МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ДНІПРОПЕТРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

КАФЕДРА ЕКОНОМІЧНОЇ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЙ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Матеріали Всеукраїнського науково-практичного семінару (м. Дніпро, 26 листопада 2020 р.)

Дніпро – 2020

ББК 67.9(4УКР)305

П 685
УДК 347.23 (477)

Рекомендовано до друку Науково-методичною радою Дніпропетровського державного університету внутрішніх справ.
(протокол № 4 від 17.12 2020)

П 685 **СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ**: матеріали Всеукраїнського науково-практичного семінару (26 листопада 2020 р., м. Дніпро). – Дніпро: Дніпропетровський державний університет внутрішніх справ, 2020. – 179 с. *(в авторській редакції)*

СКЛАД ОРГАНІЗАЦІЙНОГО КОМІТЕТУ
Всеукраїнського науково-практичного семінару "Сучасні інформаційні технологій в діяльності Національної поліції України"

Голова оргкомітету – **Наливайко Лариса Романівна**, проректор університету, д.ю.н., професор, Заслужений юрист України

Заступник голови оргкомітету – **Рижков Едуард Володимирович,** завідувач кафедри економічної та інформаційної безпеки, к.ю.н., доцент

Члени оргкомітету:

Шнурко Яна Вікторівна - завідувач відділення зв'язків з громадськістю;
Самотуга Андрій Валерійович - к.ю.н., доцент, заступник завідувача редакційно-видавничого відділення;
Гребенюк Андрій Миколайович – відповідальний секретар семінару, доцент кафедри економічної та інформаційної безпеки; к.т.н., доцент;
Мирошниченко Володимир Олексійович – професор кафедри економічної та інформаційної безпеки, к.т.н., доцент;
Тютченко Світлана Миколаївна – старший викладач кафедри економічної та інформаційної безпеки
Рибальченко Людмила Володимирівна – доцент кафедри економічної та інформаційної безпеки, к.т.н., доцент;
Прокопов Сергій Олександрович – старший викладач кафедри економічної та інформаційної безпеки.

ББК 67.9(4УКР)305

ЗМІСТ

КУРСАНТИ ТА СТУДЕНТИ ПІД НАУКОВИМ КЕРІВНИЦТВОМ	
Глушаченко В.В. ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ	**102**
Чечель А.О. ПОШУК ЗНИКЛИХ ДІТЕЙ ЯК ОДИН ІЗ НАПРЯМКІВ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ	**105**
Грищенко Д.Р. МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ ПРОЗОРСТІ І ВІДКРИТОСТІ ОРГАНІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ В КОНТЕКСТІ ВПРОВАДЖЕННЯ ЕЛЕКТРОННОГО ВРЯДУВАННЯ	**106**
Трень Т.О. ІНФОРМАЦІЙНА БЕЗПЕКА В ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ	**109**
Дума А.А. ІНФОРМАЦІЙНА БЕЗПЕКА НАЦІОНАЛЬНОЇ ПОЛІЦІЇ	**111**
Філімонов В.О. ВИЗНАЧЕННЯ МІСЦЕЗНАХОДЖЕННЯ ЧЕРЕЗ ГЕОІНФОРМАЦІЙНУ СИСТЕМУ	**113**
Пяничук М.С. ЗАКОРДОННИЙ ДОСВІД ЗАСТОСУВАННЯ НОВІТНІХ ТЕХНОЛОГІЙ В ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ	**115**
Голубєва Д.В. ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ПРАВООХОРОННІЙ ТА ЮРИДИЧНІЙ ДІЯЛЬНОСТІ	**118**
Тарантюк А.Р. ТЕОРЕТИЧНІ ЗАСАДИ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ ДІЯЛЬНОСТІ	**119**
Штундер В.Є. ВДОСКОНАЛЕННЯ СИСТЕМИ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ПРАВООХОРОННИХ ОРГАНІВ	**121**
Гавриш Б.О. ПЕРЕВАГИ ТА ПРОБЛЕМИ ДИСТАНЦІЙНОГО НАВЧАННЯ	**123**
Кочетова В.С. КІБЕРБУЛІНГ- РОЗВАГА ЧИ ЗЛОЧИН?	**125**
Батура Д.В. ФІНАНСОВЕ ШАХРАЙСТВО В СОЦІАЛЬНИХ МЕРЕЖАХ	**128**
Байрак К.С. ПРОБЛЕМИ КІБЕРБЕЗПЕКИ В УКРАЇНІ	**130**
Андрусяк Л.В. ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ВИЯВЛЕННЯ ЗЛОЧИНІВ, ЩО ВЧИНЯЮТЬСЯ ПІД ЧАС ПУБЛІЧНИХ ЗАКУПІВЕЛЬ	**132**
Федченко Т.К. ПОСЯГАННЯ НА КІБЕРБЕЗПЕКУ ЯК АКТУАЛЬНА ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ УКРАЇНИ	**134**
Сергійчук К.М. СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ	**136**
Попова Т.В. ВАЖЛИВІСТЬ ВИКОРИСТАННЯ СОЦІАЛЬНО-ПСИХОЛОГІЧНОЇ ХАРАКТЕРИСТИКИ ІНТЕРНЕТ-ШАХРАЯ У РОЗСЛІДУВАННІ ЗЛОЧИНІВ ВЧИНЕНИХ В ІНТЕРНЕТ ПРОСТОРІ	**138**

ТЕЗИ ВИСТУПІВ

Мордвинцев М.В.
провідний науковий співробітник науково-дослідної лабораторії з проблем розвитку інформаційних технологій Харківського національного університету внутрішніх справ, к.т.н, доцент
Хлєстков О.В.
старший науковий співробітник науково-дослідної лабораторії з проблем розвитку інформаційних технологій Харківського національного університету внутрішніх справ
Ницюк С.П.
старший науковий співробітник науково-дослідної лабораторії з проблем розвитку інформаційних технологій Харківського національного університету внутрішніх справ

СТАН СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ ТА ВІДЕОФІКСАЦІЇ, ЯКІ ВИКОРИСТОВУЮТЬСЯ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

В Національній поліції України (далі – НП України) для забезпечення громадської безпеки, збору доказів злочину, пошуку і затримання злочинців, охорони власності, дотримання правил дорожнього руху т.і. використовуються системи відеоспостереження та відеофіксації, які належать силовим структурам, а також ті що знаходяться в приватній власності [1].

Патрульна поліція України використовує нагрудні відеокамери (відеореєстратори), системи відеоспостереження, встановлені на службових транспортних засобах, і стаціонарні системи відеоспостереження. Основною метою використання відеореєстраторів є забезпечення об’єктивної оцінки дій патрульного під час виконання ним своїх обов’язків, ретельний збір доказів правопорушення.

Управління силами та засобами патрульної поліції здійснюється за допомогою системи централізованого управління нарядами патрульної служби «ЦУНАМІ». До складу цієї системи входить система стаціонарного відеоспостереження, яка забезпечує оперативний візуальний контроль за основними криміногенними місцями, вулицями, майданами, транспортними потоками, об’єктами що

охороняються. На сьогодні органи і підрозділи НП Україні мають можливість використовувати інформацію з понад ніж 24 тис. відеокамер, з яких майже 2,8 тис. це так звані «розумні».

За допомогою систем відеоспостереження, встановлені на службових транспортних засобах функціонує інформаційна підсистема «Гарпун». Система «Гарпун» використовує спеціалізоване аналітичне програмне забезпечення створене для розшуку викрадених транспортних засобів та номерних знаків, виявлення одночасного перебування номерних знаків на різних транспортних засобах, фактів використання знищених номерних знаків, а також для автоматизованого інформування про такі факти чергових диспетчерів патрульної служби. «Гарпун» є підсистемою інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України».

До Єдиного аналітичного сервісного центру Головного управління Національної поліції в Донецькій області належить система UASC, в якій використовують інтелектуальні відеокамери. Система проводить ідентифікацію автомобіля, на який встановлений державний номер і виявляє відповідність номера автомобіля згідно з реєстрацією, розпізнає тип і марку автомобіля та його колір, перевіряє чи знаходиться автомобіль у розшуку, чи відповідає державний номер автомобіля, ідентифікує осіб, які знаходяться на передньому сидінні. Система виявляє скупчення людей, може фіксувати їх неадекватну поведінку, розпізнає заборонений або нетиповий рух автотранспорту т.і.

В структурі апарату НП України створено Управління організації діяльності підрозділів поліції на воді та повітряної підтримки (УПВП). Його запроваджено для організації, координації й контролю службової діяльності підрозділів поліції на воді та забезпечення повітряної підтримки підрозділів НП України. Підрозділи поліції застосовують БпЛА для: висотного спостереження під час проведення масових святкувань, політичних демонстрацій, спортивних заходів, а також під час припинення масових заворушень; висотного спостереження при загрозі нападу на стратегічні об’єкти та об’єкти, які знаходяться під охороною; виявлення злочинів та адміністративних правопорушень; організації відео документування; забезпечення зв’язку й управління наземними нарядами поліції; організації взаємодії підрозділів поліції з іншими силовими структурами; забезпечення та контролю безпеки дорожнього руху; проведення спостереження при здійсненні оперативних заходів, відстеження оперативної обстановки під час виконання службових завдань; пошуку підозрюваних, які намагаються сховатись; пошуку зниклих людей.

КАСКАД – комплексна система контролю автомобільних доріг (Київ). Єдиний повнофункціональний пристрій що впроваджений в експлуатацію, та розроблений під особливості національного технічного регулювання, законодавчу базу. Встановлені комплекси фіксують події з ознаками порушень ПДР: швидкісний режим; проїзд на забороняючий сигнал світлофора; порушення розмітки, перетин суцільної смуги; порушення правил паркування; рух смугою громадського транспорту. Дані передають до системи збору та обробки даних (АСОД).

В Україні прийнято ряд законів, інструкцій та інших документів, що регламентують впровадження системи фото- і кінозйомки, відеозапису в

Національній поліції.

Використані джерела:

1. Коршенко В.А., Чумак В.В., Мордвинцев М.В., Пашнев Д.В. Стан систем безпеки з використанням технічних засобів відеозапису та відеоспостереження: зарубіжний досвід, перспективи впровадження в діяльність Національної поліції України / В.А. Коршенко, В.В. Чумак, М.В. Мордвинцев, Д.В. Пашнев // Право і безпека. – 2020. – № 2(77) – С. 86-92.

Лізунов С.І.
доцент кафедри захисту інформації
Національного університету
«Запорізька політехніка»,
к.т.н., доцент

ЗАХИСТ ВІД ПРИХОВАНОГО МАЙНІНГА

Майнінг - це діяльність по створенню нових структур для забезпечення функціонування криптовалютних платформ.

Для видобутку криптовалюти можливо не тільки використання власного комп’ютера, але і безлічі чужих машин [1].

Наприклад, у магазині Google Play знайшли додаток під назвою Vilny.net, що працює як VPN-сервіс, проте в той же час використовує ресурси смартфонів, щоб майніти криптовалюту Monero [2].

На сьогоднішній день прихований майнінг може зробити будь-який користувач. Для цього досить лише завантажити готову програму, написати номер свого електронного гаманця і все. Програма модифікована так, що вона не відрізняється від троянського вірусу: вона може поширюватися в мережі, копіювати сама себе на зовнішній накопичувач, приховувати свої процеси в диспетчері завдань і використовувати комп’ютер коли ним ніхто не користується.

Для прихованого видобутку криптовалюти не потрібно зламувати комп'ютер і встановлювати троян. Поки у користувача в браузері відкрита сторінка з шкідливим скриптом, процесор буде непомітно майніти.

І необов'язково, що навантаження на відеокарту або процесор має зрости до 100% - зловмисники обережні і не стануть навантажувати машину учасника своєї мережі в нерозумних межах. Ви можете, в принципі, і не помітити великої різниці,

якщо у вас досить потужна техніка. Це важлива умова для збереження прихованої роботи майнера.

"Підвисання" на комп'ютері, які зникають, якщо розірвати з'єднання з інтернетом є ознакою, що ресурси вашого комп'ютера витрачаються із зовні. Варто обірвати з'єднання і шукати проблеми в системі.

Найчастіше програму майнінг ховають під системний процес svchost.exe. Для того, щоб знайти цю програму необхідно зробити наступне [3].:

1. Svchost.exe повинен завжди виконуватися від імені системи, network і local сервісів. Якщо він запущений від імені будь-якого користувача, то варто перевірити його директорію на жорсткому диску. Істинний файл знаходиться у папці Windows/system32 і ніяк інакше.

2. Слід перевірити таблицю автозавантаження Windows. У цій таблиці не повинен знаходитися файл svchost.exe. Цей процес операційна система повинна запускати самостійно, без участі користувача або шкідливої програми, яка занесла цю програму до списку автозавантажень.

Якщо програму майнінг знайдено, необхідно її видалити. Для цього слід використовувати програму Process Hacker. Криптовані процеси або упаковані процеси - найчастіше приховані. Майнер виступає саме як "упакований процес" в svchost.exe або іншій програмі, який відображається рожевим кольором в Process Hacker (packet procces). Слід відшукати такі процеси і проаналізувати їх директорію на жорсткому диску. Найчастіше вони ховаються від імені cmd.exe (прихованого командного рядка). Коли цей процес знайдено, перед тим як його зупинити, слід знайти місце розташування цього процесу. Після того, як ця програма зупинена, необхідно її видалити з жорсткого диску і, бажано, просканувати системний реєстр на посилання на цю директорію.

Якщо програму майнінгу модифікувати, то можливе знімання інформації про всі дії користувача. Тому, для захисту інформації, слід обов'язково знищувати програми майнінгу.

