав-членів ЄС шляхом: сприяння обміну інформацією між Європолом та співробітниками зв'язку з Європолом; сприяння обміну інформацією з третіми державами та третіми органами влади відповідно до положень відповідних угод Європолу; забезпечення оперативного аналізу та підтримки операцій у державах-членах Європолу; надання експертизи та технічної підтримки для розслідувань та операцій, що проводяться в межах ЄС, під наглядом та юридичною відповідальністю держав-членів Європолу; формування стратегічних звітів (таких як оцінка загрози) та аналіз злочинів на основі інформації та розвідувальних даних, що надаються державами-членами Європолу або збираються з інших джерел [3].

Європол забезпечує обмін інформацією між країнами-членами Євросоюзу через офіцерів зв'язку, які представляють національні правоохоронні органи, діють у межах законодавства своєї держави і не є підконтрольними керівництву Європолу.

Водночас слід зазначити, що Європол має ряд відмінностей від інших міжнародних правоохоронних організацій. Зокрема, суб'єктами взаємодії можуть виступати не тільки органи поліції держав-членів, а й органи охорони державного кордону, податкові, митні, фінансові, імміграційні, розвідувальні та інші органи, що уповноважені проводити оперативно-розшукову діяльність чи розслідування кримінальних справ.

Підставою для початку роботи співробітників Європолу над певною категорією справи є офіційний запит держави-члена ЄС. До того ж необхідно, щоб викладена в запиті інформація стосувалась двох чи більше держав-членів ЄС, свідчила про причетність до вчинення злочинів організованих груп і відповідала компетенції Європолу.

Оперативна та стратегічна угода між МВС України та Європолом щодо розширення співробітництва у боротьбі з транскордонною злочинною діяльністю була підписана 14 грудня 2016 року і ратифікована Верховною Радою України 12 липня 2017 року. На підставі зазначеної угоди Україна створила національний контактний пункт, який є центральним пунктом обміну інформацією між Європолом та правоохоронними органами України. Крім того, в МВС України встановлено спеціальний захищений канал зв'язку SIENA для обміну інформацією з Європолом. Використання безпечної мережевої програми обміну інформації SIENA дозволяє швидко та зручно обмінюватися оперативною та стратегічною інформацією, пов'язаною зі злочинністю, між офіцерами зв'язку Європолу, аналітиками та експертами; країнами-учасницями ЄС; третіми країнами, які мають відповідні угоди з Європолом.

Крім того, важливе значення для протидії торгівлі людьми мають проєкти Європолу AP Phoenix (справи по торгівлі людьми) та AP Twins (злочинність, пов'язана з сексуальною експлуатацією та насильством дітей).

Отже, використання інформаційних систем Інтерполу і Європолу має важливе значення для підвищення ефективності діяльності оперативних підрозділів Національної поліції у сфері протидії злочинам, пов'язаним з торгівлею людьми.

Література:

1. Офіційний веб-сайт Інтерполу URL: https://www.interpol.int/
2. Про затвердження Інструкції про порядок використання правоохоронними органами України інформаційної системи Міжнародної організації кримінальної поліції – Інтерпол: наказ МВС, Офісу Генерального прокурора, НАБУ, СБУ, ДБР, Мінфіна, Мінюста від 17 серпня 2020 р. № 613/380/93/228/414/510/2801/5, зареєстрований в Міністерстві юстиції України 04 вересня 2020 р. за № 849/35132.
3. Офіційний веб-сайт Європолу URL: https://www.europol.europa.eu/

Mikhaleva M.,
Hetman Petro Sahaidachnyi National Army Academy, Professor of the Department of Electromechanics and Electronics, Associate Professor, Ph.D.

Shabatura Y.,
Hetman Petro Sahaidachnyi National Army Academy, Head of the Department of Electromechanics and Electronics, Professor, Doctor of Technical Sciences

Yarovenko V.,
Hetman Petro Sahaidachnyi National Army Academy, cadet

Kozachenko M.,
Hetman Petro Sahaidachnyi National Army Academy, cadet

Uzhak D.,
Hetman Petro Sahaidachnyi National Army Academy, cadet

Tikhomirov D.,
Hetman Petro Sahaidachnyi National Army Academy, cadet

CREATION OF METHODS AND MEANS FOR OPERATIONAL CONTROL OF THE COMPOSITION OF TECHNICAL FLUIDS, WAYS TO BRING MILITARY EQUIPMENT CLOSER TO NATO COMPATIBILITY

Implementing NATO standards and improving them with new developed methods ensures the systematic increase in the combat capability of troops, achieving compatibility with the forces and means of the world's leading countries, and improving the efficiency of the use of state resources in the field of defense.

We conduct research and develop new methods and techniques for automated control of technical fluids (brake fluid, motor oil, rocket fuel, coolant). The novelty of such methods is to determine the level of quality and safety by electrical parameters. Based on the obtained results, drafts of improved National Standards on Metrological Testing Methods of Equipment in the Armed Forces of Ukraine are being developed, which are adapted and harmonized with NATO requirements. The introduction of new methods and techniques will help increase the technical level and improve the provision of the Armed Forces of Ukraine.

The set of scientific developments in these studies is the basis for contributing to the development of technical principles for the development of electrical methods and methods for determining the concentrations of substances of multicomponent liquids by electrical parameters (admittance) for their operational control. The implementation of the developed method and methods creates conditions for the transition from laboratory control conditions to operational ones during the operation of the equipment. The obtained results allow to solve the problem of increasing the reliability of control, uninterrupted operation of equipment and preservation of the environment.

The main research results are as follows.

Experimental studies of model fluids of different chemical nature have been performed and the use of ultrasound to amplify the test signal has been proposed.

Tests of work of models, knots, converters and elements of VIS (measuring information system) are carried out.

On the basis of experimental researches the requirements to a design of the electric primary converter are proved.

Based on the scientific facts obtained during the experimental research, a method and measuring model of operational control of the coolant composition for the engine of self-propelled artillery equipment was developed.

On the basis of the obtained results of experimental researches the electric method of control of brake liquid, liquid types of rocket fuel, motor oil, etc., for uninterrupted work of military equipment is improved.

Tasks of further researches are formulated.

The introduction of new methods and techniques will help increase the technical level and improve the provision of the Armed Forces of Ukraine. Using the results of research of this work and implementation in the

educational process - in conducting practical, laboratory and scientific work improves the training process of future officers, aimed at performing professional tasks at the highest technical level

On the basis of joint research and the agreement on scientific and technical cooperation between Hetman Petro Sahaidachnyi National Army Academy and "Research Institute of Metrology of Measuring and Control Systems" (DNDI "System") obtained new theoretical and practical results, which are implemented for water control in the National Primary Standard Unit of Ultrasound Power NDETU AUV-01-2018.

Improving the systems of operational control of fluids is important for the supply of troops, and their use in military equipment will contribute to the smooth operation of machines, save money and reduce environmental impact.

On the basis of scientific research the method and methods of operative control of the composition of liquids are argued and proposed, which is based on the dependence of the value of the active and reactive component of conductivity on the signal frequency (imitation method). This method allows to estimate the composition of the liquid in non-laboratory conditions for up to 2 seconds and to ensure its control, which will be introduced in the new national standards. The new method makes it possible to create a cyberphysical system that will consist of sensors (configured for each controlled substance), RLC meter and computer.

The aim of the work is to develop the structure of IBC control of technical fluids on the basis of a new electrical method

The subject of research – technical fluids used in military equipment of artillery units.

The object of study – the dependence of the electrical properties of multicomponent liquids on their composition (brand of technical fluid)

Expected results – methodological proposals for the use of the electric method, IMS control of technical fluids for the smooth operation of military equipment.

In laboratory conditions, studies of model (standard) fluids and real technical fluids (coolants for military equipment) were performed.

The proposed algorithm of the new technique has theoretical and practical significance for the creation and application of a new physico-chemical method of controlling the composition of multicomponent liquids (which are real liquids in industry) by electrical parameters.

Conclusion. On the basis of theoretical and practical researches the method of operative control of structure of cooling liquids which is based on dependence of value of active and reactive component of conductivity on frequency of a signal is offered. This method allows you to quantitatively and qualitatively assess the composition of the liquid for the content of controlled components and ensure uninterrupted operation of the equipment in a short time (up to 2 seconds).

The tests were performed for real brands of coolants of different composition – untreated – (1) and treated (2) on an industrial RLC meter.

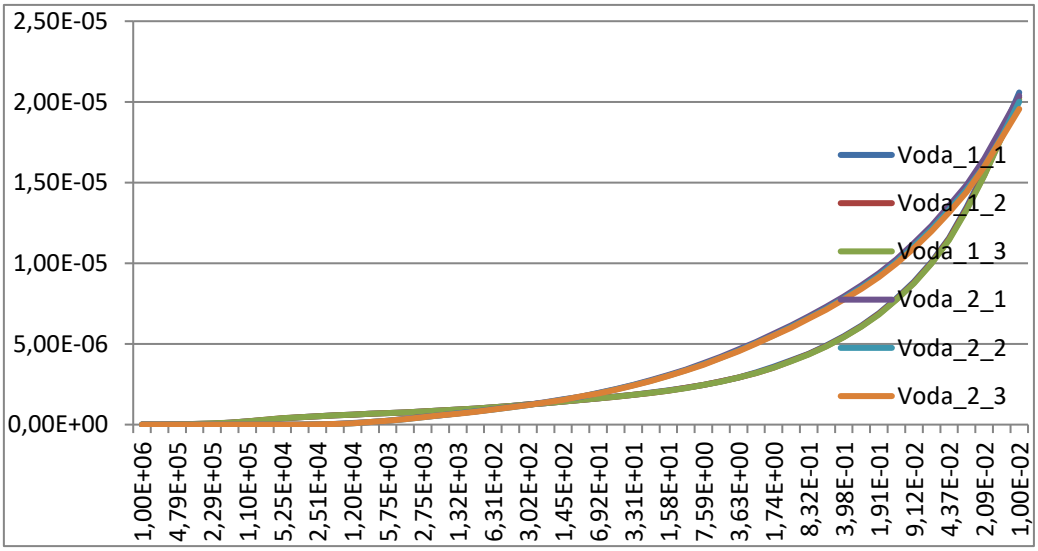

Figure 1 Admission spectra of the dependence of the active component on the frequency of the electromagnetic signal for model fluids

The results of the research led to conclusions about the sensitivity of the method and selectivity (selective) for the control of multicomponent liquids.

So, in this paper:

- the process of harmonization of National Technical Military Standards with NATO standards on technical fluid control was analyzed
- electrical parameters of aqueous solutions in different-frequency electromagnetic field for creation of control systems of multicomponent liquids on the basis of electric sensors are investigated

Algorithms of a new method and means of fast non-laboratory method of quality control of technical liquids by electrical parameters have been developed.

The work is of theoretical and practical importance for the development of a new electrical method and the improvement of National Standards for Express Automated Control and Testing of Real Objects of Technical Fluids.

Implementing NATO standards and improving them with new developed methods ensures the systematic increase in the combat capability of troops, achieving interoperability with the forces and means of the world's leading countries, and improving the efficiency of the use of state resources in the field of defense.

During scientific conferences at Hetman Petro Sahaidachnyi National Army Academy, discussions are held on improving the technical level of control of equipment in the Armed Forces of Ukraine through the use of new methods and means of control at work, testing and metrological traceability.

Revision and improvement of National Military Technical Standards contributes to the development of the Armed Forces. Using the results of research of this work and implementation in the educational process - in conducting practical, laboratory and scientific work and master's projects improves the training process of future officers, aimed at performing professional tasks at the highest technical level.

The participation of scientific and pedagogical staff with the involvement of cadets of the military institution in scientific and technical developments, their introduction into the educational process promotes the development of cadets scientific, technical thought, which will ensure him to constantly learn throughout life and improve the technical level of the Armed Forces.

Literature:

Mikhaleva M., Bourdainiy M. Yarovenko V., Kozachenko M., Uzhak V. Research of the process of harmonization of technical national military standards with NATO standards. Prospects for the development of armaments and military equipment of the land forces Collection of abstracts of the International Scientific and Technical Conference (Lviv, May 14, 2021) P. 24.

Огірко О. І.,
доцент кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів Львівського державного університету внутрішніх справ, кандидат технічних наук, доцент

ОСНОВНІ АСТЕКТИ КІБЕРБЕЗПЕКИ ЕЛЕКТРОННИХ ПЛАТЕЖІВ

Інформаційних технологій охоплюють усі сфери суспільного життя, їх використовують для ведення бізнесу, торгівлі та навчання, вони надають нам можливість отримувати та ділитись інформацією із будь-якого куточку світу навчатись, працювати та стають основним механізмом фінансових переказів між банками та іншими установами.

У широкому значенні електронні платежі це електронний переказ грошей з одного банківського рахунку на інший, або в рамках однієї фінансової установи, або декількох установ, через комп'ютерні системи без прямого втручання банківського персоналу [1]. За інформацією ПриватБанку, за два останні роки в Україні кількість операцій клієнтів з готівкою в касах відділень банку знизилась у 2,5 рази, кількість щоденних операцій зі зняття знизилася ще більше зі 137 до 31 тис. операцій на день. Кількість електронних платежів у 2021 році в порівнянні з 2019 роком зросла на 34% [2].

Система електронних платежів, яка забезпечує розрахунки банків та їхніх клієнтів у гривні в межах України, середньому в день обробляє 1,6 млн платежів на суму близько 199 млрд грн [3]. Як, бачимо, електронні платежі вже стали буденним явищем, особливо в умовах пандемії та карантинних обмежень.

Чим більше ми використовуємо інформаційних технологій у фінансовій системі тим вразливішою вона стає до кіберзагроз. За даними CSI 2021 Banking Priorities Survey проблема кібербезпеки сьогодні має найбільший вплив на діяльність банків. Згідно з даними дослідження, 81% банкірів вважають соціальну інженерію найбільшої загрозою для кібербезпеки у 2021 році (рис. 1) [2, 3].

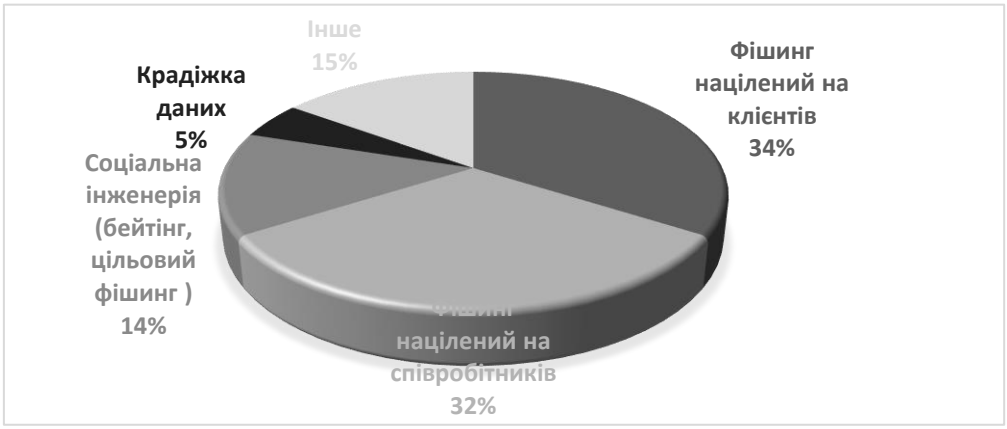

Рис. 1 Найбільші загрози кібербезпеки банку

В теперішній час, кібербезпека електронних платежів є актуальною та важливою, як для окремих людей, так і багатьох підприємств, тому дуже важливо правильно її спланувати та реалізувати. Проведення електронного платежу відбувається в системі клієнт-інтернет-банк, яка дозволяє підтримувати зв'язок з банком безпосередньо з персонального комп'ютера клієнта (організації), за наявності мережі Internet. З огляду на це кібербезпеку електронних платежів доцільно розглядати, як двофакторну модель, яка залежить від кібербезпеки клієнта та банку.

До основних аспектів кібербезпеки при проведенні електронних платежів в системі інтернет-банку зі сторони *клієнта* належить [2-6]:

1. Не розголошування свої конфіденційні дані (логін, пароль тощо), навіть особам, що представились співробітниками Банку.
2. Використання лише відповідних адрес для входу на WEB-сторінку системи клієнт-інтернет-банк.
3. Зберігання таємного ключа виключно на переносних носіях інформації.
4. Уникнення використання системи клієнт-інтернет-банк з комп'ютерів в публічних місцях
5. Обмеження доступу до комп'ютера, який використовується для роботи з системою клієнт-інтернет-банк.
6. Доступ до таємних ключів повинен бути тільки в період роботи з системою клієнт-інтернет-банк.

7. Виймати зовнішній носій інформації по завершенні роботи з системою.
8. Використання складних паролів до ключа.
9. Регулярна зміна паролю.
10. Використання на робочому місці системи клієнт-інтернет-банк засобів антивірусного захисту та регулярно оновлювати їх.
11. Послуга фіксована IP-адреса, що обмежить комп'ютери, з яких буде дозволений доступ до системи клієнт-інтернет-банк для здійснення операцій по рахунку.

Особливість кібербезпеки *банку* в механізмі її забезпечення полягає в тому, що, з одного боку, вона є об'єктом застосування регуляторних та управлінських впливів (керівна підсистема), з іншого – є системним параметром функціонування, без якої банк не матиме змогу продовжувати виконувати свою місію та здійснювати безперервну діяльність. Відповідно до цього, показники кібербезпеки мають включатись до загальної стратегії банку та узгоджуватись з цільовими кількісними та якісними параметрами стратегічних планів [7].

У технологічній складовій системи безпеки *інтернет-банку* можна виділити такі напрямки [2-7]:

1. Авторизація користувача системи. Ідентифікація користувача системи проводиться банком з використанням статичного логіна і пароля.
2. Авторизація платіжних операцій, що здійснюються дистанційно. Для автентифікації (авторизації) платіжних операцій в інтернет-банку банками використовуються методи:
   - одноразові паролі;
   - електронно-цифровий підпис.
3. Дані, які передані в банк або прийняті від банку, шифруються спеціальним методом згідно стандартів ISO 8730 та ISO 8731 з використанням пароля і підрахунком контрольної суми файлу, що забезпечує повну конфіденційність прийому і передачі інформації.
4. До бази даних відсутній доступ за допомогою будь-яких засобів, крім як з програми "Клієнт-Банк", тобто база даних є повністю ізольованою від стороннього втручання.
5. Кожен сеанс зв'язку з банком має унікальну систему викривлення, що генерується випадковим чином, що не дозволяє дешифрувати дані в каналі.

Кібербезпека електронних платежів – це процес, який повинен включати в себе достатньо велику кількість важливих рішень, та заходів, одним з яких є створення та запровадження політики безпеки не лише банку, а кожного окремо взятого підприємства, клієнта. Звичайно що неможливо досягти стовідсоткової безпеки, проте виконання наданих порад дозволить вирішити безліч питань, пов'язаних з безпечним використанням електронних платежів.

Література:

1. Трубін І. О. Платіжні системи на основі електронних грошей як складова системи електронних платежів. Проблеми та перспективи розвитку юридичної науки та освіти в Україні : матеріали Всеукр. наук.-практ. конф. до Дня науки (Київ, 17 трав. 2012 р.). Київ: Омега-Л, 2012. С. 479–481.
2. Кібербезпека платежів: що робити, щоб не було запізно. URL: https://rating.zone/chem-obernetsia-dlia-ukrayny-rekordnyj-rost-tsen-na-syrevye-tovary/ (дата звернення: 08.12.2021).
3. Система електронних платежів – Національний банк України. URL: https://bank.gov.ua/ua/payments/sep (дата звернення: 08.12.2021).
4. Інтернет банк для Юридичних осіб і корпоративних клієнтів. URL: https://www.otpbank.com.ua/big-corporate/rko/cash-management/otp-online/ (дата звернення: 08.12.2021).
5. Інтернет клієнт-банк – Ощадбанк. URL: https://www.oschadbank.ua/internet-klient-bank (дата звернення: 08.12.2021).
6. 6. Для юридичних осіб iFOBS | KredoBank. URL: https://kredobank.com.ua/internet-banking/dlya-yurydychnykh-osib-ifobs (дата звернення: 08.12.2021).
7. Криклій О. А. Теорія та практика забезпечення кіберстійкості банків. Ефективна економіка. № 10, 2020.

Попова Т. В. ,
здобувач вищої освіти Дніпропетровського державного університету внутрішніх справ

Прокопов С. О.,
старший викладач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ

ПРОБЛЕМИ ДИСТАНЦІЙНОГО НАВЧАННЯ В ДНІПРОПЕТРОВСЬКОМУ ДЕРЖАВНОМУ УНІВЕРСИТЕТІ ВНУТРІШНІХ СПРАВ

Дистанційне ведення навчальних занять, відсутність зустрічей, не можливість особисто пояснити і допомогти при виникненні проблеми – кілька місяців тому викладачі вищої освіти навіть не уявляли собі подібних ситуацій у своїй роботі. Однак пандемія внесла несподівані зміни та змусила всіх терміново освоювати цифрові інструменти, нові педагогічні підходи та методи. Обов'язкове дистанційне навчання стало викликом для всіх учасників освітнього процесу: вчителів, студентів та курсантів.

Першими на потреби викладачів та здобувачів вищої освіти відгукнулась ІТ галузь: інформаційно-освітніми технологіями і системами комунікації. Звичайно, якісно створені мультимедійні підручники є частиною ресурсу дистанційного навчання, проте головний його аспект – це постійне інтерактивне спілкування студента з викладачем, звісно, можна користуватись Skype чи влаштовувати групові чати-дзвінки-конференції в мессенджерах типу Viber, Telegram та інших, але для проведення відеоконференцій дуже популярним програмний виявився засіб ZOOM[1].

З метою організації та проведення навчальних занять в ДДУВС для забезпечення неперервності освітнього процесу використовуються такі освітні мережі як: MIA: Освіта , «Moodle» – (розраховані на таку категорію користувачів, як слухачі (курсант, студент), а також на науково-педагогічних працівників, що задіяні в навчальному процесі); платформа «StuddyMo» освітня розробка ДДУВС, а саме проведення дистанційного навчання студентів(заочної форми відділення).

Концептуальними напрямами розвитку системи дистанційного навчання в Університеті постають: інтеграція ефективних дистанційних навчальних технологій з традиційним очним і заочним навчальним процесом; впровадження повноцінної форми дистанційної освіти[2].

Робота користувача в особі MIA: Освіта спрямована на ефективне управління ресурсами, а також на планування, організацію, контроль та регулювання дистанційного навчання. Дозволяє організувати навчання в процесі спільного вирішення навчальних завдань, здійснювати взаємообмін знаннями.

Система дистанційного навчання має ряд переваг і значно розширює коло потенційних студентів. Дистанційна форма навчання підходить майже всім, тому що дає можливість гармонійно поєднувати навчання та повсякденне життя. Варто відзначити, концепції дистанційного навчання, а саме всебічне забезпечення ефективної діяльності Університету з метою створення сприятливих умов для організації навчально-виховної, пізнавальної та наукової діяльності учасників освітнього процесу; впровадження новітніх інноваційних технологій в освітній процес; розширення переліку освітніх послуг, що надає Університет; впровадження інформаційних систем для вирішення завдань планування та прогнозування освітньої діяльності здобувачів вищої освіти, науково-педагогічних працівників, організації наукової та науково-дослідної роботи тощо; розробка повного циклу підготовки здобувачів вищої освіти за дистанційною формою, розробка дистанційних курсів для підвищення кваліфікації різних категорій службовців, працівників організацій, підприємств і установ галузей народного господарства[2].

Успіх реалізації Концепції дистанційного навчання значною мірою визначається рівнем конструктивних відносин між учасниками освітнього процесу, їхнім прагненням до самовдосконалення та постійного особистісного зростання.

Серед основних переваг ДДУВС забезпечує використання в освітньому процесі сертифікованих електронних освітніх ресурсів та проводить внутрішній моніторинг якості дистанційного навчання. Сертифіковані веб-ресурси (електронні освітні ресурси, в тому числі дистанційні курси), що необхідні для забезпечення дистанційного навчання, містять: методичні рекомендації щодо їх використання, послідовності виконання завдань, особливостей контролю тощо; відео- та аудіозаписи лекцій, семінарів тощо; мультимедійні лекційні матеріали; термінологічні словники; практичні завдання із методичними рекомендаціями щодо їх виконання; віртуальні тренажери із методичними рекомендаціями щодо їх використання; пакети тестових завдань для проведення контрольних заходів, тестування з

автоматизованою перевіркою результатів, тестування із перевіркою науково-педагогічним працівником; ділові ігри із методичними рекомендаціями щодо їх використання; електронні бібліотеки чи посилання на них; бібліографії; дистанційний курс, що об'єднує зазначені вище веб-ресурси навчальної дисципліни (програми) єдиним педагогічним сценарієм тощо[3].

Окрім переваг дистанційного навчання, існують також і проблемні моменти, це зумовлено, насамперед, специфічними умовами навчання в таких закладах, що ускладнює їх реформування у загальному руслі відповідних процесів.

Наразі дистанційне навчання у Дніпропетровському державному університеті внутрішніх справ перебуває у найскладнішій ситуації через неможливість проведення практичних занять з «Вогневої підготовки», «Спеціально фізичної підготовки», «Тактико-спеціальної підготовки» курсанти дистанційно продовжують опановувати загальні дисципліни, практичні ж заняття в відтерміновано до завершення карантину або перенесено на наступний термін.

Загалом, «інформаційний» етап розвитку світової системи освіти об'єктивний і незворотний. Використання інформаційних технологій в освіті, які відповідають світовому рівню – єдино можливий шлях поступального інноваційного розвитку Університету. Водночас необхідно враховувати і внутрішні фактори. Сучасні вимоги, продиктовані реформуванням економіки та суспільства, призвели до значного збільшення ресурсоємності освітнього процесу. Для забезпечення більшої доступності навчання та зниження ресурсоємності – освітні технології повинні стати максимально ефективними, тобто забезпечувати високий ступінь економічності освітнього процесу при більш високій якості навчання. Необхідно широке застосування інноваційно-інформаційних методів навчання, що мають інтенсифікувати освітній процес. Все це можна досягти широким впровадженням сучасних інформаційно-комунікаційних технологій.

Література:

1. Організація дистанційного навчання. Створення електронних навчальних курсів та електронних тестів: навч. посібн. / В.В.Вишнівський, М.П. Гніденко, Г.І. Гайдур, О.О. Ільїн. – К. : ДУТ, 2014. – 140 с
2. Концепція: Розвитку дистанційної освіти Дніпропетровського державного університету внутрішніх справ на період 2020 – 2025 роки Схвалено Вченою радою Дніпропетровського державного університету внутрішніх справ 28.05.2020 р., протокол № 9. URL: https://dduvs.in.ua/wp-content/uploads/files/nmc/2020/kdk.pdf.
3. Наказ ДДУВС від 05.03.2020 № 232 ПОЛОЖЕННЯ про дистанційне навчання у Дніпропетровському державному університеті внутрішніх справ URL: https://dduvs.in.ua/wp-content/uploads/files/nmc/polog/n20p20-n.pdf.