Використані джерела:

1. Скрытый майнинг: найти и уничтожить [Електронний ресурс]. – Режим доступу: https://bitnovosti.com/2017/08/16/skritiy-mayning-nayti-unichtojit/

2. В украинском приложении VPN нашли майнинговый вирус [Електронний ресурс]. – Режим доступу: http://mignews.com.ua/society/19587813.html

3. Как обезопасить себя от скрытого майнинга криптовалют [Електронний ресурс]. – Режим доступу: https://tjournal.ru/59579-kak-obezopasit-sebya-ot-skrytogo-mayninga-kriptovalyut

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

ОКРЕМІ АСПЕКТИ ВДОСКАНАЛЕННЯ ТА ВИКОРИСТАННЯ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ І ВІДЕОАНАЛІТИКИ У ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

Остатнім часом важливу роль в діяльності Національної поліції у сфері протидії злочинності, забезпечення публічного порядку стали відігравати системи відеоспостереження і ведеоаналітики [1]. У зв'язку з цим, на одне з перших місць виходять питання оптимізації розподілу завдань та обов'язків між окремими структурними підрозділами та працівниками. Удосконалення цього напряму роботи є найважливішою умовою забезпечення ефективної взаємодії між окремими підрозділами й працівниками, а також забезпечення узгодженості рішень, дій, сприяє підвищенню особистої відповідальності за кінцевий результат і, зрештою, забезпечує раціональне застосування індивідуальних можливостей кожного працівника Національної поліції.

Вказаний аспект надзвичайно важливо враховувати на усіх етапах розроблення, впровадження та розвитку систем відеонагляду та відеоаналітики. У зв'язку із цим, для найефективнішого використання можливостей систем відеонагляду та відеоаналітики в органах та підрозділах Національної поліції є доцільність у встановлені порядку та розподілу функціональних обов'язків за напрямками діяльності окремих структурних підрозділів ГУ Національної поліції та територіальних (відокремлених) підрозділів.

Так, наприклад, організацію оперативного реагування, своєчасного орієнтування нарядів патрульної поліції під час виявлення програмними комплексами систем відеоспостереження та відеоаналітики правопорушення або автотранспорту, який перебуває в розшуку, доцільно покласти на підрозділи Управління аналітичного забезпечення та оперативного реагування та Управління патрульної поліції; розкриття злочинів по «гарячих слідах» – на Управління карного розшуку; до опрацювання відеоматеріалів з архівів систем відеоспостереження та відеоаналітики з метою отримання інформації, що може сприяти виявленню, припиненню та розслідуванню кримінальних правопорушень, раціональніше залучати працівників підрозділів Слідчого управління, Управління карного розшуку та кримінального аналізу ГУ Національної поліції; у випадку проведення масових заходів різного характеру активне використання можливостей систем відеонагляду та відеоаналітики доцільно покласти на Управління аналітичного забезпечення та оперативного реагування (ситуаційні центри) із залученням Управління патрульної поліції, а також представників Управління превентивної діяльності.

Також з урахуванням того, що працівники підрозділів превентивної діяльності та кримінальної поліції постійно проводять моніторинг території обслуговування, найдоцільніше покласти на них обов'язок стосовно наповнення ними каталогів

камер відеоспостереження у системі «Інформаційний портал Національної поліції», у тому числі даними про відеокамери, які не є муніципальною чи власною складовою систем відеоспостереження та відеоаналітики, але можуть фіксувати інформацію, що сприятиме реалізації завдань поліції, які визначені нормативно-правовими документами [2].

Силами підрозділу Управління інформаційно-аналітичної підтримки доцільно забезпечити технічні питання встановлення, супроводження експлуатації та використання камер систем відеонагляду та відеоспостереження. У разі потреби до виконання вказаних завдань доцільно залучати спеціалізовані комерційні фірми, приватні підприємства та спеціалізовані установи.

Також на підрозділи Управління інформаційно-аналітичної підтримки слід покласти завдання щодо встановлення, підключення, налаштування мережевого обладнання та підтримання безперебійного подавання сигналу, надання оперативної інформації із систем відеоспостереження та відеоаналітики оперативним та іншим зацікавленим підрозділам та службам за їх письмовими запитами.

Також важливими питаннями, вирішення яких слід організувати працівникам Управління інформаційно-аналітичної підтримки, є забезпечення інтеграції аналітичних даних, у першу чергу номерних знаків автотранспортних засобів, які отримані шляхом використання зовнішніх систем відеоспостереження та відеоаналітики, модернізації та програмної підтримки каталогу камер відеоспостереження, їх відображення на електронній мапі, а також розвиток аналітичних модулів опрацювання даних відеоспостереження у інформаційній системі «Інформаційний портал Національної поліції» [3].

Використані джерела:

1. Сеник В.В., Сидор В.В. Аналіз стану розвитку систем відеонагляду в діяльності Національної поліції України / Інформаційні технології в освіті та практиці : збірник наукових статей за матеріалами доповідей Всеукраїнської науково-практичної конференції 20 грудня 2019 року / упорядник Т. В. Магеровська. – Львів: ЛьвДУВС, 2019. – С. 51–54.

2. Положення про Національну поліцію : постанова Кабінету Міністрів України від 28 жовтня 2015 р. № 877. URL : http://www.kmu.gov.ua/control/uk/cardnpd?docid=248607704.

3. Про затвердження Положення про інформаційно-телекомунікаційну систему «Інформаційний портал Національної поліції України» : наказ МВС України від 03.08.2017 р. № 676. URL : http://zakon2.rada.gov.ua/laws/show/z1059-17.

Сеник С.В., науковий співробітник відділу організації наукової роботи, викладач кафедри адміністративного права та адміністративного процесу Львівського державного університету внутрішніх справ, PhD

ДО ПИТАННЯ УДОСКОНАЛЕННЯ НОРМАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ ТА ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Однією з найважливіших умов, яка веде до підвищення ефективності роботи Національної поліції, є удосконалення інформаційної діяльності, насамперед, використання для цього сучасних досягнень у галузі інформаційних технологій. Нинішні системи інформаційно-аналітичного забезпечення діяльності Національної поліції мають бути гнучкими, мобільними, здатними адаптуватися до будь-яких змін, до швидкої та комплексної перебудови стосовно реалізації нових викликів.

Нині основними тенденціями у розвитку інформаційних технологій у діяльності Національної поліції є: удосконалення форм та методів управління системами інформаційного забезпечення; централізація й інтеграція баз (банків) даних; використання сучасних інформаційно-телекомунікаційних технологій для створення та впровадження різних видів обліків; розбудова та широке використання ефективних і потужних інформаційно-телекомунікаційних мереж; застосування спеціалізованих засобів захисту інформації; налагодження ефективного взаємообміну різного розу інформацією на міждержавному рівні [1, с. 12].

Керуючись цими тенденціями вважаємо, що питання удосконалення діяльності Національної поліції в інформаційній сфері доцільно розглядати всесторонньо. При цьому одним із головних напрямів має стати удосконалення нормативно-правового регулювання інформаційних відносин. Нині низка питань у сфері інформаційної та інформаційно-аналітичної діяльності залишається ще не до кінця врегульованими. А це потребує не лише ґрунтовного аналізу законодавства, а й створення нових нормативних документів, які б регулювали інформаційну та інформаційно-аналітичну діяльність Національної поліції.

У своїх наукових працях окремі дослідники відзначають те, що стан сучасного законодавства в інформаційній сфері характеризується відсутністю чіткої ієрархічної єдності, що викликає суперечливе тлумачення та застосування його норм на практиці [2, с. 222]. Наприклад, І. П. Катеринчук акцентує увагу на таких недоліках інформаційного законодавства, що стали причиною неоднозначного тлумачення сутності інформаційних відносин: неточне тлумачення поняття «інформація» та відсутність чітких критеріїв поділу її на види, відсутність у Законі України «Про інформацію» [3] тлумачення понять «відомості», «дані», внаслідок чого потрібно звертатися до тлумачних словників, які надзвичайно широко інтерпретують ці категорії [4, с. 378]. На актуальності питання удосконалення нормативного-правового забезпечення інформаційної діяльності правоохоронних органів в умовах сучасності наголошують і інші науковці, наприклад,

Г. М. Шорохова [5, с. 185].

З метою вирішення проблеми удосконалення нормативно-правового регулювання інформаційної та інформаційно-аналітичної діяльності Національної поліції науковці означили два напрями, які відповідають підходам нормативно-правового регулювання інформаційних правовідносин в Україні. За основу першого взято доктрину загального права, яка полягає у фрагментарному удосконалені питань нормативно-правового регулювання інформаційних правовідносин на законодавчому рівні у деяких законах з використанням ситуаційного підходу. За основу другого – доктрину європейської системи права, виокремлення галузей законодавства та систематизацію їх на рівні кодифікації. Такий підхід для України є прийнятнішим, особливо в умовах прагнення України до Євроінтеграції.

Тут хотілось би зазначити, що на сьогодні, незважаючи на намагання провести кодифікацію інформаційного законодавства, відсутній навіть і проект кодексу України у цій сфері. Хоча його розроблення було ініційовано ще Національним агентством з питань інформатизації при Президентові України у 1995 році. Однак, попри доведення науковцями необхідності кодифікації інформаційного законодавства, його створенню і прийняттю перешкоджає відсутність політичної волі [6].

Однак, це не єдина причина. Проблема удосконалення законодавчого регулювання у сфері інформаційних відносин є складною ще й тому, що цей процес охоплює різні комплекси не лише правових, а й економічних і технічних проблем [7, с. 7–32].

Тож, можемо констатувати: попри те, що сьогодні законодавство України у сфері інформаційних відносин набуло надзвичайно важливого значення у правовій системі держави, для нього все ще характерне стихійне і ситуативне прийняття різних нормативно-правових актів, а тому стверджувати, що воно ефективне, неможливо.

У зв’язку із вищевикладеним пропонуємо, насамперед, втілити пропозиції науковців щодо потреби проведення систематизації нормативно-правових актів у цій галузі з урахуванням сучасного міжнародного нормативно-правового досвіду регулювання інформаційних правовідносин і лише після цього узгодити нормативно-правове забезпечення інформаційної та інформаційно-аналітичної діяльності підрозділі Національної поліції з цим законодавством. Оскільки окреслений процес нині проводиться низькими темпами, то у зв’язку з цим у питанні удосконалення нормативно-правового забезпечення інформаційної та інформаційно-аналітичної діяльності Національної поліції виникає чимало проблем. Так нормативно-правова база у галузі інформаційної та інформаційно-аналітичної діяльності Національної поліції складається з десятків наказів, рішень, протоколів, угод, які часто готували безсистемно та без узгодження між собою. У них визначено порядок функціонування, зберігання, формування, використання, обмін інформаційними ресурсами, побудови, впровадження, використання інформаційно-телекомунікаційних систем та мереж, інколи розпорядниками яких є різні органи державної влади. Однак уже сьогодні ці нормативні документи не відповідають сучасному стану і темпу розвитку інформаційних технологій, є громіздкими,

взаємодоповнюючими та суперечливими, а тому є необхідність їх уніфікації, гармонізації, у тому числі з урахуванням норм європейського законодавства. Окрім цього, враховуючи, що інформаційні ресурси масово опрацьовують в інформаційно-телекомунікаційних системах, уже нині виникла необхідність розроблення нових та узгодження існуючих нормативно-правових актів, які визначають порядок функціонування ЄІС МВС України, з вимогами інформаційного законодавства.

Використані джерела:

1. Кудінов В. А., Смаглюк В. М., Ігнатушко Ю. І., Іщенко В. А. Інформаційні технології в правоохоронній діяльності : посібник. Київ : НАВСУ, 2013. 82 с.
2. Беляков К. І. Інформатизація в Україні: проблеми організаційного, правового та наукового забезпечення : монографія. Київ : КВІЦ, 2008. 576 с.
3. Про інформацію : Закон України 2 жовтня 1992 р. № 2657-XII. *База даних* «*Законодавство України*» / *ВР України*. URL: http://zakon2.rada.gov.ua/laws/show/2657-12
4. Катеринчук І. П. Актуальні проблеми інформаційного забезпечення правоохоронних органів України. *Форум права*. 2011. № 2. С. 376–380.
5. Шорохова Г. М. Проблема вдосконалення інформаційного забезпечення діяльності правоохоронних органів України. *Шоста Міжнар. наук.-практ. конференція НАНР Економіко-правові виклики 2016 року* (12 січня 2016 р.). Львів : НАНР-Національна академія наукового розвитку, 2016. Т. 2. 202 с. URL: http://univd.edu.ua/science-issue/scientist/50
6. Ганжа Л. Інформаційний кодекс: реанімація привиду, який харчується мільйонами. *Українська правда*. 26.06.2015. URL: http://www.pravda.com.ua/columns/2015/06/26/7072512
7. Правове забезпечення інформаційної діяльності в Україні / за заг. ред. Ю. С. Шемшученка, І. С. Чижа. Київ : Юридична думка, 2006. 384 с.

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

Зачек О.І., доцент кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів Львівського державного університету внутрішніх справ, к.т.н., доцент

ПРОБЛЕМИ ОРГАНІЗАЦІЙНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ДЕРЖАВИ

З огляду на той факт, що чітких і зрозумілих нормативно-правових документів та організаційно-правових заходів щодо забезпечення національної системи

кібербезпеки, захисту інформаційного простору держави нема, тому і розв'язання проблем у системі правового забезпечення кібербезпеки без впровадження нових законодавчих, нормативно-правових актів і нової політики держави у сфері безпеки цифрового простору, тобто без розгляду інформаційних відносин з пункту бачення об'єкта правового регулювання є неможливим.

Аналіз причин незадовільного забезпечення інформаційної та кібербезпеки держави оголює цілу низку системних проблем у галузі нормативно-правової бази, ігнорувати які стає дедалі важче.

Розглянемо основні проблеми та прогалини у організаційно-правовому забезпеченні протидії кіберзлочинності.

В Україні відсутня офіційна державна статистика, яка б об'єктивно відтворювала відомості про кіберзлочини на основі методів кримінального аналізу (звітність про вчинення кіберзлочинів розпорошена серед різних підрозділів правоохоронних органів), що безпосередньо зачіпає сферу менеджменту у розробленні і супроводі нормативно-правового забезпечення протидії кіберзлочинності.