Проць І. М.,
доцент кафедри адміністративно-правових дисциплін Інституту права Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент

ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ПРОКУРОРСЬКОГО НАГЛЯДУ

Реформування державної та економічної сфери життя суспільства, проведена в країні правова реформа, поставили на порядок денний проблеми побудови якісно нових взаємин між державою та громадянином. Військова агресія Російської Федерації щодо України інші негативні явища викликали підвищення вимог держави та суспільства до організації роботи всіх ланок органів прокуратури, і в більшій мірі до обласних і окружних прокуратур. Саме на ці прокуратури припадає значний, що перевершує за масштабами навантаження прокуратур вищих рівнів, обсяг наглядової діяльності, участі в розгляді судами кримінальних, адміністративних і цивільних справ.

Удосконалення роботи прокуратур тісно пов'язане з науковою організацією праці, застосуванням на практиці досягнень науки, техніки, передового досвіду для оптимізації діяльності прокуратур. Це передбачає раціональний розподіл обов'язків між працівниками, забезпечення узгодженості дій; створення необхідних умов для ритмічної та безперервної роботи, повне і високоефективне використання трудових ресурсів, робочого часу, використання різноманітних прийомів і методів наглядової діяльності, технічних засобів, включаючи персональні комп'ютери та оргтехніку [1, с. 24].

Інформаційно-аналітичне забезпечення прокурорського нагляду це науковий і прикладний напрям міждисциплінарного характеру, що інтегрує знання, перш за все, прокурорського нагляду, кримінально-процесуального, цивільно-процесуального, адміністративного, інших галузей права і управління.

Інформаційно-аналітична діяльність є важливою характеристикою процесу державного управління. Значення її зростає в силу ускладнення управлінських завдань, що виражається в збільшенні числа об'єктів наглядової діяльності, їх диференціації, як наслідок, постійного наростання комплексу розв'язуваних проблем. З одного боку, ці проблеми обумовлені впливом глобальних тенденцій, що проявляються на всіх рівнях самоорганізації соціуму; з іншого боку, необхідністю переорієнтації управлінської стратегії на конкретну людину, що виступає основним зовнішнім клієнтом по відношенню до державних структур. Остання обставина відображена у Цілях сталого розвитку України на період до 2030 року щодо поліпшення якості життя населення, яка розглядається сьогодні як головний орієнтир для суб'єктів соціального регулювання [2].

Завдання інформаційно-аналітичного забезпечення діяльності прокуратури полягає в тому, щоб особи, які приймають рішення, мали необхідний і достатній для прийняття рішення об'ємом інформації. На державному рівні цей баланс покликані забезпечувати аналітичні служби і підрозділи, на рівні обласних і окружних прокуратур – інформаційно-аналітичні відділи, експертні групи, інші організаційні структури.

Маючи подвійну природу та будучи нерозривно пов'язаними з процесом управління, інформація є необхідним компонентом будь-якої діяльності, що вказує на характер мети, способу визначення найкоротшого шляху до неї, методи та засоби подолання цього шляху [3, с. 67].

Під інформаційно-аналітичною роботою в органах прокуратури автори підручника «Прокурорське право» розуміють діяльність по збору, накопичення та аналізу інформації про виконання законів, виявлені порушення, а також про стан боротьби зі злочинністю, прокурорської та слідчої практики [4, с. 143].

Поняття інформації для аналітичної роботи в органах прокуратури формулює, зокрема, Є. М. Блажівський. Під такою інформацією він розуміє дані, що відображають дійсність про злочинність і правопорушення, будь-які інші дані, які свідчать про організацію роботи правоохоронної системи, у тому числі прокуратури. Сукупність якісних і кількісних характеристик цих явищ в їх єдності і розвитку

Інформація, яку використовує прокурор у практичній діяльності, має низку особливостей, що дає можливість говорити про її специфічність. Інформаційно-аналітична робота, яка здійснюється працівниками органів прокуратури з метою оперативного прийняття належно виважених управлінських рішень, передбачає використання лише актуальної інформації, отриманої у передбачений законом спосіб. Необхідним є також використання даних, наданих відповідними контролюючими піднаглядними прокуратурі органами, а також відомостей, що надійшли безпосередньо від громадян [5, с. 116].

На думку С. С. Єсімова, інформаційно-аналітична робота представляє постійний процес збору, обліку, накопичення, обміну інформації (інформаційне забезпечення) і її логічної обробки: з'ясування, узагальнення, оцінки, побудови висновків і пропозицій (аналітичне забезпечення) [6, с. 190].

Зміст інформаційно-аналітичної роботи складається з цілеспрямованих і взаємозалежних дій з обробки інформації, виконуваних на основі практичного досвіду, професійних знань і здорового глузду, спрямованих на досягнення поставлених цілей.

Метою інформаційно-аналітичного забезпечення в прокуратурі є підвищення ефективності діяльності прокуратури і її підрозділів. Ефективність прокурорського нагляду в значній мірі залежить від організації перевірки та ступеня інформованості прокурора про стан законності.

Особливості інформаційно-аналітичного забезпечення управлінської діяльності органів прокуратури як механізму ефективної взаємодії органів державної влади з інститутами громадянського суспільства, які полягають, перш за все в функціонуванні каналів зворотного зв'язку з населенням для розвитку можливостей особистої участі громадян в державному управлінні та інформуванні населення про основні напрями діяльності органів влади.

Література:

4. Ковалів М. В., Стахура І. Б. Особливості адміністративно-правового статусу органів виконавчої влади. Вісник Національного університету «Львівська політехніка». Юридичні науки. 2014. № 807. С. 22-26.
5. Про Цілі сталого розвитку України на період до 2030 року : Указ Президента України від 30.09.2019 р. № 722/2019. Законодавство України. URL.https://zakon.rada.gov.ua/laws/show/722/2019#Text
6. Тогобіцька-Громова А. А. Керівник в органах прокуратури: адміністративно-правовий статус: дис. … канд. юрид. наук.: 12.00.07. Суми, 2019. 226 с.
7. Прокурорське право: навчальний посібник / Г. Д. Борейко, О. М. Броневицька, Ю. О. Лісіцина, В. В. Луцик, В. В. Навроцька, І. Р. Серкевич, Б. М. Телефанко; За заг. ред. В. В. Луцика. Львів: ЛьвДУВС, 2019. 640с.
8. Блажівський Є. М. Значення інформації у діяльності органів прокуратури України. Науково-інформаційний вісник право. 2013. № 7. С. 115-119.
9. Єсімов С. С. Інформаційно-аналітична діяльність МВС України як об’єкт правового регулювання. Науковий вісник Львівського державного університету внутрішніх справ. серія юридична. 2017. Випуск 1. С. 184-195

Рудік Г. С.,
Здобувач вищої освіти Дніпропетровського державного університету внутрішніх справ

Станіна О. Д.,
доцент кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ, кандидат технічних наук

КІБЕРБЕЗПЕКА ЯК МІРА СОЦІАЛЬНОЇ СВІДОМОСТІ

Сьогодні Інтернет є відображенням загальних тенденцій інформаційної революції кінця XX – початку XXI ст. В процесі свого розвитку «світове павутиння» перетворилося на глобальну комерційну інфраструктуру інформаційного обміну, побічним ефектом чого стало те, що в результаті все частіше підвищується небезпека злому систем, мереж та пристроїв простої людини чи цілої компанії кіберзлочинцями.

Останні кілька років стали періодом надзвичайно швидких та масштабних змін у галузі кібербезпеки. Сьогодні впровадження ефективних заходів безпеки всередині Інтернет-мережі особливо важкий та водночас надважливий процес, оскільки пристроїв стає все більше, а методи атак, які застосовують хакери, – все різноманітніше.

Науковці зазначають [1], що Інтернет-простір став частиною повсякденного життя і перестав бути чимось унікальним, і тим самим ускладнюється можливість регулювати та захищати всі інформаційні дані. Сьогодні треба вивчати специфіку та характеристики кіберпростору, що дасть змогу державам захистити свої національні кордони. Тому простір «світового павутиння» – це специфічне середовище, яке функціонує завдяки телекомунікаційній інфраструктурі в кожній окремо взятій країні.

Численні дослідження показали [1-3], що питання захисту та врегулювання інформаційних технологій набувають актуальності у зв'язку з тим, що їх використання стало відображенням глобалізації. Феноменальний успіх сучасних систем призводить до широкого використання можливостей, що надаються Інтернетом в багатьох державах. Завдяки цьому розширюється та змінюється географія та аудиторія інтернет-користувачів, що, власне, приваблює дедалі більше кіберзлочинців.

Так, серед найбільш розповсюджених видів інформаційних правопорушень науковці виділяють наступні:

1. Соціальна інженерія – психологічне маніпулювання задля здійснення певних неправомірних дій. Соціальну інженерію зловмисники використовують, щоб змусити людину розкрити конфіденційну інформацію. Кіберзлочинці можуть попрохати зробити грошовий переказ або надати доступ до конфіденційних даних. Сюди ж слід віднести фішинг - відправлення фальшивих електронних листів, які схожі на повідомлення від надійних адресатів. Цей вид шахрайства найпоширеніший серед кібератак. Стратегія європейських країн передбачає захист від фішингу за допомогою навчання користувачів або блоку шкідливих електронних листів.
2. Віруси або «мальваре» (malware, malicious software), за допомогою яких можна вимагати гроші, блокувати доступ до файлів чи комп'ютерних систем тощо. «Мальваре» може використовуватися також для спланованих DDoS-атак чи, наприклад, майнінга криптовалют.
3. Протиправний контент. Сюди відноситься контент насильницького характеру, пропаганда тероризму, злочинності, расизму та ненависті. На відміну від перших двох типів правопорушень, цей тип інформаційного злочину в першу чергу діє на соціально-психологічний стан суспільства, а потім вже опосередковано - на безпеку держави та її громадян.

На думку таких дослідників, як Трофіменко О. Г. і Прокоп Ю.В [2], для того щоб регулювати інформаційні технології та захистити дані користувачів від кіберзагроз, потрібно управляти Інтернетом на правовому рівні та мати відповідні просвітянські програми. Дослідник Когут Ю.І. зазначає [3], що лідери багатьох держав вже сформулювали найважливіші проблеми, які вимагають свого подальшого рішення на міжнародному рівні, а саме: адміністративне управління зоною Інтернету; порядок присвоєння мережевих IP-адрес та розподілу адресного простору; уточнення порядку приєднання інформаційних та телекомунікаційних мереж на міжнародному рівні та їх взаємодія; стабільність та безпека глобальної мережі та її користувачів; запобігання протиправному поширенню інформації в Інтернеті, включаючи спам; забезпечення основних прав і свобод людини при використанні Інтернету, включаючи, насамперед,

свободу слова та висловлювання своєї думки; захист інформації та права на недоторканність приватного життя; дотримання прав споживачів при наданні мережевих послуг.

Таким чином, Інтернет створювався і розвивався як технологічна система інформаційного обміну між особами, що передають та одержують інформацію за різними маршрутами, використовуючи одну й ту саму мережу. Інтернет – це «технічний винахід» людства, який об'єктивно вимагає технічної підтримки та технологічного забезпечення функціонування його інфраструктури. Сьогодні питання кібербезпеки стає особливо гострим в результаті розповсюдження все нових інформаційних технологій та систем. Тому індивідуальна кібербезпека як складова інформаційної безпеки держави напряму залежить від свідомого використання електронних пристроїв кожної окремо взятої людини.

На жаль, найчастіше без спеціальної освіти буває важко відрізнити реальні загрози від вигаданих. Ризики кібератак зростають, проте вивчення способів та методів кіберзахисту – для зниження та запобігання таких атак в мережі Інтернет – допомагає забезпечити необхідну безпеку всередині «світового павутиння». І вже давно не секрет, що повсякмісна освіта та навчання звичайних громадян в сфері комп'ютерної безпеки разом дають змогу державі ставати завидно сильною та захищеною від зовнішніх (та й внутрішніх) нападів недоброзичливців.

Література:

1. Дубов, Д., Олексюк, Л., Потій , О., Семенченко , А. Функціонування експертної ради інформаційної та кібербезпеки як демократичний інноваційний інструмент державно-приватної взаємодії. Науковий вісник: Державне управління, (2(8), 92–110. URL: https://doi.org/10.32689/2618-0065-2021-2(8)-92-110
2. Трофіменко О. Г., Прокоп Ю.В. Кібербезпека України: аналіз сучасного стану. Захист інформації. 2019. № 3. С. 154-156.
3. Когут, Ю. І. Кібертероризм (історія, цілі, об'єкти): практичний посібник. Київ: Сідкон, 2021. 304 с.

Савайда О. І.,
доцент кафедри теорії права, конституційного та приватного права Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент

ІНФОРМАЦІЙНА ОСВІДЧЕНІСТЬ ПРАЦІВНИКІВ ПРАВООХОРОННИХ ОРГАНІВ

За чисельної кількості інформації в сучасному суспільстві, логічно постає питання про її доцільність, відповідність, правдивість та достовірність. Особливо, ці принципи інформаційної сфери, як ніколи, актуальні для правовохоронної системи, як елементу виконавчої гілки влади держави та для розуміння та усвідомлення сучасної інформаційної війни, яка відбувається на теренах (інформаційних зокрема) нашої держави.