Кіберпростір України є дуже вразливим, бо не існує єдиної об'єднаної стратегії кіберзахисту. Основні завдання в сфері кіберзахисту, які повинні формуватися і реалізовуватися на державному рівні, полягають у наступному:

- захист суверенітету кіберпростору та забезпечення базової кібербезпеки;
- захист об'єктів критичної інфраструктури;
- розвиток і запровадження диджиталізації процесів державного управління та on-line культури;
- протидія кіберзлочинності, шпигунству і тероризму;
- розвиток кіберменеджменту;
- зміцнення міжнародного співробітництва шляхом імплементації у національне законодавство окремих норм нормативно-правових актів, прийнятих в країнах ЄС та НАТО у сфері захисту інформації, які на державному рівні визнаються усіма країнами. Регулятори в Україні явно запізнюються з розробленням правової бази для регулювання питань захищеності об'єктів критичної інфраструктури, а також з наповненням змістом та підзаконними актами рамкових законів щодо кібербезпеки. На часі розроблення та прийняття цілої низки нормативних документів, зокрема: вимог до кіберзахисту об'єктів критичної інфраструктури та оцінка кіберзагроз; порядку аудиту інформаційної безпеки [1].

Відсутній трансформаційний підхід до управління кібербезпекою з боку держави, що передбачає наявність організації, яка візьме на себе функції управління впровадженням програми з кібербезпеки, та регулярного контролю за процесом впровадження. Тобто, функції регулярного контролю за виконанням програми повинні належати неурядовій структурі, уповноваженій впроваджувати реформи у сфері кібербезпеки. Очевидно, це має бути не функція контролю (як зараз), а скоріше фасилітації (організація процесу колективного розв'язання проблем) і допомоги у розв'язанні проблем кібербезпеки державним і недержавним структурам [2].

Загалом управління кібербезпекою в Україні на державному рівні важко назвати ефективним. Національна система кібербезпеки обмежується переважно участю в ній правоохоронних органів. Приватний бізнес та кіберспільнота до розв'язання важливих питань практично не залучаються.

На наше переконання, необхідно врахувати ще один вагомий чинник. Важливою особливістю функціонування інформаційного і кіберпростору держави є його висока динамічність та мінливість загроз. Це обумовлює неможливість створення ефективного організаційно-правового забезпечення у сфері кібербезпеки на тривалий період. Тому, щонайменше, кожні два роки чинне законодавство у цій сфері потребуватиме корегування відповідно до нових загроз, а також змін у геополітичному безпековому середовищі.

Крім того, вкрай небажаним та, можливо, шкідливим, стане, якщо держава піде шляхом, коли для впровадження відповідних вимог щодо кіберзахисту необхідно буде здійснювати затвердження проекту технічних умов з захисту інформації (ЗІ) у державній інституції. Другим негативним сценарієм у цьому процесі може стати відсилання для сертифікування до процедур безнадійно застарілих комплексних систем захисту інформації (КСЗІ) [3].

Необхідно внести зміни до Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" з метою прийняття на території України вимог сімейства стандартів систем менеджменту інформаційною безпекою (СМІБ) для окремих категорій інформації, захист якої забезпечується законодавством України.

Для цього необхідно або адаптувати сучасні міжнародні стандарти систем ЗІ, або – розробляти та впроваджувати власні, якісно нові стандарти безпеки для державних органів та силових структур, що є неприйнятним з огляду на часові обмеження і матеріальні витрати.

На противагу КСЗІ в організаційно-правову структуру системи ЗІ повинні гармонізуватися та впроваджуватися в дію сучасні міжнародні стандарти, насамперед – серія міжнародних стандартів ISO/IEC 27000.

Сертифікування за стандартами також вимагає проведення регулярних аудиторських перевірок з метою забезпечення відповідності виконання вимог та належного функціонування процесу управління кібербезпекою. Це скорочує розрив, який зараз існує між різними нормативними актами та законодавством, допомагає переконати регулюючі органи, що організація постійно дотримується вимог законодавства.

Зміна нормативно-правової бази в сфері кібербезпеки – це виклик часу і тільки якнайскоріша модернізація організаційно-правового забезпечення дасть можливість забезпечити виконання поставленої задачі – сталого функціонування кіберпростору держави. Всупереч поширеній думці, безпека – це не стан, а процес.

Висновки.

1. Вважаємо, що існуюча нормативно-правова база у сфері кібербезпеки повинна бути істотно доповненою. На організаційно-правовому рівні необхідно чітко ідентифікувати проблему забезпечення кібербезпеки та своєчасно надавати нові, сучасні правові інструменти для протидії цим загрозам.

2. Пропонуємо внести зміни до Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" і на законодавчому рівні закріпити вимоги стандартів сімейства СМІБ для окремих категорій інформації, захист якої забезпечується законодавством України.

Використані джерела:

1. Юрій Котляров. Архітектура права сфери кібербезпеки в Україні. Електронний ресурс. URL: https://www.pressreader.com/ukraine/yurydychna-gazeta/20180515/ (дата звернення: 10.11.2020).

2. Живко З. Б., Рудий Т. В., Сеник В. В., Родченко С. С. Проблеми нормативно-правової бази забезпечення кібербезпеки в Україні: стан і перспективи / Соціально-правові студії: науково-аналітичний журнал / гол. ред. О. Балинська. Львів: ЛьвДУВС, 2020. Вип. 3 (9). С. 18-25.

3.Костенко О.В. Проблеми правового регулювання та розвиток кібернетичної безпеки України на сучасному етапі / Інформація і право. Науково-дослідний інститут інформатики і права Національної академії правових наук України. Київ. № 3(30)/2019. С. 96-104.

Каблуков А. О.
доцент кафедри медичної і фармацевтичної інформатики та новітніх технологій Запорізького державного медичного університету, к.т.н., доцент
Страхова О.П.
ассистент кафедри медичної і фармацевтичної інформатики та новітніх технологій Запорізького державного медичного університету, к.ф-м.н, асистент

ПІДГОТОВКА СПЕЦІАЛІСТІВ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ВУЗАХ МВС УКРАЇНИ

В результаті стрімкого розвитку комп'ютерних технологій і їх застосування в різних сферах нашого життя людство увійшло в нову еру інформатизації, коли комп'ютер є необхідним інструментом в самих різних сферах життєдіяльності людини.

Впровадження в управлінський процес і інші сфери життя суспільства електронно-обчислювальної техніки, без якої зберігання, обробка і використання величезної кількості найрізноманітнішої інформації було б неможливим, принесло неоціненну користь у розвиток науки, техніки та інших галузей знань. Однак

вигоди, які можна отримати завдяки використанню цієї техніки, стали використовуватися і в злочинних цілях. Так, з'явився новий вид злочинної діяльності - комп'ютерні злочини, суспільно-небезпечні наслідки, від здійснення яких не йшли в порівняння зі шкодою від інших злочинів.

За оцінками експертів правоохоронних органів країн Центральної та Східної Європи з питань боротьби з комп'ютерною злочинністю, прибутки злочинців від злочинів у сфері використання електронно-обчислювальних машин посідають третє місце після доходів наркоторговців і від продажу зброї, а завдані збитки вже зараз оцінюється мільярдами доларів. На 73-й сесії Генеральної асамблеї ООН генеральний секретар Антоніу Гутерреш оцінив щорічні збитки від кіберзлочинності в світі в розмірі 1500 млрд доларів.[1, с.1]

Україна, як і всі країни світу, щодня стикається з викликами в сфері кібербезпеки. Тільки за останні кілька років державні установи неодноразово атаковані з кіберпростору. За інформацією голови Департаменту кіберполіції Сергія Васильовича Демедюк, щорічно кількість кіберзлочинів в Україні збільшується в середньому на 2,5 тисячі. Згідно зі звітом, який міститься на сайті цього правоохоронного органу, в 2019 працівники Департаменту кіберполіції були залучені до розслідування більше 11 000 кримінальних проваджень, скоєних в сфері високих інформаційних технологій.[1, с.3].

Таким чином, вивчення проблем запобігання та розслідування злочинів у сфері комп'ютерної інформації виступає однією з найгостріших проблем сучасної криміналістичної науки.

Сьогодні, поліція по всьому світу має підрозділи по боротьбі з комп'ютерними злочинами, створюються спеціальні центри з навчання фахівців у цій галузі. Так Європейський Союз створив орган під назвою «Форум по кіберзлочинності». Безліч країн підписала Конвенцію Ради Європи щодо кіберзлочинності, яка намагається стандартизувати європейські закони, що стосуються злочинності в Інтернеті [2, С.3].

В Україні політика з кібербезпеки покладається на ряд державних органів, а саме на Державну службу спеціального зв'язку та захисту інформації України, Національної поліції України, Службу безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України. У кожному із зазначених органів діють відповідні підрозділи.

Наявність таких підрозділів в якійсь мірі дозволяє запобігати і розкривати кіберзлочини, однак сьогодні злочинні групи і спільноти для досягнення корисливих цілей все частіше застосовують системний підхід при плануванні своїх дій, розробляють оптимальні варіанти проведення і забезпечення кримінальних «операцій», створюють системи конспірації прихованим зв'язку, вживають додаткових заходів з надання ефективної протидії співробітникам правоохоронних органів, використовуючи сучасні технології і спеціальну техніку, в тому числі і різні комп'ютерні пристрої і нові інформаційно-обробні технології.

Таким чином, очевидно, що сьогодні однією з найважливіших проблем є забезпечення підрозділів поліції МВС України грамотними комп'ютерними

фахівцями. Співробітник поліції, який працює в областях пов'язаних із захистом секретної службової інформації, розслідуванням комп'ютерних злочинів і т.п. звичайно повинен володіти всіма необхідними навичками. Однак зараз, дуже часто, в цих областях працюють люди, які прийшли після закінчення цивільних ВНЗ, тому одним із пріоритетних напрямків розвитку освіти в МВС є навчання саме фахівців в комп'ютерній сфері.

В даний час тільки кілька відомчих вищих закладів МВС займаються підготовкою фахівців з кібербезпеки, а саме: Харківській національний університет внутрішніх справ, Дніпровський державний університет внутрішніх справ, Одеський державний університет внутрішніх справ. Аналіз результатів роботи МВС показує, що кількість фахівців з кібербезпеки, в МВС України, недостатньо для ефективної боротьби з даним видом злочинів. Для вирішення цієї проблеми необхідно в вузах МВС збільшити кількість студентв що навчаються за вищевказаною спеціальністю, а також створити курси підвищення кваліфікації з кібербезпеки для співробітників МВС, які курують цей напрям. Для курсів можна використовувати дистанційну форму навчання, що дозволить підвищувати кваліфікацію офіцерів за місцем служби. Найбільш доцільним для дистанційного навчання є використання сучасних хмарних технологій (Cloud computing), які забезпечують доступ до навчальних матеріалів протягом всього часу.

Висновок.

Для забезпечення ефективної боротьби з кіберзлочинами необхідно:

1. Вузам МВС підвищити кількість випускників за спеціальностями, пов'язаними з кіберзлочинами.

2. Створити курси підвищення кваліфікації для співробітників МВС, що працюють в підрозділах, що займаються кібербезпекою.

Використані джерела:

1. Кибербезопасность: начало эпохи новых видов преступлений// Информационный юридический портал Status-Quo.

(http://www.s-quo.com/ content/comment/ 288/7347/), 2019.

2. Д.Л. Шиндер. Компьютерная преступность - перед лицом проблемы // Центр исследования компьютерной преступности, 2010. (http://www.crime-research.ru/library/cybercrimes3.html).

3. А.Грабовий. Закон про кібербезпеку та стратегія кібербезпеки України// Електронне видання «Юрист & ЗАКОН», №26 -2017. (http://uz.ligazakon.ua/ua/magazine_article/EA010553).

Шинкарук О.М.
заслужений працівник освіти України, лауреат Державної премії України в галузі науки і техніки, д.т.н., професор Львівський Державний університет внутрішніх справ, проректор
Яшина О.М.
к.т.н., доцент кафедри Інженерії програмного забезпечення, доцент, Хмельницький національний університет.
Онишко О.Г.
к.пед.н., доцент кафедри Інженерії програмного забезпечення, доцент, Хмельницький національний університет

ФУНКІОНАЛЬНЕ ТЕСТУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНИХ СИСТЕМ

Сучасна діяльність переважної більшості структурних підрозділів Національної поліції України тісно пов'язана з широким використанням відомчих правоохоронних інформаційних систем (мереж, баз даних, тощо). Ефективність функціонування цих інформаційних систем (ІС) знаходиться в прямій залежності від якості програмного забезпечення (ПЗ), що покладено в основу їх розробки. Тому, одним із важливих етапів розробки ІС слід вважати тестування якості базового програмного забезпечення [1,2,3].

Збільшення функціональності ПЗ обумовлює необхідність застосування ефективних інструментів тестування. До таких інструментів відноситься автоматизоване функціональне тестування (АФТ), що поділяється на чотири категорії: тестування продуктивності, тестування безпеки, тестування точності, тестування надійності [4,5,6]. Інструменти автоматизованого функціонального тестування ПЗ сприяють полегшенню обробки інформації, обміну даними та інш. Отже, використання відповідного інструмента АФТ програмного забезпечення ефективно і дієво покращує процес тестування [7].

Пошук ефективних інструментів автоматизованого функціонального тестування ПЗ дозволив визначити такі основні показники, як: зручність і легкість використання; наявність технічної підтримки; простота установки та відтворення; графічний інтерфейс [8,9]. За даними показниками ефективності інструментів тестування ПЗ встановлено, що, до прикладу, автоматизована система функціонального тестування (АСФТ) *Appium* є відповідним інструментом тестування мобільних додатків платформи *Android*, в той час як АСФТ *Ranorex* слід вважати одним з найбільш ефективних інструментів тестування для веб-додатків. Також слід відмітити, що АСФТ *OpenScript* і *Selenium* є ефективними системами автоматизованого тестування фреймворків і браузерних додатків [10,11].

З метою визначення ефективних інструментів АСФТ програмного забезпечення авторами проведено відповідне тестування на різних етапах створення

програмних продуктів, що покладені в основу розробки певних ІС. За результатами даного тестування встановлено, що деякі інструменти АСФТ імітують середовище кінцевого виконання, як засіб прискорення виконання тесту, а деякі інструменти автоматизують розробку плану тестування, а інші досліджувані інструменти збирають дані щодо продуктивності. Тому, слід відмітити, що ефективність інструментів тестування залежить і від особливостей ПЗ. Так, деякі інструменти тестування можуть більше або менше ефективними в конкретних випадках тестування відповідного ПЗ. Дані обставини свідчать про те, що не існує одного ідеального інструменту для автоматизованого функціонального тестування базових програмних продуктів, які забезпечують функціонування ІС.

Таким чином, важливим етапом розробки ІС є функціональне тестування якості базового ПЗ, яке забезпечує ефективність функціонування впродовж життєвого циклу та гарантує відсутність помилок і дефектів. Тому для розробки базових програмних продуктів, що покладені в основу функціонування ІС для потреб структурних підрозділів Національної поліції України доцільно використовувати автоматизовані інструменти функціонального тестування.

Використані джерела:

[1] Pressman, R. S. (n.d.). Software engineePressman, R. S. (n.d.). Software engineering (2nd ed.). New York: McGraw-Hill Book Company.ring.

[2] Chauhan, R. K. & Singh, I. (2014).Latest Research and Development on Software Testing Techniques and Tools, 4(4), 2368–2372.

[3] Wala, T. & Sharma, A. K. (2014).Improvised Software Testing Tool, 3(9), 573–581.

[4] Merina, C. (2019). Tool Usability Parameter in Determining the Performance of Software Testing Tool, IJTB (International J. Technol. Business), 3(1), 8–18. [

[5] Jain, V. &Rajnish, K. (2018).Comparative Study of Software Automation Testing Tools: OpenScript and Selenium, Int. J. Eng. Res. Appl., 8(2), 29–33. https://doi.org/10.9790/9622-0802032933

[6] Odun-Ayo, I., Falade, A., & Samuel, V. (2018). Cloud Computing and Open Source Software: Issues and Developments, Lecture Notes in Engineering and Computer Science: Proceedings of The International MultiConference of Engineers and Computer Scientists 2018, 14-16 March, 2018, Hong Kong,140-145.

[7] Uppal, N. & Chopra, V., (2012).Design and Implementation in Selenium IDE with Web, Int. J. Comput. Appl., 46(12), 8–11.

[8] Santos, R. &Gehrke, K. (2017). Oracle ® Functional Testing OpenScriptProgrammer' s Reference.

[9] Kaur, H. & Gupta, G. (2013). Comparative Study of Automated Testing Tools: Selenium, Quick Test Professional and Testcomplete, Int. Journal of Engineering Research and Applications, 3(5), 1739–1743. [10] Mustafa, K. M., Al-Qutaish, R. E., &Muhairat, M. I. (2009). Classification of software testing tools based on the software testing methods, in 2009 International Conference on Computer and Electrical Engineering, ICCEE 2009, 1, 229–233.

[11] Kolli, R. (2016). An Empirical Study on Software Test Estimation.[15] Silverstein, M. (2003).Logical capture/replay. STQE Magazine, 5(6), 36–42.

Сервецький І.В.
професор кафедри
Національної безпеки
Міжрегіональної академії
управління персоналом,
доктор юридичних наук, доцент

ВИКОРИСТАННЯ ЕЛЕКТРОННИИИХ ДОКАЗІВ В ДІЯЛЬНОСТІ ПОЛІЦІЇ

Розвиток електронних технологій забезпечує використання у роботі поліції електронних доказів щодо пошуку і фіксації протиправної діяльності підозрюваних осіб. Тому однією з функцій успішної роботи поліції є процес пошуку і фіксація інформації, що утворились від цифрових слідів і використання її в доказуванні протиправної діяльності.

Д.О. Литкевич веде розмову про іноваційні технології та кримінальне процесуальне доказування протиправної діяльності [1].

І. О. Крицька розглядає «цифрову інформацію» як різнових речових доказів [2]

В.С. Петренкко веде розмову про «електронні докази» але обмежується цивільним процесом [3].

Так, Татаренко Г. В., Болгарєва К. В.,Татаренко Д. В. ведуть розмову відносно нового різновиду доказів – електронних доказів, які впроваджено в судовий процес у зв'язку із всеохоплюючою автоматизацією всіх сфер життя суспільства, внаслідок появи та широкого застосування новітніх інформаційних технологій. Більш детальному дослідженню та аналізу піддано такий засіб доказування в судовому процесі як електронний документ [4]

Так, М.Е. Шумило, Раймундас Юрка, Миколаса Ромеріса Вільнюс, В. А. Капліна ведуть розмову про інформаційну теорію доказів та електронних засобів доказування у кримінальному провадженні [5].

Серед вчених існують різні поняття та тлумачення щодо засобів пошуку та фіксації інформації різними категоріями співробітників поліції.

Як випливає із законодавчих актів у складі поліції функціонують: кримінальна поліція, патрульна поліція, органи досудового розслідування, поліція охорони, спеціальна поліція, поліція особливого призначення. Виконання різних функцій поліцією, таких як: превентивні, профілактичні, адміністративні, оперативно-розшукові, процесуальні тощо [6] змушує нас виробити єдине поняття, «електронний документ», «електронний підпис» та «електронний доказ», що є важливою складовою у ефективному пошуку та фіксації первинної інформації про протиправну діяльність підозрюваних осіб.

Тому, усі підрозділи повинні мати єдині способи пошуку і фіксації протиправної діяльності. Більше того, підрозділи кримінальної поліції здійснюють пошук і фіксацію інформації під час здійснення оперативно – розшукової діяльності, як гласно так і негласно, використовуючи при цьому специфічні технічні засоби

фіксації протиправної діяльності. Але не дивлячись на це, підрозділи кримінальної поліції повинні мати єдині як за формою, змістом і назвою єдине «електронне документування» та «електронне доказування», «електронний підпис» тощо . Це важливо тому, що будь- яка отримана інформація співробітником кримінальної поліції як до початку так і під час кримінального провадження може бути доказом протиправної діяльності [7].

На жаль, Український законодавець не закріпив та в певній мірі не врегулював проблеми, що існують в діяльності поліції.

Встановлено, що наразі в українському законодавстві присутній певний дисбаланс та відсутній єдиний підхід стосовно понять **електронних документів** як уніфікованого засобу фіксації інформації, що суттєво зменшує процес доказування, механізмів ідентифікації та автентифікації тощо.

Висновок. Законодавство та судова практика змушує нас до вироблення єдиного поняття електронних доказів та використання їх в роботі поліції.

У світі прослідковується єдиний підхід до спрощення вимог та умов роботи поліції, за яких електронний доказ може бути прийнятий та досліджений судом під час судового засідання за умови дотримання принципу вільної оцінки доказів нарівні з іншими засобами доказування, незважаючи на наявність чи відсутність на них окремих реквізитів чи електронного підпису тощо

Таким чином, відсутність єдиного підходу до роботи поліції значно знижує її ефективність, що призводить до втрат доказів або визнання їх недопустимими або неналежними, що призводить до неможливості доказати протиправну діяльність осіб, які вчиняють тяжкі та особливо тяжкі злочини.

Використані джерела:

1. Литкевич Д.О. іноваційні технології та кримінальне-процесуальне доказування: постановка проблеми. Національний юридичний університет ім. Ярослава Мудрого Науковий журнал. Право і суспільство. 2018. №.1. 113-118.

2. Інститут речових доказів за кримінальним процесуальним законодавством України та деяких зарубіжних країн: порівняльно-правовий аналіз / І. О. Крицька // Право і суспільство. - 2015. - № 5(3). - С. 169-174. - Режим доступу:http://nbuv.gov.ua/UJRN/Pis_2015_5%283%29__33

3. Петренко В.С. Електронні зокази як елемент інформаційних технологій у цивільному судочинстві. В. С. Петренко // Молодий вчений. - 2018. - № 1(1). - С. 111 115.- Режим доступу:http://nbuv.gov.ua/UJRN/molv_2018_1%281%29__29

4. Електронні документи як засіб доказування : сутність та правове регулювання / Г. В. Татаренко, К. В. Болгарєва, Д. В. Татаренко // Актуальні проблеми права : теорія і практика. - 2019. - № 1. - С. 111-119

5. Kaplina, V.A., Raimundas, J., & Shumylo, M.Ye. Informational theory of evidence and the problems of using the electronic means of proving in criminal procedure. Journal of the National Academy of Legal Sciences of Ukraine, (2019). 26(2), 118–130.

6. Про Національну поліцію. Закон України. //Відомості Верховної Ради (ВВР), 2015, № 40-41, ст.379)

7. Кримінальний процесуальний кодекс України. 2012 р. - К.: Істина, – 380 с.

Чучко Сергій Віталійович
ад'юнкт кафедри криміналістики та домедичної підготовки Дніпропетровського державного університету внутрішніх справ

ВІРТУАЛЬНІ (КОМП'ЮТЕРНІ) СЛІДИ ШАХРАЙСТВА, ПОВ'ЯЗАНОГО ІЗ ТОРГІВЛЕЮ ТОВАРАМИ ЧЕРЕЗ МЕРЕЖУ ІНТЕРНЕТ

Згідно традиційної думки, сліди у широкому розумінні розглядаються як будь-які зміни в середовищі, що виникають внаслідок вчинення злочинної діяльності. При чому, у класичному варіанті до недавнього часу всі сліди поділялися на дві групи: матеріальні та ідеальні.

В контексті сказаного не можна не визнати той факт, що за останні десятиріччя у криміналістиці з'явився третій вид слідів, який не відноситься ані до матеріальних, ані до ідеальних слідів. Аналіз криміналістичної літератури показав, що ця група слідів має різні назви: «комп'ютерні сліди», «віртуальні сліди», «інформаційні сліди», «електронні сліди» та ін. Вважаємо не принциповим застосування будь-якого із вказаних термінів, якщо вони повністю відображають сутність злочинів, вчинених внаслідок використання комп'ютерної мережі.

Віртуальні сліди розглядаються як будь-яка зміна стану автоматизованої інформаційної системи (утвореного нею «кібернетичного простору»), пов'язана з подією злочину та зафіксована у вигляді комп'ютерної інформації на матеріальному носії, у тому числі й на електромагнітному полі [1, с. 21].

В криміналістичній літературі можна виділити різні підходи до класифікації віртуальних (віртуальних) слідів.

Так, Я. Найдьон поділяє віртуальні сліди на 4 групи:

1) за походженням: електронна інформація, створена ЕОМ у процесі своєї роботи; електронна інформація, створена в процесі діяльності людини; похідна електронна інформація, створена комп'ютером на основі введених даних користувачем, або навпаки, інформація, створена з даних, згенерованих комп'ютерною системою;

2) за формою подання: інформація, доступна для сприйняття людиною; інформація, представлена у вигляді машинного коду;

3) за місцем зберігання: дані, що зберігаються в комп'ютерних системах; дані, скопійовані або переміщені користувачем на електронні носії (жорсткі диски, компакт-диски, накопичувачі); паперові копії (копії листування, скріншоти та ін.);

4) за формою: вихідні дані (інформація, введена людиною); бази даних; коди шифрування; програмне забезпечення різних видів; комп'ютерні системи [2, с. 305].

Деякі складові до такої класифікації додав Д. В. Бахтеєв. Вчений здійснив криміналістичну класифікацію цифрової доказової інформації за наступними критеріями:

- за формою носія: цифрові (віртуальні) сліди, розташовані на оптичних, напівпровідникових і магнітних носіях;
- за способом доступу: доступ до яких здійснюється локально або віддалено,

розміщені у відкритому доступі і захищені сліди;

- за місцем зберігання: у володінні злочинця (персональний комп'ютер, жорсткий диск, мобільний телефон), на пристроях потерпілого, свідка, сторонніх осіб та цифрові сліди, які одночасно зберігаються на пристроях усіх указаних осіб і в мережі Інтернет;

- за типом пристрою, на якому зберігаються цифрові сліди: стаціонарні і мобільні;

- за цільовим призначенням: шкідливі програми і корисні програми (додатки з різноманітними функціями, необхідні для здійснення тактичних операцій або дій, що допомагають у повсякденній діяльності, у побуті, роботі тощо) [3, с. 19].

Є. С. Хижняк звернув увагу, що А. Волєводза в основу класифікації віртуальних слідів взагалі обрав один єдиний критерій – фізичний носій «віртуального сліду». Зокрема: 1) сліди на жорсткому диску (вінчестері); 2) сліди на магнітній стрічці, оптичному диску (CD, DVD); 3) сліди в оперативних запам'ятовуючих пристроях (ОЗУ) ЕОМ; 4) сліди в ОЗУ периферійних пристроїв (лазерного принтера, наприклад); 5) сліди в ОЗУ комп'ютерних пристроїв зв'язку і мережевих пристроїв; 6) сліди у провідних, радіооптичних та інших електромагнітних системах і мережах зв'язку [4, с. 305]. Деякі вчені в основу класифікації покладають процесуальне положення суб'єкта: 1) сліди на комп'ютері злочинця; 2) сліди на комп'ютері жертви [5, с. 56]. Хоча, як на наш погляд, така класифікація є дещо узагальненою і не охоплює інші складові, наприклад, сліди у провідних та інших електромагнітних системах і мережах зв'язку та ін.

Аналізуючи наведені погляди на класифікацію можна побачити, що здебільшого вчені покладають в основу класифікації віртуальних (комп'ютерних) слідів такі критерії, як: місце зберігання, форма, походження та призначення.

Для більш повного розуміння суті шахрайських дій, вчинених при здійсненні цивільно-правових угод через мережу Інтернет, та слідів, які залишаються внаслідок таких дій, необхідно проаналізувати особливості діяльності сайтів і мобільних додатків, які слугують для спілкування між шахраєм та потерпілим.