Інформаційна складова в діяльності правоохоронних орнагів посідає вагоме місце серед інших повноважень та зобовязань вказаної системи.

Як відомо, інформаційна сфера діяльності людини зараз набуває значних оберті та швидкісного розвитку, і не має жодної сфери діяльності особи, яка б так чи інакше не використовувала в своїх процесах життя інформацію та інформаційні елементи, методи та засоби. Всі ці стуктурні елементи інформаційної сфери лише покращують життєдіяльність людини, проте, вміле та вдале використання інформації може приводити як до позитивних так і до негативних наслідків.

Й тому, постає питання про освідченість людини, особи, і зокрема правовохоронця у вмілому та правильному трактувані (спийнятті) інформації та використані її в своїй професійній діяльності.

За швидкісним та плиним розвитком суспільних відноситн, є накопичення та нагромадження значної кількості інформаційного матеріалу, який повинен вдало бути особою розподілений та застосований. В правоохороній діяльності фахівець (а він в своїй діяльності зіштовхується з різними видами порушень, правопорушень, злочинів тощо) повинен як мінімум володіти обізнаністю (володіти відповідною інформаційною складовою про розвязання суспільного конфлікту) та вдало усвідомлювати, розуміти, використовувати правильну, відповідну інформацію щодо вчинення того чи іншого діяння.

Вся система правоохоронних органів так чи інакше побудована на інформаційному просторі. Адже, першопочатково (наприклад, повідомлення до чергової частини, на гарячу лінію поліції), інформація, яка приходить до правоохоронної структури повинна бути правильно та відповідно до закону кваліфікована, а це свідчить про інформаційну освідченість правоохоронця.

Ще один акцент, на який ми б хотіли звернути вашу увагу, полягає в тому, що інформаційна освідченість включає в себе значну кількість різних чиників особистості, а саме: рівень інтелекту, психологічні якості людини, освіту, професійні якості тієї чи іншої займанятості в професії в системі правоохоронних органів (мається на увазі, фізичні, інтелектуальні, управлінські, творчі та інші здібності особи).

Безперечно, шо інформаційна освідченість – це головний аспект інформаційної безпеки. Звичайно, інформаційна освідченість стосується не лише систмети правоохоронних органів, але й громадян зокрема. Тому, цей подвійний процес так чи інакше впливає на формування інформаційної безпеки всього суспільства, й держави зокрема. Тільки в тісній співпраці правоохоронної системи з громадянами може відбуватися та функціонувати нормальний правдивий інформаційний простір.

Й, звичайно, захистити свою інформацію (персональну зокрема) може тільки освідчена людина. Тому освідченість громадян та освіченість населення у інформаційних технологіях, осіб та державних працівників - це одна з найбільших потреб сучасного українського суспільства.

Й тому, навчальні заклади (зокрема проведенням наукових заходів, які більш детально досліджують інформаційний простір та впровадженням інформаційних курсів, різноманітних навчальних заходів) безпосередньо, допомагають підвищувати цей рівень освіченості інформаційного простору.

Багато змін та роботи в цьому напрямку зараз проводиться в самій стуктурі та системі поліції. Створюються нові структурні підрозділи, які цілеспрямовано працють з інтернет простором, з інформаційною телекомунікацією, із кібер злочинністю, створюються різноманті інтернет канали звязку з різними структурними підрозділами правоохоронної система, що звичайно покращує діяльність правоохоронців та їх взаємозвязок з громадянами.

Всі ці й освітні, й наукові, й практичні заходи та структурні змінии, які відбуваються в правоохоронній системі сприяють підвищеню рівня інформаційної освідченості не лише правоохоронців,

а осіб, суспільства зокрема, адже правоохоронна система покликана забезпечувати безпеку всіх сфер діяльності людини, зокрема й інформаційної. Й інформаційна освідченість (обізнаність) відіграє значну та вагому роль, для того, щоб працівники правоохоронної системи розуміли та увідомлювали значення інформаційного простору для сучасної людини (адже значна частина життя сучасної людини тепер відбувається саме в такій площині) та могли надати кваліфіковану та відповідну допомогу в разі порушення прав та свобод людини та громадянина в інформаційній сфері.

ЛІТЕРАТУРА:

1. https://24tv.ua/ru/informatsiyna_osvita__naygolovnishiy_punkt_informatsiynoyi_bezpeki__kerivnik_derzhinformresursu_n1320100.
2. Karpenko Olena. Media Education as a Component of Reforming Higher Educaton in Ukraine / Olena Karpenko // Media4u Magazine: Proceedings of 10th International Research Electronic Conference Media and Education 2017. Special Issue. P. 59–63

Сапрун А. М.,
здобувач вищої освіти Львівського державного університету внутрішніх справ

Огірко О. І.,
доцент кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів Львівського державного університету внутрішніх справ, кандидат технічних наук, доцент

АНАЛІЗ ВИКОРИСТАННЯ СУЧАСНИХ ТЕХНОЛОГІЙ ВІРТУАЛЬНОЇ ТА ДОПОВНЕНОЇ РЕАЛЬНОСТІ В ОСВІТІ

Використання інформаційних технологій в освіті є актуальною темою, оскільки через пандемією короновірусу (COVID-19), система освіти трансформується та пристосовується до нової моделі освітнього процесу. Сучасні технології – це альтернативний спосіб навчання, додаткова можливість використання чогось нового в навчанні, підвищення інтересу до науки у молоді.

До сучасних інформаційних технології в освіті відносять також віртуальні технології (VR) та технології доповненої реальності (AR), які здатні проектувати цифрову інформацію (зображення, відео, текст, графіку) поза екранами пристроїв та об'єднувати віртуальні об'єкти з реальним середовищем [1]. Ці технології корисні як для викладачів, так і для здобувачів освіти. Використання таких технологій допоможе викладачам привернути увагу своїх слухачів та залучити їх активніше до занять. Використання технологій VR та AR, не тільки зробить навчання більш цікавим та захоплюючим, для здобувачів освіти, але й збільшить можливість глибше вивчати предмети, візуалізувати та аналізувати.

Все більше університетів впроваджують віртуальні технології та технології доповненої реальності в освітній процес. Так, у Державному університеті Північної Кароліни VR використовують під час вивчення біології, та інших природничих наук [3]. Міжнародний Європейський Університет презентував VR - кімнату, яка дозволяє студентам досліджувати місця призначення з усього світу, навіть не покидаючи аудиторію [4]. Сучасна освітня платформа сприяє кращому вивченню та викладанню медичних наук та анатомії на настільних, мобільних та віртуальних пристроях. Королівський коледж хірургів в Единбурзі, також використовує віртуальні технології у навчанні, поміщаючи студентів у простір резус-кімнати, де їм належить вжити заходів, які врятують пацієнта. Проект відтворює ситуацію, типову для молодих лікарів, які лікують пацієнтів зі смертельними травмами [5]. Такий підхід до навчання підвищує ефективність навчання та готує здобувачів до реальних робочих ситуацій.

Згідно дослідження вчених Техаського університету [2, 4-6] використання віртуальних лекцій щороку зростає, як серед слухачів, так і серед викладачів (рис.1).

Так у 2018 році лише 6,1 % слухачів щодня користувалися віртуальними лекціями, 38,3% щомісяця використовували лекції, а 39,1 % слухачів віртуальних лекції взагалі не використовували. Також віртуальні лекції не часто використовували і викладачі, 45,9 % не дали жодної віртуальної лекції.

У 2020 році 35,4% слухачів користуються віртуальними лекціями щодня, а 52,2% – щомісяця, відсоток тих, хто взагалі не користується віртуальними лекціями знизився з 39,1 % до 2,9 %.

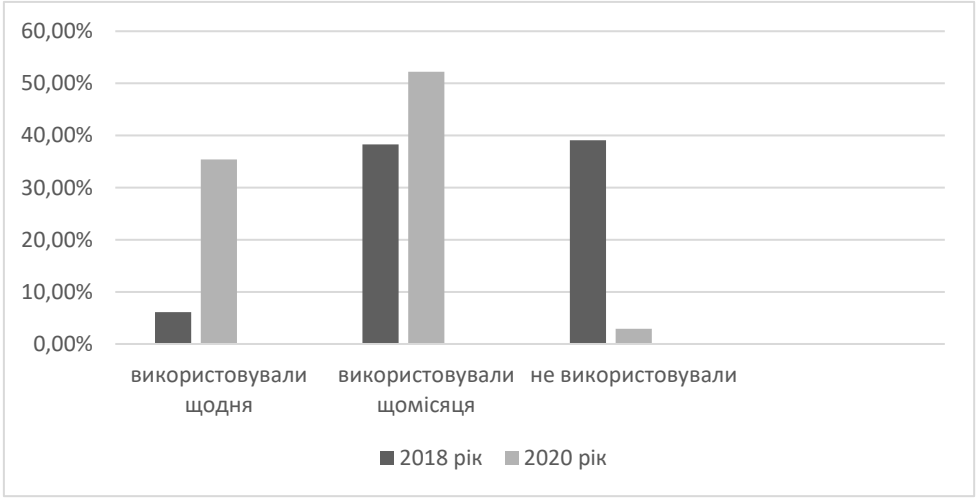

Рис.1 Використання віртуальних лекцій

Використання віртуальних технологій та технологій доповненої реальності, це великий крок вперед в системі освіти. Основними перевагами такого навчання є [1-5]:

- допомога слухачам краще сприймати складну інформацію;
- отримувати нові навички;
- допомога викладачам демонструвати та застосовувати теорію під час заняття;
- захопливий процес навчання, що заохочує молодь до вивчення предмета;
- менша кількість факторів, що відволікають від засвоєння матеріалу.

Освіта з використанням віртуальної реальності дає змогу більш наочно проводити лекції і семінари, тренінги, демонструвати здобувачам всі аспекти реального об'єкта або процесу, покращує якість і швидкість освітніх процесів Технології віртуальної та доповненої реальності дозволяють використовувати те, що людина 80% інформації отримує з навколишнього світу з допомогою зору, при цьому люди запам'ятовують 20% того, що вони бачать, 40% того, що вони бачать і чують, і 70% того, що вони бачать, чують і роблять [7]. У результаті відбувається повне залучення здобувачів у навчальний процес, що підвищує їхню мотивацію й успіхи в отриманні знань.

Впровадження сучасних інформаційних технології в традиційний навчальний процес дають змогу замінити реальні об'єкти їх імітаційними моделями й інтерактивними тренажерами, що дозволяє краще готувати фахівців з різних спеціальностей.

Література:

1. Огірко О. І. Використання вітруальних технології та технології доповненої реальності в освітньому процесі. Інформаційні технології в освіті та практиці: матеріали Всеукраїнської науковопрактичної конференції (Львів, 18 грудня 2020). Львів: ЛьвДУВС, 2020. С. 36-38.
2. Волинець В. Використання технологій віртуальної реальності в освіті. Неперервна професійна освіта: теорія і практика, №2, 2021. С. 40–47. URL: https://doi.org/10.28925/1609-8595.2021.2.5.
3. Віртуальна та доповнена реальність: як нові технології надихають вчитися URL: https://osvitoria.media/opinions/virtualna-ta-dopovnena-realnist-yakoyu-mozhe-buty-suchasna-osvita/
4. Unimersiv: VR Training // Virtual Reality Education URL: https://unimersiv.com/
5. Nearpod: Make every lesson interactive URL: https://nearpod.com/
6. Min-Jeong Choa , Joon Pio Hongb The emergence of virtual education during the COVID-19 pandemic: The past, present, and future of the plastic surgery education. Journal of Plastic, Reconstructive & Aesthetic Surgery 74 (2021) 1413–1421 URL: https://e-tarjome.com/storage/panel/fileuploads/2021-06-26/1624681200_E15479.pdf
7. Трач Ю. VR-технології як метод і засіб навчання. Освітологічний дискурс. 2017. № 3–4, С. 309–322. URL: http://nbuv.gov.ua/UJRN/osdys_2017_3-4_26.

Сеник В. В.,
завідувач кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів Львівського державного університету внутрішніх справ, доцент кафедри обчислювальної математики та програмування Національного університету «Львівська політехніка», кандидат технічних наук, доцент

Ментинський С. М.,
старший викладач кафедри обчислювальної математики та програмування Національного університету «Львівська політехніка»

ДО ПИТАННЯ НОРМАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ ВИКОРИСТАННЯ ХМАРНИХ СЕРВІСІВ В ІНФОРМАЦІЙНОМУ ПРОСТОРІ УКРАЇНИ

Упродовж останніх двох років Україна, як і увесь світ, живе у нових реаліях, які сформувалися внаслідок поширення короновірусної інфекції COVID-19. Зокрема, нові реалії зумовили швидкий розвиток окремих галузей ІТ-технологій, серед яких слід візначити електронну комерцію, технології дистанційного навчання, надання адміністративних послуг он-лайн тощо. У часі загальної діджиталізації, розвитку електронних послуг, виникла потреба у дослідженні, створенні та реалізації різноманітних засобів забезпечення їх надійного функціонування. На вістря вийшли проблеми повязані із забезпеченням кібербезпеки під час проведення комерційних (банківських) операцій, підвищення компютерної грамотності населення, (особливо у напрямі запобіганню шахрайств з використанням компютерних технологій) тощо. Упродовж періоду панування короновірусної інфекції COVID-19 нами проводились дослідження у окремих згаданих напрямах, результати та висновки за якими наведені у роботах [1, 2]. У роботі [2] нами, зокрема, наголошувалося на потребі проведення дослідження нормативно-правової складової забезпечення захисту інформаційних ресурсів, які опрацьовуються засобами хмарних технологій. Тому у даній публікації ми хочемо висловити окремі думки щодо цього питання.

Проблема нормативно-правового регулювання використання хмарних сервісів для України не є новою. У грудні 2019 року групою депутатів внесено до розгляду Верховною Радою України проект Закону України «Про хмарні послуги» [3], яким зпропоновано врегулювати правовідносини, повязані із обробленням та захистом інформації під час використання хмарних технологій. Передбачалось, що прийняття даного закону активізує роботи із використання сучасних інформаційно-телекомунікаційних технологій у суспільстві, дасть змогу забезпечити умови для ефективного використання як приватних, так і держаних інформаційних ресурсів. Однак не дивлячись на на давно назрілу необхідність, на сьогодній день даний, чи альтернативний нормативно-правовий документ не прийнятий.

В результаті затягування прийняття цього та внесення змін до відповідних дійючих нормативно-правових актів призвело до ряду проблем, пов'язаних у тому числі із пандемією, спричиненої короновірусом COVID-19. До таких проблем слід віднести:

- стримування розвитку інформаційно-телекомунікаційних технологій в державі, насамперед у галузі електронного урядування, освітньому процесі, у сфері науки;
- зростання навантаження на різні державні та комерційні структури, у тому числі на структури, які відповідають за захист інформації;
- стримування реформування застарілої ситсеми розподілу регуляторних функцій державних органів влади та органів місцевого самоврядування;
- підвищення витрат на створення та розбудову державними та комерційними структурами власних інформаційних та інформаційно-телекомунікаційних систем;
- затримання у створенні сприятливих умов для ефективної взаємодії між держаними, комерційними та іншими органами, а також у створенні передумов для подальшої інформатизації суспільства, можливості використання сучасних досягнень у галузі інформаційних та інформаційно-телекомунікаційних технологій для підтримання діяльності органів державної та виконавчої влади;
- зростання витрат на оновлення апаратного та іншого інформаційно-телекомунікаційного обладнанння різних державних і комерційних структур;
- стримування розвитку структури та динаміки державних закупівель;
- стримування ринку створення програмного забезпечення для запровадження хмарних сервісів всередені держави тощо.

Таким чином прийняття згаданого нормативно-правового документу дало б змогу врегулювати правовідносини, повязані з обробленням даних з використанням хмарних сервісів, створило б підгрунтя для розвязання вказаних вище проблем. Тобто створило б передумови для використання суб'єктами владних повноважень та державними підприємствами, установами та організаціями новітніх інформаційних технологій та впровадження систем ефективної взаємодії держави та суспільства, дозволило б утворити надійну економічну систему надавачів хмарних послуг всередині країни, стимулювати перехід на хмарну модель більшості секторів української економіки, дало б поштовх до прискореного розвитку ринку розробок програмного забезпечення для внутрішнього ринку, знизило б ризики корупційної складової під час закупівлі за бюджетні кошти.

Для справедливості слід зазначити, що у червні 2020 року Верховна Рада України у першому читанні прийняла проект Закону «Про хмарні послуги». Однак на сьогодні його відсутність гостро відчувається суспільством. Різноманітні державні, а особливо комерційні структури підтримують законопроект «Про хмарні послуги» та закликають Верховну Раду України якнайшвише прийняти даний закон у другому читанні. До цього хочемо долучитися і ми – науковці, та закликати депутатів не стримувати розвиток і впровадження IT-технологій у державі, створити подальші умови для їх розвитку на теренах України.

Література:

1. Шинкарук О. М., Сеник В. В., Зачек О. І., Магеровська Т. В. Стан та особливості протидії кіберзлочинності в Україні в умовах пандемії COVID-19. Соціально-правові студії. 2021. Випуск 3 (13). С. 68–76.
2. Сеник В. В., Ментинський С. М, Кулешник Я. Ф. Стан та перспективи розвитку технологій захисту хмарних сервісів / Економічна та інформаційна безпека: актуальні питання та інновації: міжнародна науково-практична конференція. Дніпро. 04 листопада 2021.
3. Про хмарні послуги : Закон України (проект) URL: http://search.ligazakon.ua/l_doc2.nsf/link1/JI01021A.html

Старушко О. Б.,
здобувач вищої освіти Дніпропетровського державного університету внутрішніх справ

Прокопов С. О.,
старший викладач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ

ШЛЯХИ БОРОТЬБИ З КІБЕРБУЛІНГОМ

У 21 столітті Інтернет став однією з частин нашого оточення. З одного боку, це засіб розвитку знань та комунікативних навиків, а з іншого підвищений ризик зіткнення з певними загрозами. Зокрема, Інтернет-середовище та новітня технологія, яка створює можливість для поширення нового виду насильства – кібербулінг, яким найчастіше страждають діти та підлітки, вони найактивніші користувачі. Особливо цьому сприяють неконтрольовані використання змісту та відсутність або слабка сформованість критичного мислення. [1]

Кібербулінг- це одна із форм агресії. Вона передбачає певні жорстокі дії які завдають шкоди особі, принижують людську гідність за допомогою інформаційних засобів. Такими засобами можуть бути мобільний телефон, соціальні мережі, різні електронні пошти.[4]

Кібербулінг є одним із нападів на особу через мережу Інтернет. Основною метою є нанесення шкоди, які можуть здійснюватися через повідомлення в чати, фотографії чи відеофайли які миттєво розповсюджуються. Найбільшою проблемою є те, що діти можуть стикатися з небезпекою не тільки в навколишньому середовищі, а також у віртуальному просторі.

Багато підлітків стали жертвами знущань з боку своїх однокласників, які знімають принизливі відео та без дозволу розміщують в Інтернет, де їх можуть побачити мільйони людей. Нажаль, досить багато випадків суїциду через кібербулінг, спрямований на розповсюдження неправдивих чуток, образливі текстові повідомлення.

Для ефективної роботи по забезпеченню безпеки дітей в мережі Інтернет та усунення загроз для їх нормального розвитку, виникає необхідність у створенні новітнього сучасного інструменту – безпечного Інтернет ресурсу (мобільного додатку). Проект «My safety friends» – це вся програма побудови додаткової сучасної прийнятої комунікації громадою, службою у справах дітей та сім'ї, ювенальною поліцією, навчальними закладами, державними та неурядовими організаціями, а також дитиною та її батьками (опікунами) для обміну українськими необхідними інформація та допомога. Інтернет ресурс «My safety friends» (рис.1) зменшить кількість фактів булінгу, дозволить дітям знайти відповіді на всі актуальні питання під час дорослішання, отримати інформацію про цікаві дитячі заходи, акції, вікторини, конкурси, тощо, обмінюватися інформацією та мати всі останні новини, як серед друзів, так і в суспільстві. [2]

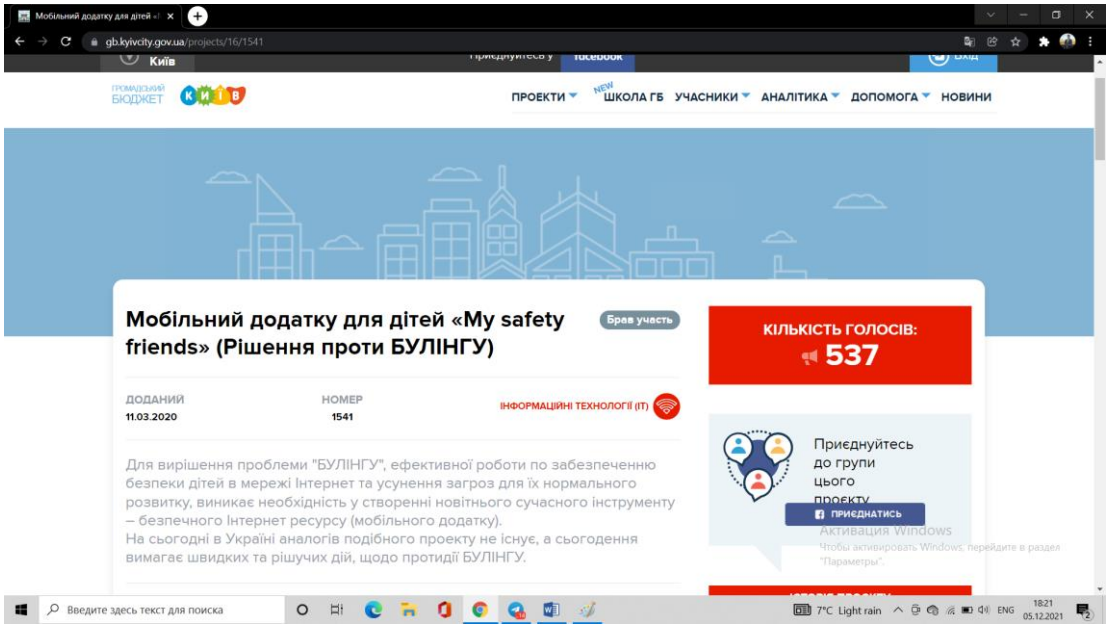

Рис.1. Загальна форма Інтернет ресурсу «My safety friends»

Для зменшення випадків булінгу створили різноманітні чат-боти, які є комп'ютерними програмами, розроблені на основі нейромереж і новітніх технологій, яка веде бесіду за допомогою слухових або текстових методів. Чат-боти використовуються в діалогових системах для різних практичних цілей, включаючи обслуговування клієнтів або отримання інформації. Вони створені для загального доступу, але деякі з них зберігають важливу інформацію, за допомогою якої поліцейські можуть отримувати інформацію про особу, його зв'язки або об'єкт посягання практично миттєво. Найбільш запроваджених чат-ботів розміщено в TELEGRAM, тому, що в ньому найбільш ефективно реалізовано його функції.

Одним із таких є чат-бот «KidsPolice» (рис.2) розроблено на базі месенджера Telegram, щоб діти та їхні батьки могли отримати не лише найбільш вичерпну інформацію про роботу ювенальної поліції, а й підтримку та оперативну допомогу. За допомогою цього боту можна знайти велику кількість інформації про те, як проявляється кубербулінг, що робити якщо саме ти став жертвою. В ньому можна дізнатися, як видалити самостійно принизливі матеріали із мережі Інтернет.[3]

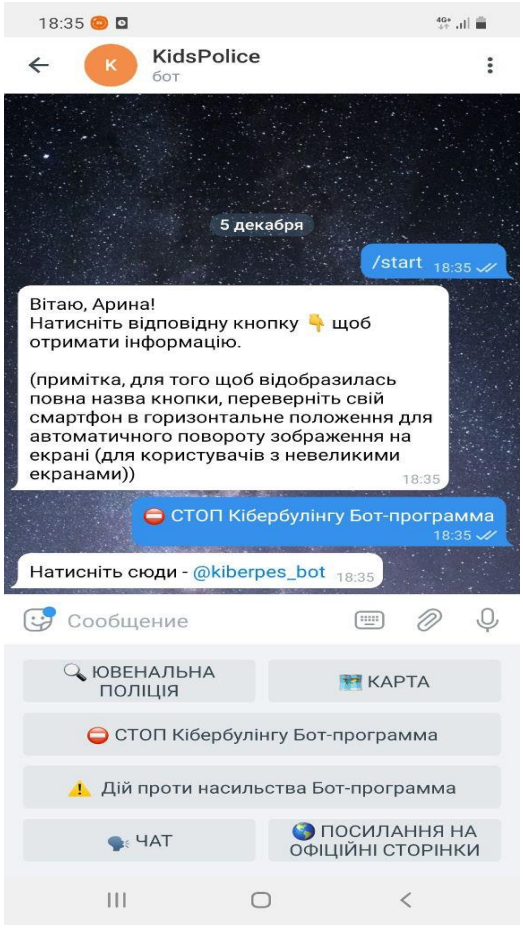

Рис.2. Загальна форма чат-боту «KidsPolice»

Щоб увійти до чат-боту, необхідно відсканувати спеціальний QR-код або знайти KidsPolice у "Телеграм" і натиснути кнопку "Розпочати". Після цього з'явиться меню з шести пунктів. Тут ви знайдете інформацію про те, як діяти батькам, дітям та вчителям у випадку кібербулінгу, як самостійно видалити образливі матеріали із соціальних мереж та куди звертатись по допомогу.[3]

У розділі «Ювенальна поліція» можна знайти поліцейського, який служить на вашій території, зателефонувати йому або написати особисте повідомлення.

У розділі «Карта» можна отримати геолокацію найближчого поліцейського відділу.

У розділі «ЧАТ» можна буде долучитися до обговорення різних питань із іншими учасниками.

Отже, на підставі зазначеного, можна зробити висновок, для того щоб не бути жертвою кібербулінгу, потрібно дотримуватися певних правил. При заході або реєстрації на різних сайтах не треба писати особисту інформацію, вказувати номер мобільного телефону, номер пошти та адрес проживання. Вмикати лише веб-камеру при спілкуванні з друзями або родичами. Всі випадки агресії та знущань в мережі Інтернет треба ігнорувати, то для того, щоб припинити кібербулінг на ранній стадії. Для зменшення

випадків кібербулінгу в нашій країні створили чат-боти «KidsPolice» та «My safety friends» на базі месенджеру «TELEGRAM», щоб діти та батьки змогли отримати не лише найбільш вичерпну інформацію про роботу ювенальної поліції, а також про їх допомогу в таких випадках.