Як повідомляють дослідники у напряму підвищення безпеки проведення фінансових операцій в мережі Інтернет, алгоритм фінансових операцій в мережі здебільшого відбувається у такий спосіб. Сайти надають можливість своїм користувачам виставляти лоти на продаж та вести торги за вже виставлені лоти. Для цього всі користувачі повинні: 1) зареєструватися на сайті – для кожного окремого інтернет порталу встановлюється адміністрацією порталу; 2) підтвердити реєстрацію; 3) виставити лот, встановивши його початкову вартість. Сайт виступає в якості посередника між продавцем та покупцем, надаючи «середовище» для проведення торгів. На більшості таких сайтах є можливість: − продивлятись фотографії лотів, їх відео-записи; − читати відгуки та коментарі стосовно певних лотів, осіб, що виставляють лоти (продавців) та осіб, що беруть участь в аукціоні як покупці, а також вести переписку між користувачами для обговорення деталей угоди (форма відправки товару, терміни відправки, форма сплати тощо). Відповідно до загально прийнятих правил після закінчення торгів продавець та покупець домовляються про спосіб передачі товару та форму сплати. Для цього покупцю

надсилаються контактні дані продавця [6, с. 153-154].

Отже, хід тривалого спілкування між шахраєм та потерпілим не є прихованим фактом, а може бути відображений у пам'яті електронних пристроїв, за допомогою яких передається інформація. Так, сліди у вигляді віртуальної переписки з питань купівлі-продажу товарів можуть міститися в електронній скриньці, куди надходить інформація від шахрая. Це можуть бути файли і папки зберігання вхідних та вихідних повідомлень електронної пошти, конфігурації поштової програми тощо.

На сторінці веб-сайту також можуть міститися віртуальні сліди (фотографії, відгуки та коментарі стосовно певних лотів, результати переписки між користувачами та продавцями тощо). Сліди можуть міститися й у історії голосових повідомленнях та і відеодзвінках (відеододатки Skype, Google Hangouts, Zoom тощо). Втім, найцінніша інформація криється у доменній адресі (Ip), що дозволяє встановити місцезнаходження точки доступу до комп'ютера, з якого здійснювалося спілкування.

Як справедливо наголошує Є. С. Хижняк, домен є головним атрибутом електронного документа, розміщеного в мережі Інтернет. Окрім домену, відіграє важливу роль й URL веб-сторінки, який завжди є індивідуальним, тому використовується як один із способів ідентифікації веб-сторінки, на якому розміщені електронні матеріали, що мають значення для розслідування [4, с. 83].

Як показав аналіз матеріалів кримінальних проваджень, у 62 % випадків шахрай та потерпілий зв'язувалися по телефону з метою обговорювання умов угоди купівлі-продажу товарів. Внаслідок чого в пам'яті мобільного телефону, в пам'яті SIM-карти, в пам'яті флеш-карти залишаються віртуальні сліди. Це можуть бути: сліди з'єднання, смс повідомлення, електронно-цифрові сліди у вигляді фотографій товару тощо.

Оскільки здебільшого шахраї і потерпілі обирають спосіб електронних розрахунків через електронні платіжні засоби та системи, електронні гаманці, інші види безготівкових розрахунків, у телефоні, в комп'ютері може міститися програмне забезпечення, звідки можна отримати слідову інформацію про проведені банківські операції. За таких обставин банківська карта, рахунок власника картки або рахунок телефонного номера виступають об'єктом слідоутворення.

Використані джерела:

1. Мещеряков В. А. Основы методики расследования преступлений в сфере компьютерной информации : автореф. дис. на соискание учен. степени доктора юрид. наук : спец. 12.00.09. Воронеж, 2001. 39 с.

2. Найдьон Я. Поняття та класифікація віртуальних слідів кіберзлочинів. *Підприємство,господарство і право*. 5/2019. С. 304-307.

3. Бахтеев Д.В. Криминалистическая классификация цифровой доказательственной информации. Криминалистика в условиях развития информационного общества (59-е ежегодные криминалистические чтения): сб. статей Международ. науч.- практ. конф. М.: Академия управления МВД России, 2018. С. 44–55.

4. Хижняк Є. С. Поняття віртуальних слідів та їх значення у процесі розслідування злочинів. *Актуальні проблеми держави і права*. 2017. С. 159-166.
5. Мочагин П.В. Виртуально-информационный процесс отражения следообразований как новое направление в криминалистике. *Вестник криминалистики*, 2013. № 3. С. 51–57.
6. Бойко А.О., Чещевий Є.І., Безрук В.В. Алгоритмізація процесу підвищення безпеки проведення фінансових операцій в мережі Інернет. *Вісник СумДУ. Серія "Економіка",* № 3' 2017. С. 152-158.

Пекарський С.П. доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки факультету № 1
Донецького юридичного інституту МВС України, кандидат юридичних наук

ВИКОРИСТАННЯ АВТОМАТИЗОВАНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОПЕРАТИВНОГО ПРИЗНАЧЕННЯ ЄДИНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ МВС

Стаття 25 Закону України «Про Національну поліцію» [1] визначає повноваження поліції у сфері інформаційно-аналітичного забезпечення. Відповідно до положень даної статті поліція в рамках інформаційно-аналітичної діяльності: формує бази (банки) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України; користується базами (банками) даних Міністерства внутрішніх справ України та інших органів державної влади; здійснює інформаційно-пошукову та інформаційно-аналітичну роботу; здійснює інформаційну взаємодію з іншими органами державної влади України, органами правопорядку іноземних держав та міжнародними організаціями.

На підставі зазначеного та відповідно до предмету даного дослідження проведемо аналіз використання автоматизованої інформаційної системи оперативного призначення єдиної інформаційної системи МВС. Так використання інформаційних технологій в діяльності Національної поліції має правову регламентацію. Зокрема, Законами України: «Про Національну поліцію», «Про оперативно-розшукову діяльність», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про державну таємницю», тощо визначені повноваження кримінальної поліції щодо використання інформаційних технологій. Окрім того, Положення про автоматизовану інформаційну систему оперативного призначення єдиної інформаційної системи МВС, яке затверджено наказом МВС України від 20.10.2017 № 870 [2] визначає основні завдання, функції,

інформаційні ресурси, суб'єктів, структуру автоматизованої інформаційної системи оперативного призначення єдиної інформаційної системи МВС (далі - АІС ОП), яка є сукупністю програмно-технічних і телекомунікаційних засобів та призначена для накопичення й обробки відомостей, що утворюються в процесі оперативно-розшукової діяльності Національної поліції України. Безпосередньо АІС ОП утворена для наповнення та підтримки в актуальному стані бази даних єдиної інформаційної системи МВС та є її складовою частиною. На нашу думку АІС ОП має важливе значення для забезпечення діяльності територіальних та міжрегіональних підрозділів кримінальної поліції, оскільки основними завданнями її є:

- підвищення рівня інформаційно-аналітичного забезпечення оперативно-розшукової діяльності Національної поліції України;
- забезпечення процесу підтримки управлінських рішень керівництвом Національної поліції України;
- об'єднання отриманої в процесі оперативно-розшукової діяльності Національної поліції України інформації в єдиному інформаційному просторі з використанням сучасних інформаційних технологій, комп'ютерного і телекомунікаційного обладнання;
- протидія злочинності та проведення профілактичної роботи, спрямованої на запобігання вчиненню правопорушень [2].

До функції АІС ОП відноситься::

- автоматизація процесів обліку отриманої в процесі оперативно-розшукової діяльності Національної поліції України інформації;
- збір, зберігання, пошук та узагальнення інформації;
- відображення повнотекстової, графічної, табличної та статистичної інформації, а також фото- і відеозображень;
- утворення електронного досьє;
- формалізація технологічних процесів обробки інформації, визначення типових маршрутних технологічних схем для їх виконання;
- забезпечення надійного зберігання інформаційних обліків та їх систематизація;
- забезпечення комплексного захисту інформації та розмежування доступу до інформації, що зберігається в АІС ОП [2].

Розпорядником інформації, яка обробляється в АІС ОП, є Національна поліція України, яка вживає заходів із організації матеріально-технічного та кадрового забезпечення, що необхідні для ефективного функціонування системи. Своєю чергою розпорядником АІС ОП є Департамент кримінального аналізу, який забезпечує управління (адміністрування) АІС ОП, контроль за формуванням та підтриманням в актуальному стані інформаційних ресурсів, надання користувачам прав доступу до АІС ОП, ведення їх обліку, ужиття заходів щодо розвитку і вдосконалення АІС ОП. Своєю чергою системним адміністратором центрального вузла АІС ОП є працівник ДКА, який згідно зі своїми функціональними (посадовими) обов'язками відповідає за експлуатацію програмно-технічного комплексу АІС ОП. Системний адміністратор центрального вузла АІС ОП

координує діяльність системних адміністраторів регіональних вузлів та відповідає за:

- цілодобове функціонування програмно-технічного комплексу АІС ОП;
- підключення нових або відключення існуючих апаратних модулів;
- резервне копіювання системи;
- інсталяцію програмних продуктів;
- діагностику системи [2].

Користувачами АІС ОП є посадові особи Національної поліції України, яким в установленому порядку надано право наповнювати, підтримувати в актуальному стані та використовувати інформаційні ресурси АІС ОП. Також користувачі АІС ОП відповідають за достовірність інформації, що вводиться ними до АІС ОП, та зобов'язуються не розголошувати у будь-який спосіб інформацію, що міститься у системі, крім випадків, передбачених законодавством України.

АІС ОП має свою структуру, яка побудована на двох рівнях. Перший рівень - центральний вузол АІС ОП, який розташовується в службових приміщеннях ДКА, де накопичується та систематизується узагальнена інформація, здобута в результаті оперативно-розшукової діяльності Національної поліції України. Другий рівень становлять регіональні (обласні) вузли АІС ОП, які розташовуються в службових приміщеннях, де накопичується та систематизується інформація, здобута в результаті оперативно-розшукової діяльності Національної поліції України, за територіальним принципом [2].

Отже, інформаційними ресурсами АІС ОП є об'єктивно поєднаний набір відомостей, що безпосередньо стосуються осіб та подій (кримінальних правопорушень), які накопичуються в процесі здійснення оперативно-розшукової діяльності Національної поліції України. Саме тому обліку в АІС ОП підлягають відомості про осіб, відносно яких заведено оперативно-розшукові справи, отримані від осіб, які конфіденційно співробітничають з оперативними підрозділами Національної поліції України та в ході проведення оперативно-розшукових заходів у рамках оперативно-розшукових справ. Безпосередньо інформація про особу надається на запит органів досудового розслідування, прокуратури та суду. Найвищим ступенем обмеження доступу до інформації, що обробляється в АІС ОП, є ступінь секретності «таємно» [2].

Підводячи підсумок слід зазначити, що інформаційні ресурси АІС ОП є складовою державних інформаційних ресурсів та сприяють підрозділам кримінальної поліції накопичувати та обробляти відомості, що утворюються в процесі оперативно-розшукової діяльності.

Використані джерела:

1. Про Національну поліцію : Закон України від 2 липня 2015 року № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text

2. Про затвердження Положення про автоматизовану інформаційну систему оперативного призначення єдиної інформаційної системи МВС: наказ МВС України від 20.10.2017 № 870. URL: https://zakon.rada.gov.ua/laws/show/ z1433-17#n13

Бабанін С.В.
доцент кафедри кримінального права та кримінології Дніпропетровського державного університету внутрішніх справ, к.ю.н., доцент

КРИМІНАЛЬНО-ПРАВОВИЙ ЗАХИСТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В УКРАЇНІ

Одним з завдань розділу XVI «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» Особливої частини КК України є забезпечення кримінально-правового захисту інформаційних технологій в Україні. Ефективність такого захисту залежить, зокрема, від якості законодавчої техніки, яка застосовується у процесі розробки диспозицій відповідних норм вказаного розділу КК України (описі об'єктивних та суб'єктивних ознак кримінальних правопорушень у цій сфері).

На наш погляд, конструкція норм розділу XVI Особливої частини КК України далека від досконалості.

Аналіз диспозицій ст.ст. 361-363[1] КК України свідчить про їх неконкретність щодо визначення ознак суспільно небезпечних діянь у сфері інформаційних технологій та їх наслідків, що, у свою чергу, дозволяє надавати достатньо широке тлумачення цих об'єктивних ознак і, відповідно, дезорієнтує практичного працівника при вирішенні питання кваліфікації таких діянь і притягнення особи до відповідальності.

Так, ч. 1 ст. 361 КК передбачає відповідальність за несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації [1].

На сьогодні комп'ютери у своїй власності має чи не кожна родина, підприємство, установа, організація. Під ознаки ч. 1 ст. 361 КК підпадає будь-яке діяння, пов'язане з несанкціонованим втручанням в роботу будь-якого комп'ютера, що призвело до відповідного наслідку. Тому, наприклад, формально за ч. 1 ст. 361 КК слід кваліфікувати дії студента, який з ноутбука свого товариша без його відома шляхом вільного доступу «зкачав» будь-яку інформацію (фільм, фотографію, курсову роботу тощо). Проте таке діяння, на нашу думку, не становить достатнього для криміналізації ступеня суспільної небезпеки.

Пропонуємо передбачити у цій статті відповідальність за: 1) комп'ютерне шпигунство, що полягає у незаконному доступі до інформації, а також незаконне одержання інформації, яка має відношення до державної безпеки, міжнародних відносин і питань атомної енергетики України; 2) незаконний доступ до інформації Офісу Президента України, Кабінету Міністрів України, Верховної Ради України, міністерств та відомств України, а також незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних

мереж чи мереж електрозв'язку цих органів.

Крім того, пропонуємо: 1) надати нормативне визначення поняття «комп'ютерні кримінальні правопорушення», до яких віднести не лише кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (ст.ст. 361-363[1] КК України), а й ряд кримінальних правопорушень, передбачених іншими розділами Особливої частини КК України (ст. 301 «Ввезення, виготовлення, збут і розповсюдження порнографічних предметів» та ін.); 2) класифікувати поширені види шкоди у сфері інформаційних технологій та передбачити відповідальність за її заподіяння залежно від ступеня тяжкості у кваліфікованих та особливо кваліфікованих складах кримінальних правопорушень розділу XVI «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» Особливої частини КК України.

У зв'язку з поширенням у мережі Інтернет такого суспільно небезпечного явища як розміщення підроблених сайтів з метою заволодіння конфіденційною інформацією пропонуємо передбачити у розділі XVI Особливої частини КК України відповідальність за розміщення веб-ресурсів в мережі Інтернет з метою незаконного заволодіння персональними або автентифікаційними даними, реквізитами платіжних карток, банківських рахунків.

Використані джерела:

1. Кримінальний кодекс України: Закон України від 05 квітня 2001 р. / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 14.11.2020).

Рижков Е.В., завідувач кафедри економічної та інформаційної безпеки,, к.ю.н., доцент
Мирошниченко В.О., професор кафедри к.т.н., доцент

ПАТЕНТНА ДІЯЛЬНІСТЬ ЯК ПРЕДМЕТ ТРАНСФЕРУ ТЕХНОЛОГІЇ (НА ПРИКЛАДІ ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ «ПРИСТРІЙ РАДІОЛОКАЦІЙНОГО РОЗПІЗНАВАННЯ ОБ'ЄКТІВ»)

Патентна діяльність науково-педагогічних колективів у навчальних закладах зі специфічними умовами навчання є невід'ємною складовою їх загальної діяльності.

В кожному закладі є свої винахідницькі напрацювання, які з часом породжують свій профіль, традиції та школи.

За результатами роботи відповідних комісій колективу Дніпропетровського державного університету внутрішніх справ другий рік поспіль вдається досягти

лідерства у цій номінації Конкурсу на кращу наукову, науково-технічну та профорієнтаційну продукцію в системі МВС України [1]. Цього разу з патентом на корисну модель «Пристрій радіолокаційного розпізнавання об'єктів» [2].

Фаховий рішень авторів патенту дозволив опрацювати один із пріоритетних напрямів обороноздатності держави в умовах військового протистояння на Сході країни.

На теперішній час для України вкрай актуальним є питання підвищення бойової готовності збройних сил та переоснащення і розробка нових видів військової техніки. Запропонований патент на корисну модель відноситься до галузі радіолокації і може бути використаний для розпізнавання належності виявлених радіолокаційних об'єктів.

Відомі способи розпізнавання об'єктів полягають в тому, що на запитнику та відповідачі формуються синхронні шкали часу системи розпізнавання, за кодом яких на запитнику і на відповідачі визначають діючи коди сигналів запиту та відповіді. Запитником випромінюють кодовий сигнал запиту, код якого визначають за кодом шкали часу системи розпізнавання, який приймають відповідачем та порівнюють його з діючим кодованим сигналом запиту в даний момент часу. Код сигналу відповіді визначають за кодом шкали часу системи розпізнавання, який приймають запитником і порівнюють його з діючим сигналом відповіді в даний момент часу і за результатом порівняння видають сигнал розпізнавання. Недоліком такого способу обробки сигналів запитника та відповідача є те, що робота синхронізаторів запитника та відповідача вимагає чіткої синхронізації, які ніяким чином не мають гальванічного або іншого зв'язку між собою та знаходяться на різних об'єктах на значному віддалені друг від друга, що може приводити до помилок у розпізнаванні рухомих об'єктів.

В основу корисної моделі поставлена задача підвищення надійності ідентифікації радіолокаційних об'єктів шляхом забезпечення примусової синхронізації зміни шкали часу запитника та відповідача за допомогою сигналів точного часу з супутників GPS системи, які мають дуже велику точність. Введення додаткових блоків дозволяє виключити неспівпадіння часових шкал запитника та відповідача, що в свою чергу дозволить вирішити поставлену задачу.

Поставлена задача вирішується за рахунок того, що у запитник та відповідач додатково введені GPS приймачі з відповідними GPS антенами та селекторами часу GPS сигналу, які забезпечують примусову синхронізацію роботи формувачів шкал часу запитника та відповідача, які знаходяться на різних об'єктах на значній відстані друг від друга, за допомогою синхронізаторів.

Перевагами запропонованого пристрою у порівнянні з відомими є підвищена надійність розпізнавання рухомих об'єктів.

Автори патенту цілком розуміють частковість вирішення завдання щодо досягнення цілей патентної діяльності із завершенням етапу патентування самої ідеї.

Не менш значущим є етап трансферу, тобто запуск патенту у виробництво. Вважаємо, що цей сегмент діяльності потребує свого вивчення, засвоєння та безумовної реалізації [3].

З часом трансфер технологій у навчальних закладах системи МВС України за

умов підтримки з боку керівництва Національної поліції та Міністерства повинен стати нормою задля досягнення успіху у вдосконаленні правоохоронної діяльності та підвищенні обороноздатності країни через втілення патентів у виробництво.

Використані джерела:

1. Конкурс на кращу наукову, науково-технічну та профорієнтаційну продукцію в системі МВС України URL:https://www.naiau.kiev.ua/news/konkurs-na-krashhu-naukovu-naukovo-tehnichnu-ta-proforiyentacijnu-produkciyu-v-sistemi-mvs-ukrayini.html
2. Пристрій радіолокаційного розпізнавання об’єктів [Гавриш О.С., Махницький О.В., Мирошниченко В.О., Рижков Е.В., Фоменко А.Є.] Патент та корисну модель № 139240 МПК G01S 13/00, G01S 13/52 (2006.01)., Бюл. № 24/2019., 26.12.2019
3. Андрощук Г.О. Трансфер технологій в обороннопромисловому комплексі України: проблемні питання (І частина) // Наука, технології, інновації. - 2018. - № 1. - С. 62-71

Виганяйло С.М. доцент кафедри соціально-економічних дисциплін Сумської філії Харківського національного університету внутрішніх справ, к.е.н.

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ПІДТРИМКИ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Інформаційні технології невпинно впливають на всі сфери діяльності діяльності людини, не виключенням на сьогоднішній момент є і підприємницька діяльність.

Однак наряду з позитивними впливами (управління діяльністю підприємства, облік, планування, обмін інформацією, використання програм обліку чи обміну податковими накладними, аж до повного переведення функціонування бізнесу у автоматичний режим Інтернет-магазини) існує низка загроз (інформація не завжди є точною та достовірною, і вимагає додаткового аналізу, з’являється зовнішня загроза інформаційній безпеці підприємства, конкуренти можуть вільно отримати інформацію з мережі Інтернет та використовувати її на свій розсуд).

В таких умовах доцільно використовувати наступні інформаційні технології захисту інформації:

1) Використання електронного цифрового підпису;
2) Використання «хмарних» технологій - Cloud computing,(віддалене зберігання та обробка даних);
3) Створення віртуальних підприємств (група підприємств, які працюють над

виконанням одного завдання вєдиному інформаційному просторі);

4) Використання спеціального програмного забезпечення для створення бізнес-плану із формуванням звіту з описом проекту (важливо те що послуга складання бізнес-плану не замовляється у спеціалізованих компаній, таким чином неває витоку інформації);

5) Використання корпоративного порталу (так званий інтранет);

6) Використання корпоративних соцмереж. [1]

Переваги використання інформаційних технологій: легкість доступу, збереження та захист інформації, економічний ефект і висока якість послуг, забезпечення спільної віддаленої роботи, неможливість рейдерського захоплення бізнесу.

Використання інформаційних технологій (особливо для малого та середнього бізнесу) для досягнення економічної безпеки підприємства дозволяє суттєво економити кошти та організовувати цілісність збереження важливої економічної інформації, а іноді і збереження працездатності підприємства.

Використані джерела:

1. Колешня Я.А. Особенности оценки экономической безопасности малых и средних предприятий / Я.А. Колешня // Fundamental and applied sciences today VIII: Proceedings of the Conference. North Charleston, 10-11.05.2016, Vol.2 — North Charleston, SC, USA:CreateSpace, 2016, p. 159

Корнейко О.В.
завідувач кафедри інформаційних технологій та кібербезпеки ННІ № 1 НАВС, к.т.н., професор
Школьніков В.І.
старший викладач кафедри інформаційних технологій та кібербезпеки ННІ № 1 НАВС, т.в.о. начальника Центру кримінальної аналітики НАВС

ДОСВІД НАЦІОНАЛЬНОЇ АКАДЕМІЇ ВНУТРІШНІХ СПРАВ ЩОДО ПІДГОТОВКИ ФАХІВЦІВ У СФЕРІ КРИМІНАЛЬНОЇ АНАЛІТИКИ ТА ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Широке впровадження сучасних інформаційних технологій (ІТ) в усі сфери суспільного життя дуально впливає на сферу правоохоронної діяльності. З одного боку, ІТ є реальним інструментарієм, що допомагає Національній поліції України (НПУ) виконувати свої завдання щодо протидії злочинності, забезпечення публічної безпеки і порядку, охорони прав і свобод людини, а також інтересів суспільства і

держави. З іншого боку, широке застосування ІТ у вчиненні правопорушень, в тому числі у кіберпросторі держави, накладає свої особливості на попередження та протидію цим правопорушенням НПУ.

Тому Національна академія внутрішніх справ (НАВС), як заклад вищої освіти (ЗВО) системи МВС України, впроваджує в навчальний процес спеціалізовані навчальні дисципліни у сфері ІТ та протидії кіберзлочинності.

Так, ще у 2011-2015 роках кафедра інформаційних технологій НАВС здійснювала планову підготовку (щорічно однієї навчальної групи) за замовою МВС України фахівців по досудовому розслідуванню злочинів, що пов'язані з використанням ІТ. Після впровадження спеціальності 125 «Кібербезпека» та відповідної спеціалізації для слідчих підрозділів у Харківському національному університеті внутрішніх справ така планова підготовка фахівців в НАВС була призупинена.

З 2017 року, з заснуванням відповідного управління в НПУ широкий розвиток отримала технологія кримінального аналізу в діяльності поліції щодо попередження та розслідування злочинів. Тому в НАВС на базі кафедри фінансової безпеки та фінансових розслідувань у 2017-2020 роках відбувалась планова підготовка фахівців у сфері кримінального аналізу.

Також у 2017 році за рішенням ректорату НАВС кафедра інформаційних технологій була реформована в кафедру інформаційних технологій та кібербезпеки (КІТКБ), що наклала відповідний відбиток на її діяльність.

Так, навесні 2018 року КІТКБ провела 2-х місячний експериментальний тренінг в об'ємі 230 аудиторних годин для 44 курсантів 4-го курсу НАВС з сучасних ІТ, забезпечення кібербезпеки, протидії кіберзлочинності та основ ведення оперативно-розшукової діяльності (ОРД) в кіберпросторі.

За результатами доопрацювання навчальних дисциплін цього тренінгу у 2018-2019, 2019-2020 навчальних роках на КІТКБ проводилась планова підготовка курсантів, які навчались в НАВС для комплектування органів досудового розслідувань НПУ, з розширенням їх фахових компетенцій у сфері інформаційно-аналітичної підтримки слідчої діяльності. А з цього навчального року така підготовка здійснюється на КІТКБ та кафедрі оперативно-розшукової діяльності для здобувачів НАВС, які навчаються для комплектування підрозділів кримінальної поліції.

Під час навчання в НАВС, разом з опануванням традиційних для ЗВО дисциплін для оперативників НПУ, зазначені 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);

– основам здійснення оперативно-технічного документування при протидії кримінальним правопорушенням в сучасних умовах з використанням оперативних та оперативно-технічних заходів, засобів тощо;

– 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 підтримки цієї освітньої діяльності на підставі рішення Вченої ради НАВС від 07.07.2020 та за підтримки керівництва Департаменту кримінального аналізу НПУ 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 новітніх ІТ в практичну діяльність НПУ, підтримання курсантської молоді НАВС в задоволенні їхніх наукових інтересів у сфері кримінального аналізу та кіберрозвідки.

Бочковий О.В.
завідувач навчально-наукової лабораторії
з дослідження проблем превентивної діяльності
факультету підготовки фахівців
для підрозділів превентивної діяльності
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук,
старший науковий співробітник

МЕДІЙНА СКЛАДОВА ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ В УКРАЇНІ

Ми живемо у світі, в якому люди переважну більшість свого часу проводять у соціальних мережах. Враховуючи цей аспект, практично кожен державний орган чи

підрозділ, з метою інформування населення про свою діяльність створюють свої сторінки у соціальних мережах.

Разом з тим, гортаючи стрічку новин, наприклад у Фейсбук, часто натикаєшся на різноманітні викриття та розслідування щодо незаконної діяльності як представників влади так і інших осіб, які проводяться журналістами та громадськими активістами. При цьому, масштаби розслідування та резонанс більші ніж викриття правоохоронних органів.

У зв'язку з цим постає питання: чи конспіративний характер діяльності правоохоронних органів не дозволяє висвітлювати результати їх діяльності, чи їх діяльність менш ефективна ніж діяльність журналістів та активістів?

Разом з тим, аналіз показників правоохоронних органів, так само як і реєстр судових рішень щодо притягнення осіб до відповідальності не дозволяє говорити про достатню ефективність правоохоронних органів у протидії з організованою злочинністю чи корупцією.

Звісно, частина опублікованої у соціальних мережах інформації є або «інформаційним сміттям», або сфабрикованим матеріалом для дискредитація особи з політичних, економічних чи інших мотивів. Та щодо частини таких матеріалів, як показують останні події, керівництво приймає кадрові рішення (зокрема, фігуранта нещодавнього журналістського розслідування начальника УСБУ в Миколаївській області звільнили з займаної посади).

Виявляється, що діяльність журналістів, які не мають юридичних та технічних можливостей проводити негласні заходи ефективніша ніж діяльність правоохоронних органів, які наділені вищевказаними можливостями, у тому числі й підрозділів СБУ, які повинні виявляти порушення закону всередині структури.