Література:

1. Щигельська Г. О Що таке кібербулінг та як з ним боротись? URL:
2. http://elartu.tntu.edu.ua/bitstream/lib/25145/2/MSNK_2018v2_Hoi_V-What_is_cyberbullying_and_how_170-171.pdf
3. Мобільний додаток для дітей «My safety friends» (Рішення проти БУЛІНГУ) URL: https://gb.kyivcity.gov.ua/projects/16/1541
4. Поліція запровадила для дітей чат-бот «KidsPolice» URL: https://rivnepost.rv.ua/news/politsiya-zaprovadila-dlya-ditey-chatbot-kidspolice
5. Закон України Про внесення змін до деяких законодавчих актів України щодо протидії булінгу (цькуванню) (Відомості Верховної Ради (ВВР), 2019, № 5, ст.33) URL: https://zakon.rada.gov.ua/laws/show/2657-19#Text

Сьома І. Б.,
здобувач вищої освіти Львівського державного університету внутрішніх справ

Д'яков А. В.,
доцент кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів Львівського державного університету внутрішніх справ, кандидат технічних наук

КВАНТОВІ КОМП'ЮТЕРИ, ЯК НОВИЙ ЕТАП РОЗВИТКУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Інформаційні технології сьогодні займають одно з головних місць в житті людства. Винахід та розвиток друкарства, використання пошти, телефону та телеграфу стали визначними відмітками розвитку інформаційних технологій та відіграли ключову роль в інформатизації сучасного суспільства.

Враховуючи той факт, що під інформатизацією суспільства розуміють реалізацію комплексу заходів, спрямованих на забезпечення повного та своєчасного використання членами суспільства достовірної інформації, що значною мірою залежить від ступеня освоєння та розвитку нових інформаційних технологій, можна сказати, що їх розвиток безпосередньо пов'язано із розвитком технологічної бази.

Матеріальною та технологічною базою інформаційного суспільства є різного роду системи на базі комп'ютерної техніки та комп'ютерних мереж, інформаційної технології, телекомунікаційного зв'язку. Тенденції розвитку сучасних інформаційних технологій визначають постійне зростання складності програмного та апаратного забезпечення комп'ютерних технологій

З розвитком теорії квантової механіки, розроблялися принципи та основи створення нового типу обчислювальних машин, які дозволяють вирішувати деякі завдання, недоступні навіть найпотужнішим сучасним суперкомп'ютерам. При цьому різко зростає швидкість багатьох складних обчислень; повідомлення, надіслані лініями квантового зв'язку, неможливо ні перехопити, ні скопіювати. Обчислювальний пристрій, що використовує явища квантової механіки для передачі й обробки даних назвали квантовим комп'ютером.

Основна відмінність квантового комп'ютера від класичного полягає в поданні інформації. Класичний комп'ютер працює на основі транзисторів та кремнієвих чіпів, які використовують для обробки інформації бінарний код, що складається з нулів та одиниць. Біт, як мінімальна одиниця інформації, має два базові стани: 1 і 0. Зміни цих станів можна легко контролювати: об'єкти можуть або перебувати в конкретному місці, або – не знаходиться. Саме тому багато фізичних об'єктів зовнішнього світу можна перенести у віртуальний за допомогою складних комбінацій бітів.

Робота квантового комп'ютера ґрунтується на принципі суперпозиції, а замість традиційних одиниць виміру бітів використовуються кубіти (квантові біти), які одночасно можуть перебувати у різних станах (в 1 і 0 одночасно), за рахунок цього квантові комп'ютери для певних класів завдань у мільйони разів потужніші за звичайні. З'явився вираз «квантова перевага» (Quantum supremacy): класичний комп'ютер проводить обчислення послідовно, перебирає варіанти один за одним, квантовий може вирішувати багато завдань одночасно.

Сьогодні вже описані десятки різних алгоритмів роботи квантового комп'ютера, розробляються спеціальні мови програмування.

З головних новітніх технологій реалізації квантового комп'ютера слід виділити:

- твердотільні квантові точки на напівпровідниках: в якості логічних кубитів використовуються або зарядові стани (знаходження або відсутність електрона в певній точці), або напрям електронного та/або ядерного спина в даній квантовій точці. Управління через зовнішні потенціали чи лазерним імпульсом;
- напівпровідні елементи (джозефсонівські переходи, СКВІД та ін). В якості логічних кубитів використовуються присутність/відсутність куперівської пари в певній просторовій області. Управління: зовнішній потенціал/магнітний потік;
- змішані технології: використання заздалегідь приготованих заплутаних станів фотонів для керування атомними ансамблями або як елементи керування класичними обчислювальними мережами;

- оптичні технології: використання генерації квантових станів світла, швидкого та переналаштовуваного управління цими станами та їх детектування.

Квантові комп'ютери (і програми для них) ґрунтуються на зовсім іншій моделі світу. У класичній фізиці стан об'єкта чітко визначений. У світі квантової механіки визначити стан квантового об'єкта може лише спостереження. До цього моменту стан об'єктів та взаємозв'язок між ними інтерпретуються лише ймовірнісно.

Таким чином, враховуючи принципово нову фізичну реалізацію, якісно нові підходи до процесів обробки інформації, застосування нової системи обчислення, можна зробити висновок, що квантовий комп’ютер – це принципово нова система, яка відрізняється від існуючих в самому фундаменті, фізичних основах, на яких він працює.

Виходячи з цього можна стверджувати, що квантовий комп’ютер ознаменував початок нового етапу розвитку інформаційних технологій та комп’ютерної техніки.

Федчак І.,
доцент кафедри оперативно-розшукової діяльності Львівського державного університету внутрішніх справ кандидат юридичних наук, доцент

Корпан В.,
Здобувач вищої освіти Львівського державного університету внутрішніх справ

ОСОБЛИВОСТІ СКЛАДАННЯ ПСИХОЛОГІЧНОГО ПОРТРЕТА СЕРІЙНОГО ВБИВЦІ ТА РОЗКРИТТЯ ЙОГО ПСИХОЛОГІЧНИХ ОСОБЛИВОСТЕЙ

Феномену серійних вбивств приділяють дедалі все більшу увагу, зокрема питанню складання психологічного портрета. Тема залишається не досить розробленою, оскільки в Україні є лише кілька відомих випадків психологічного портретування.

Актуальність дослідження полягає у тому, що при розслідуванні злочинів з прихованою мотивацією є випадки коли відсутні відомості про осіб, які вчинили злочин. Відсутність такої інформації в слідчій діяльності дозволяє компенсувати психологічний аналіз злочину та особи, яка його вчинила. Тому виявлення вказаних психологічних особливостей нерідко відіграє вирішальне значення. Саме дослідження особистості та психологічного портрета серійного вбивці й дозволяє покласти в основу криміналістичних версій і напрямів розслідування та ефективного розшуку таких осіб [1].

У різні часи проблемами методики розслідування вбивств займалися такі вчені, як Ю.М. Антонян, Б.Л. Гульман, В. Ісаєнко, В.О. Коновалова, В.В. Новик, В.А. Образцов, О.С. Саінчин, В.Л. Сінчук, А.В. Старушкевич, Б.В. Шостакович. Проте такі важливі для практики питання як визначення поняття серійних вбивств, їх класифікація та відповідна характеристика маніяків є на даний час недостатньо дослідженими.

Етапами розробки ПКПЗ є:

1. Складання криміналістичної інформаційної моделі події злочину.
2. Ситуаційне моделювання (моделювання поведінки).
3. Інтерпретація через психологічне пояснення поведінки злочинця (діагностичний рівень);
4. Оформлення вивідної інформації про ознаки особистості злочинця в психологічному портреті.

На першому етапі розробки ПКПЗ (складання криміналістичної інформаційної моделі події злочину) – збирається і аналізується інформація про особу злочинця та події, які містяться в можливих її носіях. Другий етап побудови ПКПЗ (ситуаційне моделювання (моделювання поведінки) – включає у себе психологічні прийоми виявлення «індивідуальної дії» злочинця. Третій етап побудови ПКПЗ (Інтерпретація через психологічне пояснення поведінки злочинця (діагностичний рівень). Прийом психологічної інтерпретації поведінки злочинця (індивідуальних дій). Четвертий етап ПКПЗ (оформлення вивідної інформації про ознаки особистості злочинця в психологічному портреті).

Необхідність у розробці психологічного портрета злочинця свіжа, в першу чергу, при розслідуванні певної категорії неочевидних злочинів, а саме: вбивств на сексуальному ґрунті з ознаками садистського катування жертви; убивств з посмертними колотими і різаними пораненнями; безмотивних підпалів і вибухів; зґвалтувань тощо. У цьому випадку пошук ознак злочинця здійснюється найчастіше тільки виходячи зі слідів і обставин злочину. Їх психологічний аналіз у рамках методики складання психологічного портрета злочинця здатний ініціювати продуктивні версії за його ознаками, які дозволяють звужувати коло розшуку осіб, а також виявляти винного серед осіб, які потрапили в поле зору слідства.

Для того щоб зрозуміти злочинну поведінку людини, необхідно проникнути глибоко в його психологію, тобто скласти психологічний портрет злочинця. Існує декілька видів його складання: британський, у якому основна увага приділяється поведінці злочинця, виявленим доказам на місці злочину; американський підхід до складання психологічного портрета злочинця базується на статистичних даних, на підставі яких потім дається оцінка особи злочинця, місця і способу його життя.

Особистість злочинця визначають як сукупність соціально-психологічних властивостей і якостей людини, що є причинами і умовами вчинення злочинів та містить також особливості кримінологічного і криміналістичного характеру. В цілому особистість злочинця можна охарактеризувати як своєрідну модель, соціальний і психологічний портрет, який наділений специфічними рисами.

Доведено, що злочинці відрізняються від осіб, які вчиняють злочини, характерними психологічними особливостями, які і визначають їх злочинну діяльність. Злочинці, як правило, незадоволені становищем у суспільстві, соціально непристосовані. Вони імпульсивні, що впливає на

спонтанність їх дій, необдуманих вчинків. Злочинці, як правило, не здатні встановлювати контакт з оточуючими, не можуть дивитися на ситуацію з позиції іншого, занурені в себе, замкнуті та агресивні. [3]

Без сумніву більшість серійних вбивць характеризуються підвищеним інтелектуальним потенціалом, проте дані характеристики не пояснюють як можна вести подвійне життя досить довгий час. Іншими словами «маска нормальності» не може бути пояснена усвідомленими хитрощами зі створенням злочинцем собі позитивного іміджу, так як подібні спроби рано чи пізно стануть зрозумілими оточуючим людям.

Немає жодної обґрунтованої теорії, яка б свідчила про наявність взаємозв'язку між професією і злочинною поведінкою, властивою серійним вбивцям. Насправді, такі злочинці зазвичай зустрічаються там, де їх найменше очікують зустріти, тому вони і є одними з найнебезпечніших. Наприклад, велика кількість «серійних вбивць» є лікарями. Провину цих людей надзвичайно складно довести, так як у них є доступ до складних і слабо розпізнаваним отрут, а також вони є дипломованими фахівцями, які володіють анатомічними знаннями. Жертвами серійних вбивць з медичною освітою нерідко стають їх пацієнти. Мотивом може служити особисте збагачення і так зване вбивство з милосердя тяжкохворої людини. Найвідомішими лікарями - серійними вбивцями є Гарольд Шипман (Англія), Джон Бодкін Адамс (Англія), Дональ Харві (США) і ін. [5].

Виходячи з наведеного, першочергове значення при розслідуванні серійних вбивств та інших неочевидних злочинів має встановлення осіб, які вчинили ці злочини. Виявлення зазначених осіб забезпечується оперативністю та своєчасністю реакції на такі заяви; коректною і тісною взаємодією працівників правоохоронних органів з іншими органами державної влади, а також спеціалістами та експертами; якісним проведенням слідчих та інших необхідних процесуальних дій на місці вчинення злочину; максимально повним використанням сил і засобів усіх служб і підрозділів органів внутрішніх справ, які беруть участь у процесі розслідування злочинів. Важливим пунктом є здійснення глибокого аналізу вихідної інформації для побудови слідчих і розшукових версій та значенні комплексу заходів щодо їх перевірки, активного використання для встановлення причетності до злочину криміналістичних обліків, широким застосуванням науково-технічних засобів.

Підсумовуючи, слід зазначити, що проблемі наукових розробок у галузі складання та використання психологічного портрета злочинця в Україні у процесі розслідування злочинів загалом та серійних зокрема приділяється недостатньо уваги. Найбільш суттєвою перешкодою у розвитку даного напряму і широкого застосування психологічного портрета у практиці розкриття злочинів є специфіка об'єкта дослідження, що носить міждисциплінарний характер і має складно опосередковану детермінацію. При цьому основна проблема розробки психологічного портрета невстановленого злочинця в тому, що основне завдання полягає в поєднанні криміналістичних ознак, які є матеріальними (об'єктивними) з психологічними ознаками особи злочинця, що є суб'єктивними та не завжди зовнішньо спостерігаються в елементах злочинної поведінки.

Необхідно розробити відповідні методичні рекомендації по боротьбі із серійними вбивствами; змоделювати комплексний зразок побудови типового криміналістичного портрета серійних вбивць для користування при розслідуванні; ввести у навчальні програми з криміналістики навчальних закладів вивчення окремих вузькопрофільних тем, що стосуються криміналістичного моделювання психологічних портретів злочинців.