При цьому, дивуватися можливостям журналістів не приходиться, адже не секрет, що Google записує наші розмови, які здійснюються за допомогою програмних продуктів, а Facebook вмикає камери та мікрофони мобільних пристроїв для збору інформації в комерційних цілях. Загроза витоку такої інформації чи потрапляння її до рук зловмисників також, нажаль, може мати місце [7].

Практично кожна особа залишає за собою електронний слід інформації Залишатися сьогодні поза недійного чи Інтернет простору дуже складно, часто навіть неможливо. Правоохоронні органи зарубіжних країн, у зв'язку з цим, широко використовують автоматизовані інформаційно-пошукові системи, які дозволяють значно оптимізувати розкриття та розслідування злочинів, учинених членами організованих угруповань [1, С. 57].

Більше того, новітні технології дають змогу активно та продуктивно протидіяти транснаціональній злочинності за рахунок відсутності кордонів у глобальній мережі. Значно полегшується взаємодія та обмін даними між правоохоронними органами різних країн. Наприклад, розшукуваний злочинець може бути встановлений шляхом застосування однієї з програм ідентифікації особи по фото чи відео зображенню [2; 3; 4].

Донедавна фантастичні уявлення щодо прогнозування злочинності знаходять своє відображення у реальних дослідженнях. Зокрема, у США та Японії вже почали тестувати програми передбачення злочинів із залученням штучного інтелекту [5; 6].

Ми є свідками виникнення нових відносин у сфері комп'ютерних технологій й робототехніки, більшість приватних та державних структур переходять на автоматичне адміністрування, запроваджується технологія блокчейн, тощо. Вже існують технології, котрі допомагають автоматично аналізувати величезні масиви текстів, причому проводити не структурний аналіз та пошук ключових слів, а семантичний. Система фактично розуміє зміст текстів. У перспективі цей самий підхід може використовуватись для аналізу відео- та статичного зображення, а також звуку.

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

Таким чином, хочемо наголосити на необхідності переформатування діяльності правоохоронних органів й поширеного використання сучасних можливостей як медійного простору так і інформаційно-технічних ресурсів у зборі та аналізі інформації, що може бути використана під час виявлення та розслідуванні правопорушень. Час перейти від декларативних до реальних кроків щодо запровадження сучасних інформаційно-аналітичних систем у діяльність правоохоронних органів, зменшивши при цьому бюрократичний вплив на вказані процеси та.

Використані джерела:

1. Гуславский В.С. Информационно-аналитическое обеспечение раскрытия и расследования преступлений: монография / В.С. Гуславский, Ю.А. Задорожный, Б.Г. Розовский. Луганск: Элтон-2, 2008. 287 с.

2. Поиск человека по фотографии – это реальность URL: http://softopirat.com/main/399-poisk-cheloveka-po-fotografii-yeto-realnost.html.

3. По фото в соцсети можно узнать о человеке все! URL: http://3rm.info/publications/13829-po-foto-v-socseti-mozhno-uznat-o-cheloveke-vse.html

4. Создана программа для поиска человека в Интернете по фото URL: http://zhzh.info/blog/2011-11-13-3096.

5. Илюхин Олег В США втайне от граждан испытали технологию предсказания преступлений URL:https://hitech.vesti.ru/article/781523/

6. Японская полиция будет использовать искусственный интеллект для предсказания преступлений URL: http://tass.ru/obschestvo/4910175

7. Константин Шиян. Google постоянно подслушивает вас через микрофон. Вот как найти эти записи! URL: https://lifter.com.ua/628/Google-postoyanno-podslushivaet-vas-cherez-mikrofon-Vot-kak-nayti-eti-zapisi

Страхова О.П. асистент кафедри медичної і фармацевтичної інформатики та новітніх технологій Запорізького державного медичного університету, к.ф-м.н.
Каблуков А. О. доцент кафедри медичної і фармацевтичної інформатики та новітніх технологій Запорізького державного медичного університету, к.т.н., доцент

ПЕРЕВАГИ ЗАСТОСУВАННЯ ХМАРНИХ ТЕХНОЛОГІЙ У ІНФОРМАЦІЙНИХ МЕРЕЖАХ МВС УКРАЇНИ

Одним з основних трендів розвитку комп'ютерних інформаційних технологій, що набувають все більшої популярності, останнім часом стають так звані хмарні технології. Хмарні технології дозволяють створити спеціалізоване віртуальне робоче середовище в Інтернеті або в корпоративній комп'ютерній мережі, що надає необхідні обчислювальні ресурси і програмний інструментарій для вирішення певного класу задач.

Переваги хмарних технологій полягають в можливості доступу до необхідної інформації з будь-якого комп'ютера, підключеного до Інтернету (комп'ютерної мережі), водночас унеможливлення доступу сторонніх осіб до рухливих і кодованих даних. Сюди ж можна віднести безперервне забезпечення актуальності інформації, в залежності від призначення сервісу і потреби інформація може оновлюватися у дуже короткі проміжки часу; можливість одночасного перегляду та редагування однієї і тієї ж інформації декількома користувачами. Такі зручності значною мірою прискорять і полегшать роботу експертів з різних питань що виникають при роботі підрозділів МВС України. Водночас, віртуалізація обчислювальних ресурсів, перехід до технології хмарних сервісів значно знижує експлуатаційні витрати.

Подальший розвиток інформатизації діяльності підрозділів МВС на базі хмарних інформаційних технологій, створення корпоративних хмар, можливо, полягає у створенні інформаційного та інструментального професійного середовища для роботи різноманітних експертів. Оперативність роботи при цьому зростає через зникнення необхідністі в пересиланні файлів з будь-якою інформацією один одному. Чинна інформація зберігається на так званому хмарному сервері, що може фізично являти собою з’єднану за допомогою протоколів хмарних технологій сукупність серверів, розподілених в мережі. Інформація обробляється і зберігається в хмарі, і з позиції клієнта є один великий віртуальний сервер, незважаючи жодною мірою на те, що фізично ці сервери можуть перебувати між собою на великій відстані, навіть на різних континентах.

В процесі роботи різних підрозділів МВС є необхідність оперувати величезною кількістю різноманітної як довідково-допоміжної, так і чисто криміналістичної інформації. Це спонукає створювати комп’ютерні мережеві банки даних, та спеціалізовані експертні інформаційні системи. З метою раціонального використання вже існуючих напрацювань програмного забезпечення, можливо,

потрібно провести взаємоузгоджене об'єднання і зберігання об'єктів обліку, банків даних, що знаходяться в різних інформаційних системах, створити загальну систему нормативно-довідкової інформації, класифікації та кодування, організувати взаємозв'язок інформаційних систем.

Тут досить зримо проявляється перевага хмарних технологій зберігання даних, що дозволяють здійснювати доступ до віддалених баз даних і використовувати інформаційну потужність хмарних серверів з мобільних пристроїв будь-якого типу.

Мирошниченко В.О.
професор кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ,
к.т.н., доцент

ПЕРСПЕКТИВИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КЛІЄНТІВ У ФІНАНСОВІЙ СФЕРІ

У міру того як світ стає все більш цифровим, кількість паролів, які люди повинні пам'ятати, стає серйозною проблемою. Фінансові установи поступово змушені вивчати прийнятні альтернативи біометричної аутентифікації користувачів і врівноважувати обидві важливі змінні: простоту і безпеку.

Суть проблеми полягає в тому, що чим більше сервісів ми використовуємо, тим більше паролів ми змушені запам'ятовувати. Фактично, за оцінками дослідників, протягом наступних п'яти років у кожної людини буде в середньому понад 200 облікових записів, які потребують паролів. Управління зростаючою кількістю паролів стає проблемою майже для всіх користувачів. У відповідь ми можемо спостерігати кілька різних підходів до цього:

• Використання однакових паролів для всіх облікових записів. Очевидно, це найгірше через «ефекту доміно», яке призводить до злому одного аккаунта при атаці.

• Використання різних варіантів паролів. Це поєднання більш високого рівня безпеки з відносною простотою.

• Використання технологій, які генерують надійні паролі. Це найбезпечніший варіант, але і самий громіздкий у використанні.

Згідно з дослідженням, проведеним компанією TeleSign [1], яка забезпечує захист найбільших онлайн-майданчиків, мобільних додатків і хмарних систем, встановлюючи і перевіряючи мобільну ідентифікацію, 73% дорослого населення США і Великобританії використовують один і той же пароль для всього. Крім того, більше половини користувачів (54%) використовують п'ять або менше паролів, а

22% використовують тільки три або менше. Майже половина (47%) покладаються на паролі, які не змінювали п'ять років.

Для фінансових організацій однією з основних цілей оцифровки є спрощення їх банківських операцій. У спробі поліпшити взаємодію з користувачем однієї з пасток є процес перевірки пароля, необхідного для доступу до мобільного банкінгу. Однак поєднання необхідності підвищення безпеки доступу до облікового запису і прагнення до більшої простоті ускладнює балансування.

Якщо перейти від різних варіантів введення імені користувача і пароля до можливості аутентифікації користувачів по відбитку пальця, це усуне проблему перевантаження з кількістю паролів, які необхідно запам'ятати. Використовуючи біометрію, можна отримати доступ до електронної пошти, онлайн-банку, хмарним сховищам або іншим он-лайн сервісам. Паролем можна поділитися або його вкрасти, але з відбитком пальця все набагато гірше.

Технології відбитків пальців пережили значний бум за останні три роки. В даний час, за оцінками дослідників, близько 31% людей у віці від 18 до 24 років використовують біометричні технології на своїх смартфонах. Однак не є винятком і всі інші користувачі смартфонів, у яких коефіцієнт використання датчика відбитків пальців становить 8%. Дуже ймовірно, що біометрія поширеться і на більш дешеві мобільні телефони.

Поряд з технологією відбитків пальців, великі банки все частіше пропонують клієнтам можливість використовувати голосове керування, сітківку ока та інші біометричні параметри для доступу до своїх рахунків замість паролів. Мета полягає в тому, щоб підвищити безпеку клієнта на додаток до його комфорту. Біометричну аутентифікацію складно імітувати, а клієнтам дуже легко її використовувати. Інноваційні рішення в цій сфері пропонує американська кампанія USAA [2], яка займається наданням банківських послуг, інвестицій, страхуванням і пенсійним обслуговуванням для людей і сімей, які служать або служили в збройних силах Сполучених Штатів. У лютому 2015 року USAA розробила технологію розпізнавання осіб для цілей мобільного банкінгу, а також предоставила голосовий доступ. Це програма, в якій клієнти можуть активувати цю опцію, використовуючи опцію швидкого входу в додаток, і в налаштуваннях вони можуть вибрати розпізнавання обличчя і голоса. Щоб включити функцію розпізнавання голосу, клієнт повинен записати наступну заяву: «Моя особистість захищена, тому що мій голос - це мій пароль. Підтвердіть мене ». Ця заява має бути зроблена в цілому три рази. Потім при реєстрації необхідно чітко і голосно вимовити цю фразу. Розпізнавання облич виконується шляхом фотографування перед реєстрацією. При вході в систему фіксуються підморгування людини, про яку йде мова. Цей аспект допомагає боротися з шахрайством, фотозображення або відео не зможе моргнути в потрібний момент.

USAA також пропонує традиційне розпізнавання відбитків пальців в якості опції для входу в додаток мобільного банкінгу. Таким чином, у клієнтів є кілька варіантів входу в додаток, використовуючи один з кращих біометричних методів: особа, голос, відбиток пальця або введення PIN-коду. На додаток до параметрів безпеки біометричного входу в систему банк також використовує фонову

ідентифікацію пристрою, при якій код, відправлений з пристрою в USAA, зашифрований, а потім порівнюється з зареєстрованим ідентифікатором пристрою.

Одна з найбільш перспективних можливостей нових елементів доступу заснована на авторизації ризиків, т. н. динамічній системі, яка забезпечує доступ в залежності від довіри користувача, що запитує доступ, і конфіденційності інформації, яка захищається. Цей параметр використовує аутентифікацію користувача на основі різних оцінок поведінки користувача з використанням датчиків, таких як камера, акселерометр або GPS. Смартфони можуть збирати широкий спектр інформації про користувачів, включаючи типові вирази обличя, їх звичайну геолокацію, а також те, як він пише, ходить або говорить. Разом ці чинники в 10 разів безпечніше, ніж відбитки пальців і в 100 разів безпечніше, ніж чотиризначні PIN-коди. При такому рівні безпеки телефону користувача вже можна припустити, що людина перед дисплеєм дійсно є тим, хто себе називає.

Використані джерела:

1. Компания TeleSign URL: https://www.linkedin.com/company/telesign
2. Допомога членам USAA URL: https://www.usaa.com/?akredirect=true

Марценюк Л.В.
професор кафедри економіки та менеджменту
Дніпровського національного університету
залізничного транспорту, д.е.н., доцент

ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ОНЛАЙН-КУРСІВ ДЛЯ РОЗРОБНИКІВ КОНТЕНТУ

Авторське право – це сукупність правових норм, що регулюють суспільні відносини, які виникають у зв’язку із створенням та використанням творів науки, літератури, мистецтва. Згідно зі ст. 8. Закону України «Про авторське право і суміжні права» «Об’єктами авторського права є твори у галузі науки, літератури і мистецтва, а саме: …виступи, лекції, промови, проповіді та інші усні твори…». Охороні за цим Законом підлягають всі твори, зазначені у частині першій цієї статті, як оприлюднені, так і не оприлюднені, як завершені, так і не завершені, незалежно від їх призначення, жанру, обсягу, мети (освіта, інформація, реклама, пропаганда, розваги тощо) [1].

В контексті бурхливого розвитку дистанційної освіти актуальним стає питання щодо прав на онлайн-курси, які викладач завантажує на тій чи іншій платформі дистанційного навчання, які в подальшому використовуються для навчання студентів. Ці курси можуть належати як автору курсу, так і його замовнику.