Література:

1. Горлова О. Ю. Особистість та психологічний портрет серійного вбивці. О.Ю. Горлова. International Scientific Journal "Internauka" http://www.inter-nauka.com/ https://www.inter-nauka.com/uploads/public/15423575291229.pdf.
2. Користін О.Є. Тактичний кримінальний аналіз: теорія та практика; навчальний посібник / О.Є. Користін, Н.П. Свиридюк та ін. ДНДІ, ОДУВС. Одеса: РВВ ОДУВС, 2019. 216 с.
3. Кудрявцев В.Н., Эминов В.Е. Криминология: Учебник. – М. : Норма, 2009. – С. 153.
4. Меднов М.Р. Криминологическая характеристика серийных убийств, проблемы и перспективы развития / Отеч. юриспруденция. – 2016. – № 12. – С. 40-43.
5. Психологический портрет личности серийного убийцы URL: http://www.serialkillers.ru/

Шабатура Ю. В.,
завідувач кафедри електромеханіки та електроніки Національної академії сухопутних військ імені гетьмана Петра Сагайдачного, доктор технічних наук, професор

Смичок В. Д.,
доцент кафедри електромеханіки та електроніки Національної академії сухопутних військ імені гетьмана Петра Сагайдачного, кандидат технічних наук, доцент

Атаманюк В. В.,
заступник завідувача кафедри електромеханіки та електроніки Національної академії сухопутних військ імені гетьмана Петра Сагайдачного, кандидат технічних наук, доцент

Міхалєва М. С.,
професор кафедри електромеханіки та електроніки Національної академії сухопутних військ імені гетьмана Петра Сагайдачного, кандидат технічних наук, доцент

Тихоміров Д. А.,
курсант Національної академії сухопутних військ імені гетьмана Петра Сагайдачного

ОЦІНКА ОСНОВНИХ АСПЕКТІВ УРАЖЕННЯ ВОРОЖОЇ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СТРУКТУРИ І ЗБЕРЕЖЕННЯ ВЛАСНОЇ ЗА УМОВ ВИКОРИСТАННЯ ЕЛЕКТРОМАГНІТНОЇ ЗБРОЇ

У сучасному світі інформація відіграє надзвичайно велику, практично вирішальну роль в усіх процесах діяльності людей. Про інформацію в наш час прийнято говорити як про стратегічний ресурс суспільства, який визначає рівень розвитку будь-якої держави, її економічний потенціал, положення у світовій спільноті. Відповідно до цього, технічні і програмні засоби, які забезпечують створення інформації в електронному вигляді, її обробку, накопичення, збереження, передачу, поширення, відображення і т.д. є надзвичайно важливими елементами інфраструктури, яка є життєво необхідною для існування сучасного суспільства. Водночас ця інфраструктура є достатньо уразливою, причому як на фізичному так і на програмному рівнях, а тому задачі її захисту і оцінки уразливості є надзвичайно важливими і актуальними для сьогодення.

Як показав досвід військових конфліктів останніх років електромагнітна зброя уже реально існує і стоїть на озброєнні у багатьох арміях світу. Як правило вона застосовується перед проведенням активних військових дій. Наслідком її застосування стає повне виведення з ладу усіх радіоелектронних систем у визначеному радіусі дії. В тому числі знищуються усі інформаційні і телекомунікаційні структури та засоби зв'язку. Однак, потрібно зазначити, що вперше людство зустрілось з штучно викликаним явищем потужного електромагнітного імпульсу, який виводив з ладу не лише засоби зв'язку але і електроенергетичні системи, після проведення американцями висотного ядерного вибуху над атолом Джонстон в північній частині Тихого океану 1 серпня 1958 року. Внаслідок даних випробувань на Гавайських островах розташованих на віддалі в 717 морських миль було порушено електропостачання, а радіозв'язок було втрачено на величезній території аж до узбережжя Австралії.

Масштабність штучно викликаного явища зумовила початок активних досліджень направлених на розробку неядерних боєприпасів здатних створювати надпотужні електромагнітні імпульси. Основоположником створення теорії використання потужної механічної і теплової енергії, яка виділяється в процесі вибуху, для створення електромагнітних імпульсів став учений-фізик Андрій Сахаров. На основі запропонованої ним теорії були розроблені вибухомагнітні генератори, які здатні генерувати надпотужні імпульсні магнітні поля. Дещо пізніше ці генератори були доповнені в результаті чого вони стали здатними генерувати надпотужні струми, тобто створювати електромагнітні імпульси. Ці роботи стали основою для розробки повноцінних електромагнітних боєприпасів у вигляді ракет, бомб, снарядів та мін, які були об'єднані в групу ЕМІ боєприпасів.

Варто зазначити, що найбільш інтенсивно розвиток і створення нових ЕМІ боєприпасів відбувався і продовжує розвиватися в США і в колишньому СРСР з успадкуванням даного напрямку Російською Федерацією. На даний час основу ЕМІ боєприпасів складають мікрохвильові ЕМІ побудовані на основі

використання так званих віркаторів – пристроїв генерації потужних імпульсів в діапазоні надвисоких частот.

Реальний досвід використання EMI боєприпасів є у збройних силах США. Вони масово використовували дані боєприпаси у 1999 році в Сербії і в 2003 в Іраці під час проведення операції «Буря в пустині».

Загальний принцип, який лежить в основі створення EMI боєприпасів передбачає, що досить обмежений енергетичний ресурс зазнає перетворення в електромагнітну енергію. Тому для досягнення високого рівня напруженості електромагнітного поля, здатного у відповідності з принципом електромагнітної індукції Фарадея, створити такі напруги на елементах і ділянках кіл електронної техніки, які призведуть до їх пошкодження і виведення з ладу, необхідно здійснювати стиснення в часі процесу вивільнення накопиченої електромагнітної енергії. Таким чином задача зводиться до формування електромагнітних імпульсів пікосекундного діапазону шляхом своєрідної компресії електромагнітної енергії. Реалізація зазначеного принципу в EMI боєприпасах на даний час уже досить успішно здійснена, однак вона має ряд недоліків, які суттєво знижують їх ефективність. В першу чергу це усі негативні фактори, які пов′язані з використанням вибухівки і явищ, що супроводжують її детонацію. По друге, це складність здійснення чітко просторово орієнтованого спрямування випромінювання генерованого електромагнітного імпульсу, що спричиняє до значного розсіювання його енергії і утворення розширеної діаграми направленості.

З метою уникнення зазначених недоліків проведені дослідження, які показали перспективність створення портативних установок, здатних до генерації високоенергетичних електромагнітних імпульсів та їх випромінювання з вузькою діаграмою направленості та можливістю адаптивної зміни її апертури. Енергетичний потенціал такої установки спроможна забезпечити батарея суперконденсаторів (іоністорів), яка має унікальні властивості підтримувати як повільний так і імпульсний режим заряджання і найголовніше – забезпечувати імпульсний режим розряду з струмами в сотні тисяч ампер.

В експериментах використовувалась батарея з 6 суперконденсаторів ємністю в 3 фаради, які з’єднані послідовно і працювали при робочій напрузі 16 вольт. Батарея забезпечувала накопичення електричної енергії на рівні 13 Кдж.

Загальний вигляд батареї показаний на рис. 1. На рисунку 2 показано зображення антенного модуля установки.

Оціночні розрахунки показують, що випромінювання навіть одиночного електромагнітного імпульсу з даної установки буде здатне вивести з ладу спеціально не захищені електронні системи на відстані 600 - 800 метрів.

Рис.1. Батарея іоністорів з балансирами і силовим комутатором.

Рис. 2. Антенний модуль експериментальної установки.

Відносно невелика напруга джерела живлення зумовлює використання для формування пікосекундних імпульсів процесу розряду іоністорів за допомогою лавинного напівпровідникового комутатора. Максимальний струм I_{max} досягається в тому випадку, коли опір і індуктивність у контурі будуть незначними, тобто виконуватиметься нерівність: $\frac{L}{R} \ll t_s$.

Аналітичний розрахунок значення імпульсу струму можна виконати за співвідношенням:

$$I_{max} = \propto \vartheta_e U_o C F(E/p) \ .$$

При цьому тривалість імпульсу можна оцінювати за формулою:

$$t_p = [\propto \vartheta_e F(E/p)]^{-1} \ ,$$

де U_o – початкова напруга батареї іоністорів;

C – ємність батареї;

α – коефіцієнт ударної іонізації;

υ_e – дрейфова швидкість електронів;

F(E/p) – функція відношення E/p.

Проведені експерименти підвердили можливість досягнення пікосекундного діапазону комутації з досягненням відповідно гігаватного діапазону потужностей в імпульсі випромінювання.

Важливо відзначити, що, як показали експерименти, формування імпульсів надвеликої фронтальної потужності не супроводжується ні вибуховою хвилею, ні світло чи звуковими проявами, тобто характеризується повною відсутністю демаскуючих факторів. Застосування антенної системи з параболоїдним рефлектором дозволяє прицільне застосування і виключає можливість пошкодження власних систем інформаційно-телекомунікаційної інфраструктури.

Щербаков В. О.,
здобувач вищої освіти Дніпропетровського державного університету внутрішніх справ

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

ЗАХИСТ ІНФОРМАЦІЇ НА МОБІЛЬНИХ ПРИСТРОЯХ ВІД ЗАГРОЗ ТА ВИКОРИСТАННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Варто почати з того, що сучасна проблематика інформаційної безпеки на мобільних пристроях включає разом з забезпеченням безпеки інформації та інформаційних систем ще два компоненти: захист від впливу шкідливої інформації та забезпечення прийняття обґрунтованих рішень при максимальному використанні доступної інформації.

Зазначимо, що захист інформації на мобільних пристроях являє собою прийняття правових, організаційних і технічних заходів для забезпечення захисту інформації від несанкціонованого доступу, знищення, перекручення, блокування інформації, копіювання, надання, поширення та інших незаконних дій щодо такої інформації. Конфіденційність інформаційних ресурсів з обмеженим доступом, реалізація основоположного права на вільний доступ до інформації являються запорукою основних прав і свобод людини.

Нами було визначено, що забезпечення інформаційної безпеки на мобільних пристроях повинно вирішувати такі основні завдання:

- виявлення, оцінка та запобігання загрозам інформаційним системам і ресурсів;
- захист прав юридичних і фізичних осіб на інтелектуальну власність;
- збір, накопичення і використання інформації;
- захист державної, службової, комерційної, особистої та інших таємниць [1].

Загрози інформаційним системам і ресурсів для користувачів сучасних мобільних пристроїв умовно можна розділити на чотири основні групи:

1) програмне забезпечення - впровадження «вірусів», апаратних і програмних закладок; знищення і зміна даних в інформаційних системах;
2) технічні, в тому числі електронне перехоплення інформації в лініях зв'язку, електронне придушення сигналу в лініях зв'язку і системах управління;
3) фізичне знищення технологічного обладнання і носіїв інформації; крадіжка медіа та апаратних або програмних ключів та/або паролів;
4) інформація – порушення правил обміну інформацією; незаконне збирання і використання інформації; несанкціонований доступ до інформаційних ресурсів; незаконне копіювання даних в інформаційних системах; дезінформація, приховування або фальсифікація інформації; викрадення інформації з баз даних.

Варто відмітити, що даним загрозам можна протистояти, створивши і запровадивши ефективні системи захисту інформації від шкідливого ПЗ на мобільних пристроях [2, с.43].

Події останніх років вказують на те, що досить часто обговорюється і є дискусійною проблема інформаційного протиборства в Інтернеті – так званої кібервійни. Її основна мета – дестабілізувати інформаційні системи і доступ до Інтернету в державних установах, фінансових і ділових центрах, а також створити безлад і хаос в державах, які покладаються на Інтернет в своєму повсякденному житті.

Міждержавні відносини і політичне протистояння можуть тривати в Інтернеті в формі кібервійни з такими проявами: вандалізм, пропаганда, шпигунство і прямі атаки на комп'ютерні системи і сервери, шкідливе ПЗ на мобільних пристроях.

З поширенням інформаційних технологій на мобільних пристроях громадяни, підприємства і державні установи буквально стали залежати від Інтернету в своєму повсякденному житті. Їх використання для атаки на інформаційні системи іншої держави може завдати значних економічних збитків і привести до розбіжностей в повсякденному житті держави [2, с.78].

У міру того як нові технології переходять на мобільні пристрої, масштаби кібервійни постійно збільшуються і підвищують її загрози. Деякі держави приділяють особливу увагу захисту від кібервійни і надають необхідні ресурси для організації систем захисту і підтримки спеціальних сил, завданням яких є

підвищення і поліпшення інформаційної безпеки. Контроль над мобільними пристроями з доступом до мережі Інтернет в наш час визначає стан національної безпеки держави.

Отже, у висновках можна сказати, що розвиток інформаційних технологій для користувачів сучасних мобільних пристроїв має тенденцію до все більшого прискорення, тому правова база повинна невпинно змінюватися для вирішення всіх нагальних проблем людей, суспільства та міжнародної спільноти в галузі інформаційної безпеки.

Література:

1. Дмитренко М. Проблеми інформаційної безпеки України,. URL: http:// socialscience.com.ua/article/807 (дата звернення: 25.03.2021).
2. Кормич Б. Інформаційна безпека: організаційно-правові основи : навчальний посібник, Б. Кормич. Київ : Кондор, 2004. 384 с.

Долинюк Х. Т.,
здобувач освітнього рівня магістр Львівського державного університету внутрішніх справ

Рудий Т. В.,
доцент кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів Львівського державного університету внутрішніх справ, к.т.н., доцент

ЦИФРОВІЗАЦІЙНІ ВПЛИВИ І РОЗВИТОК ЕКОНОМІКИ УКРАЇНИ

Цифрова економіка – один з основних векторів розвитку української економіки протягом наступних 10 років. Цифровізація є важливою для економіки України, адже дозволить збільшити кількість нових робочих місць та досягти мінімум 4% додаткового зростання ВВП на рік. Відкриття нових сегментів та галузей прискорить розвиток промисловості та бізнесу. Для українців цифровізація означає повний доступ до цифрової інфраструктури та якісних державних і соціальних послуг"[1].

Серед основних стратегічних напрямів розвитку цифрової економіки:

- розвиток цифрової інфраструктури
- розвиток цифрових навичок
- розвиток сектору інформаційно-комунікаційних технологій
- цифровізація сфер життя та секторів економіки

Розвиток інформаційного суспільства стимулює формування економічної системи інформаційного типу – цифрової економіки. Цифрова економіка – це економіка, заснована на даних, мобільності, хмарних сервісах і новітніх інформаційних технологіях. Цифрова економіка продукує трансформаційні процеси економічних відносин у цифровий формат. Як тренд розвитку світової економіки і суспільства цифровізація (цифрова трансформація) впливає на різні сфери суспільства і від ступеня її впливу залежить місце кожної країни у світовому співтоваристві.

Цифровізація є безумовним драйвером сучасного суспільства, усіх його складових і дає багато переваг для зростання економіки. Розглядається як аксіома, що інвестиції в цифровий актив значно прибутковіші, ніж у нецифровий, а сектори, пов'язані з цифровими технологіями, показують більший приріст робочої сили, ніж світова економіка в цілому. Тому і вплив цифровізації, і ставлення до неї є неоднозначним [2].

Цифровізація надає низку переваг для розвитку економіки. Технології, інтелектуальні програми та інші інновації у цифровій економіці можуть підвищити якість послуг, що надаються, і допомогти вирішити проблеми в різних областях, включно з охороною здоров'я, сільським господарством, державним управлінням, податками, транспортом, освітою, екологією та ін. [3].

Цифровізація всіх аспектів життя обумовлена, перш за все, її можливими позитивними проявами та наслідками на всіх рівнях:

- економічний і соціальний ефект від цифрових технологій для бізнесу та суспільства;
- підвищення якості життя;
- зростання продуктивності всієї суспільної праці;
- виникнення нових моделей і форм бізнесу;
- підвищення прозорості економічних операцій і забезпечення можливості їх моніторингу;
- забезпечення доступності і просування товарів і послуг як державних, так і комерційних;
- поява людинозамінних керуючих систем [3].

Технологічні переваги, обумовлені цифровізацією:

- спільне використання інформації і відсутність конкуренції у споживанні знань та інформації;
- акумулювання великих обсягів даних, здійснення їх автоматичного оброблення та аналізу;
- синхронізація потоків інформації, можливість точкового розподілу даних у рамках усього бізнесу і, як наслідок, можливість відстеження великої кількості ланцюжків між постачальниками і споживачами, проведення інтелектуальної та точкової аналітики;
- оволодіння новими технологіями на прикладному рівні;
- перехід від паперових документів до електронних [4].

До головних проблем і перешкод на шляху впровадження та розвитку цифрової економіки в Україні слід віднести:

- не досить розвинуту інфраструктуру;

- низьку технологічну освіченість, територіальну цифрову нерівність, незначну частку інновацій у цифрову економіку;
- застарілість техніки в державних структурах;
- відсутність стандартизації цілих інформаційних систем, які б гарантували інформаційну безпеку як на індивідуальному рівні, так і на рівні надання інформаційних послуг державою;
- непропорційну структуру ринку ІТ, неузгодженість стратегічного підходу до формування політик у напрямі гармонізації цифрових ринків з ЄС [4].

Для української економіки тренди цифровізації пов'язані з серйозними викликами, оскільки питання формування цифрової економіки стають для України питаннями її національної безпеки і конкурентоспроможності на світовому ринку (зовнішні виклики), а також питаннями рівня і якості життя населення України (внутрішні виклики). Відставання України за темпами і масштабами цифровізації від країн сусідів може призвести до того, що Україна опиниться на узбіччі науково-технічного прогресу, що, своєю чергою, зумовить:

- роль України у світовій економіці буде наздоганяюча;
- забезпечення національної безпеки буде поставлене під питання;
- Україна буде позбавлена перспектив інноваційного розвитку, що істотно знизить конкурентоспроможність як окремих вітчизняних компаній, так і всієї української економіки на світовому ринку [4].

В Україні на державному рівні визнається необхідність формування цифрової економіки, а цифрові технології розглядаються в якості одного з ключових драйверів сталого розвитку.

Особливість українського цифрового розвитку полягає в тому, що індивідуальні користувачі і бізнес значно випереджають державу і промисловість. Український малий і середній бізнес уже використовують ІКТ і здебільшого цифрові методи просування своїх послуг, тоді як держава і велика промисловість в Україні кардинально відстають [3].

Роль держави у впровадженні цифрової економіки розглядають як подвійну:

- як регулятора, що запроваджує норми, принципи та основи співіснування елементів цифрової економіки, здійснює технологічні зміни, що сприяють закріпленню цифрових відносин між суспільством та владою;
- держава може використовувати Internet та інформаційні технології безпосередньо під час надання своїх послуг в онлайн-торгівлі, електронному врядуванні.
- Відставання від розвинутих країн пояснюється:
- особливістю економічної моделі, в якій значне місце посідає агропромисловий комплекс;
- надто повільними темпами впровадження цифрових технологій;
- необхідністю подолання відставання в розвитку науково-технічної бази, порівняно з постіндустріальними країнами [4].

Література:

1. Михайло Федоров: Цифровізація економіки. https://thedigital.gov.ua › news
2. Четвертая промышленная революция. Целевые ориентиры развития промышленных технологий и инноваций. Информационный документ. – Всемирный экономический форум. Електронний ресурс]. URL: http://www3.weforum.org/docs/WEF_%D0%A7%D0%B5%D1%82%D0%B2%D0%B5%D1%80%D1%82%D0%B0%D1%8F_%D0%BF%D1%80%D0%BE%D0%BC%D1%8B%D1%88%D0%BB%D0%B5%D0%BD%D0%BD%D0%B0%D1%8F%20%D1%80%D0%B5%D0%B2%D0%BE%D0%BB%D1%8E%D1%86%D0%B8%D1%8F.pdf.
3. OECD Digital Economy Outlook 2017. – OECD. Електронний ресурс]. URL: https://espas.secure.europarl.europa.eu/orbis/sites/default/files/generated/document/en/9317011e.pdf.
4. Цифрова економіка як новітній вектор реконструкції традиційної економіки. Електронний ресурс]. URL: http://inneco.org/index.php/innecoua/article/view/305/367
5. Цифрова економіка: тренди, ризики та соціальні детермінанти. [Електронний ресурс]. URL: https://razumkov.org.ua/uploads/article/2020_digitalization.pdf

Пелещак О. Р.,
здобувач освітнього ступеня доктора філософії у галузі права Львівського державного університету внутрішніх справ

КІБЕРДИВЕРСІЯ ЯК ЗАГРОЗА ДЕРЖАВІ

Кіберзлочинність, за визначенням міжнародних документів, є загрозою для міжнародного правопорядку, безпеки людства загалом та для національної безпеки окремих держав, зокрема. Не зважаючи на зусилля правоохоронних органів, спрямовані на боротьбу з кіберзлочинами, їх кількість в останні п'ять років в Україні постійно збільшується та становить найбільш серйозну небезпеку для нашої країни. Україна посіла четверте місце в Європі у списку найбільш кібернезахищених країн [1] та увійшла до трійки лідерів з DDoS-атак [2]. Перехід на віддалений режим роботи, в свою чергу, спровокував збільшення таких злочинів на 20,6%. Водночас, змінилися і цілі, на які сфокусовані кіберзлочинці. Так, у грудні 2019 основним напрямом атак були державні установи та різного роду індустрії – по 15,9% від загальної кількості злочинів. На третьому місці - атаки, націлені на персональні дані окремих фізичних осіб – 12,1%. Однак, на сьогодні, як показує статистика, основною ціллю є саме фізичні особи - 18,9%, на другому місці індустрії (17,8%), на третьому - державні установи (11,2%) [1]. Однак, це не зменшує надважливості захисту державних установ, організацій, підприємств, інформаційних систем.

Не зважаючи на вчинення злочинів у віртуальному просторі, збитки від них цілком реальні. Окрім фінансових (в т.ч. і витрати на оборону від кібератак) і цифрових втрат виникають репутаційні (іміджеві), втрати робочого часу, що супроводжуються зниженням рівня задоволення працівників своєю роботою. Відсутність визнання України країною «з належним рівнем захисту» є суттєвою перешкодою для укладання договорів з іноземними партнерами та інвесторами.

Аналіз національного законодавства України щодо регулювання суспільних відносин в інформаційній сфері дозволяє зробити твердження, що наша держава вживає необхідні заходи, спрямовані на профілактику та протидію злочинам у кіберпросторі (прийнято Стратегію кібербезпеки України, створено Національний координаційний центр кібербезпеки тощо). Однак, нормативне регулювання цієї сфери в Україні не встигає за розвитком технологій. А отже, превентивні механізми, закладені у законодавстві не можуть повністю усунути чи попередити всі негативні наслідки.

Найбільш поширеними видами кібердиверсій є злом баз даних урядових організацій, виведення з ладу об'єктів критичної інфраструктури (енергетичних об'єктів, транспорту, банківських установ) [3, с. 27]. Тому на перший план виходить кібербезпека державного сектору, хоча вартість захисних засобів часто перевищує у десять разів наслідки кібератак. Протидією кібердиверсіям в Україні займається Служба безпеки України та, частково, в міру своїх повноважень, інші відомства (Державна служба спеціального зв'язку і захисту інформації, Міністерство внутрішніх справ, Національний банк). Від взаємоузгодженості їх дій залежить ефективність протидії злочинам у цій сфері.

Пошук, фіксація, вилучення та збирання електронних доказів не можливі без використання комп'ютерних та інших технологій. Широко застосовуються вони і в оперативно-розшуковій діяльності правоохоронних органів. Криміналістичною особливістю кібердиверсій є те, що кожне покоління кіберзлочинців застосовує свої види інструментів. Різняться також і види самих злочинів: троянські програми, ботмережі для крадіжки інформації, DDoS-атаки, шифрування даних для подальшого шантажу, пошкодження антивірусних програм та ін. Особливо небезпечним є інфікування комп'ютерів і мереж шкідливими програмами з метою сталого контролю над ними.

За словами експертів з Huawei, успішність кібератак залежить на 91% саме від людських помилок (відкривання небезпечних посилань, успішний фішинг, завантаження шкідливих файлів, тощо) та лише на 9% від технічних проблем (слабка захищеність систем, відсутність спеціального софту, тощо) [1]. Більшість успішних кібератак здійснюються саме через необізнаність, неуважність, нехтування правилами кібергігієни. Тому правоохоронними органами робиться акцент на превентивній роботі з населенням (повідомлення про можливі загрози, фішинг, небезпеку переходу на неперевірені гіперпосилання, використання ненадійних паролів та ін.). Помічними в даній ситуації можуть стати багатофакторна автентифікація користувача та різноманітні методи шифрування (кодування) даних.

За даними AT&T, девайсами, через які найбільше здійснюються кіберзлочини є: ПК (70% успішності злочинів), смарфони (61%), планшети (53%), WiFi точки доступу (50%) [1]. Отже, не можна обмежуватись

лише встановленням антивірусної програми, необхідно подбати про комплексний захист державних установ та об'єктів критичної інфраструктури.

Невідворотна діджиталізація державного сектору України, як новий глобальний тренд, змушує нас задуматись про подальшими кроками для аксекурації його безпеки. Вдосконалення методів, засобів, прийомів скоєння кібердиверсій (які стають більш організованими та починають набувати форму бізнесу для отримання довгострокового прибутку) зумовлюють постійне розширення повноважень правоохоронних органів, взаємодію та координацію зусиль (різних органів, спецслужб, судової системи), зростання обізнаності (набуття нових знань, умінь та навичок) у даній сфері та необхідність покращення технічних можливостей.

Отже, протидія кібердиверсіям та забезпечення національної кіберстійкості є пріоритетним напрямком політики нашої держави, потребує подальшого комплексного вирішення на законодавчому, організаційному, технічному і рівні обміну інформацією та активізації міжнародної співпраці у цій сфері.

Література:

1. Куничак О. Найпопулярніший пароль «password» та інші проблеми кібербезпеки: п'ять порад для захисту себе та бізнесу. 2020. URL: https://biz.nv.ua/ukr/experts/yak-zahistitisya-vid-kiberzlochinciv-uspishnist-kiberatak-zalezhit-na-91-vid-lyudskih-pomilok-50086395.html (дата звернення 09.12.2021)

2. Довбиш Н. Кіберзлочинність в Україні. 2013. URL: https://www.science-community.org/ru/node/16132 (дата звернення 09.12.2021)

3. Пелещак О.Р. Деякі аспекти кримінально-правової характеристики кібердиверсій. Соціально-правові студії. Вип. 3(9). 2020. С. 26-33.

Зміст

Наукове видання

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТІ ТА ПРАКТИЦІ

МАТЕРІАЛИ ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

17 грудня 2021 року

Опубліковано в авторській редакції

Формат 60×84/8. Умовн. друк арк. 11,8.

Львівський державний університет внутрішніх справ
Україна, 79007, м. Львів, вул. Городоцька, 26.
Свідоцтво про внесення суб'єкта видавничої справи до Державного реєстру
видавців, виготівників і розповсюджувачів видавничої продукції
ДК № 2541 від 26 червня 2006 р.