Якщо людина сама створює, користується і продає онлайн-курс, то вона є і автором, і правовласником. Якщо особа робить це під замовлення, то в договорі прописано кому і які права належать щодо подальшого використання. Права на використання курсу можуть повністю переходити до замовника або розподілятися таким чином, що використовувати курс в майбутньому зможе і його автор, і його правовласник за договором.

Якщо в посадові обов'язки викладача згідно з трудовим договором входить створення таких курсів, то розроблений в рамках виконання трудових обов'язків курс матиме статус «службового твору» та належатиме роботодавцю. При цьому арава по використанню створених в рамках трудового договору авторських творів можуть належати і працівникові, але це повинно бути спеціально обумовлено відповідною угодою [2].

Автор не зобов’язаний отримувати відповідні документи на об’єкти інтелектуальної власності, але за бажанням, він може це зробити.

Задля захисту своїх матеріалів від несанкціонованого використання, автор може використовувати режим функціонального обмеження використання файлів, надаючи доступ лише до фрагментів загального документу, або встановлювати дату, після якої файли будуть недоступні, або встановлювати захист від копіювання, використовувати криптографічні конверти та вживати інші заходи щодо захисту своїх праць [3].

Вид і розмір відповідальності за порушення авторських прав визначається судом. Зокрема, суд має право постановити рішення чи ухвалу про: відшкодування моральної (немайнової) шкоди; відшкодування збитків, завданих порушенням авторського права; стягнення з порушника доходу, отриманого внаслідок порушення; виплату компенсації, що визначається судом, у розмірі від 10 до 50000 мінімальних заробітних плат, замість відшкодування збитків або стягнення доходу тощо [4].

Цікавий той факт, що викладачі – розробники онлайн-курсів отримують непоганий постійний пасивний дохід, розмістивши свої курси на відповідних освітніх платформах. Наприклад, середній інструктор на курсах Udemy отримує 7000 $ в місяць. Є «елітні викладачі» з величезною аудиторією, які отримують дохід від курсів в шестизначних цифрах [5].

Достатньо успішною є компанія Coursera, яку заснували майже десять років тому професори Стенфордського університету Дафне Коллер і Ендрю Енгом. Coursera є найбільшим в світі провайдером онлайнових освітніх курсів, де зареєстровані 36 мільйонів користувачів, завантажено 3000 курсів, при чому з власниками освітньої платформи співпрацюють майже 200 провідних університетів з різних країн. Виручка компанії за рік (за оцінками Forbes) складає близько 140 мільйонів доларів. Компанія проводить вдалу маркетингову компанію, спочатку надаючи доступ користувачам до безкоштовного контенту, поступово пропонуючи платні послуги, включаючи різного роду Сертифікати.

Коли Ендрю Енг анонсував черговий курс, за перші чотири тижні на нього записалися понад 100 000 потенційних студентів. Зазвичай, один курс проходять близько 25 000 студентів [6].

На наш погляд, майбутнє саме за такими платформами, де кожен учасник (інвестор, університет, окремий викладач-розробник курсу, студент, підприємство, що направило працівника на навчання тощо) отримає те, на що він сподівається в результаті цієї співпраці та права кожного при цьому будуть захищені у відповідній площині Закону.

Використані джерела:

1. Закон України «Про авторське право і суміжні права». Електронний ресурс. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/ed_1999_07_16/T379200.html
2. Кому за законом належать права на онлайн-курси? Електронний ресурс. URL: https://te-st.ru/2016/10/25/online-courses-copyright/
3. Я.О. Юзькова. Захист авторських прав в мережі інтернет. Електронний ресурс. URL: https://www.businesslaw.org.ua/copyright-protection-on-the-internet/
4. Л. Татаріна. Юридичні питання у створенні онлайн-курсів – авторське право і його захист. Електронний ресурс. URL: https://www.eduget.com/news/yuridichni_pitannya_u_stvorenni_onlajn-kursiv_-_avtorske_pravo_i_jogo_zaxist-2419
5. Онлайн-курсы как вид заработка: Как запустить авторский курс? Електронний ресурс. URL: https://the-steppe.com/razvitie/onlayn-kursy-kak-vid-zarabotka-kak-zapustit-avtorskiy-kurs
6. Гендиректор Coursera: мир движется к онлайн-дипломам. Електронний ресурс. URL: https://www.vedomosti.ru/management/characters/2018/11/07/785819-gendirektor-onlain-kursov

Прокопович-Ткаченко Д.І. – в.о. завідувача кафедри кібербезпеки, кандидат технічних наук (Університет митної справи та фінансів, м. Дніпро);

Кузнецов О.О. – професор кафедри інформаційних систем, доктор технічних наук, професор (Національний Державний Університет ім. Каразіна, м. Харків).

СТЕГАНОГРАФІЧНІ МЕТОДИ ПРИХОВУВАННЯ ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ 3D ДРУКУ

Стеганографія, у широкому сенсі, це такий спосіб передачі закодованого інформаційного повідомлення, при якому приховується сам факт його існування [1, 2]. На відміну від криптографії, методи стеганографії дають можливість замінити несуттєві частки даних на конфіденційну інформацію так, щоб неможливо було

запідозрити існування вбудованого таємного послання [1].

На сьогодні у зв'язку з розвитком обчислювальної техніки і нових каналів передачі інформації з’являються нові стеганографічні методи, в основі яких лежить приховування інформації в комп'ютерних файлах – контейнерах, які володіють високим рівнем природньої надмірності (фото- та відеозображення, аудіо-файли, текстові документи, тощо). Сутність приховування полягає в скритній заміні надмірних даних інформаційними повідомленнями, вилучити або навіть встановити факт наявності яких може тільки уповноважена особа, що має секретний стеганографічний ключ [1, 2].

Останніми роками з’явився та отримав розвиток новий напрям комп’ютерної стеганографії, який пов'язаний із приховуванням інформаційних повідомлень в штучно створених контейнерах, надмірність в який породжена технічними особливостями зберігання, обробки та/або передачі даних [3 – 14]. Такі методи «технічної» стеганографії набули поширення при приховуванні інформаційних повідомлень в різних за своєю природою штучних контейнерах. Зокрема, методи мережевої стеганографії у якості носія (контейнеру) використовують переданий по мережі пакет або сукупність пакетів даних, процедури приховування та вилучення інформаційних даних засновані на використанні особливостей функціонування мере- жевого стеку протоколів передачі даних [3 – 6]. Побудову прихованих кластерних каналів засновано на використанні особливостей зберігання даних у сучасних файлових системах [7 – 9]. Існують і інші напрямки розвитку технічної стеганографії, зокрема, які засновані на використанні штучної надмірності тривимірних (3D) моделей об’єктів [10 – 14]. Останніми роками тривимірні моделі набули значного поширення та розповсюдження в різних застосуваннях, зокрема при обробці медичних даних, музейних експонатів та зразків культурної спадщини, імітаційних моделей промислових зразків та виробничих процесів, комп’ютерних ігор, тощо. При цьому стеганографічні методи застосовують для захисту авторського права тривимірних моделей, скритого приховування певної інформації, захисту від випадкових викривлень або певних похибок, тощо. Отже дослідження нових методів приховування да- них із використанням 3D-технологій є перспективним напрямком сучасних досліджень.

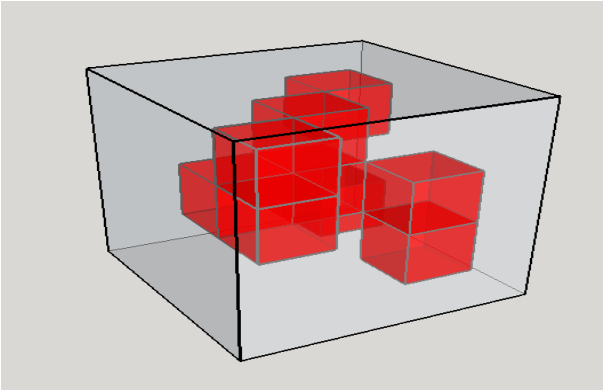
В цій роботі розвивається новий підхід, запропонований в [15 – 17], щодо стеганографі- чного приховування даних в твердотільних об'єктах за допомогою технології 3D-друку. Сут- ність цього підходу полягає в перетворенні інформаційного повідомлення на 3D-модель, яку розміщують всередині 3D-моделі контейнеру із подальшим роздрукуванням (створенням, вирощуванням). Зовнішній вигляд отриманого твердотільного об'єкту, його експлуатаційні та естетичні властивості не змінюються в процесі вбудовування інформаційного повідомлен- ня. Крім того, видалити або спотворити приховане повідомлення без руйнування або значно- го пошкодження виробу неможливо, отже маємо нову технологію стеганографічного захисту інформації як для скритної її передачі, так і для забезпечення авторського права, тощо.

1.*Приховування інформаційних даних*

В роботах [15 – 17] було запропоновано прототип комплексу

стеганографічного захисту, в якому інформаційні дані приховуються в процесі пошарового створення (вирощування) твердотільного об'єкта при використанні різних технологій 3D-друку. Основна ідея полягає у вбудовуванні (стеганографічному кодуванні) інформаційних даних в цифрову 3D-модель, за якої в подальшому пошарово створюється (роздруковується) твердий об'єкт (готовий виріб або прототип для подальшого доведення). Процес вбудовування реалізується з використан- ням секретних ключових даних, що виключає несанкціонований доступ до інформації, що захищається, порушення її цілісності, автентичності та конфіденційності. Крім того, застосо- вані методи стеганографічного захисту не повинні знижувати експлуатаційних, естетичних та будь-яких інших властивостей готового виробу, оскільки технології, що застосовуються для нанесення шарів, не модифікуються. Отже, пропонований комплекс інваріантний спосо- бу пошарового вирощування, тобто може комплектуватися довільними периферійними при-строями 3D-друку різних фірм виробників з будь-якими матеріалами і принципами пошаро- вого створення [15 – 17].

Головна ідея приховування даних полягає в розміщенні інформаційного повідомлення у середині довільної комп'ютерної моделі фізичного об'єкту, яку можна роздрукувати на 3D принтері – іграшці, статуетці, сувенірі тощо. Інформаційне повідомлення подається у двійко- вому вигляді і кожен біт перетворюється на певний фрагмент фізичної моделі. Як приклад (рис. 1), кожен біт може кодуватися тривимірним кубом встановленого розміру, причому наповненість куба відповідає вмісту відповідного біту: «0» відповідає пустому (не заповне- ному) кубу, «1» – заповненому. Інформативний признак може бути і іншим, наприклад запо- внення різними матеріалами, або одним матеріалом але із різною щільністю, орієнтованістю, формою елементарних «бітових» фізичних



моделей, тощо.

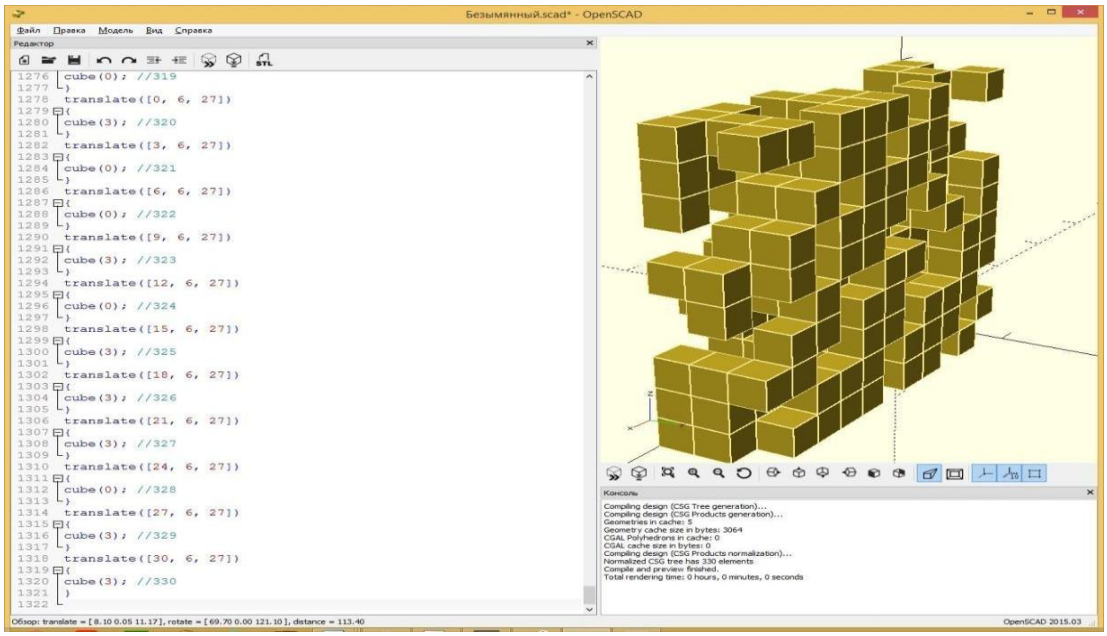
Рис. 1. Схематичне подання стеганографічного кодування – перетворення інформаційного повідомлення на фрагмент комп'ютерної моделі фізичного об'єкту

Для автоматизованого кодування було застосовано спеціалізоване програмне забезпе- чення OpenSCAD, яке призначене для створення твердотільних тривимірних САПР-об'єктів. Воно є вільним і доступним під операційними системами Linux / UNIX, Microsoft Windows і Apple Mac OS X.

На рис. 2 продемонстровано кодування інформаційного повідомлення «Tomorrow never comes until it's too late». Кожен символ повідомлення подається у бінарному вигляді за допо- могою коду ASCII. Далі, для обраної кубічної форми

«бітових» моделей та розміру 3x3x3 міліметри виконується кодування кожного інформаційного біту. Для цього було розроблено програмне забезпечення, яке формує відповідний вихідний код, що розміщується у робочому полі програми OpenSCAD. На рис. 2 всі елементарні фізичні моделі згруповано у контейнер розміром 11x3x10 відповідних кубів (ці налаштування додатково встановлюються у розроб- леному програмному забезпеченні).

Рис. 2. Приклад стеганографічного кодування за допомогою програми OpenSCAD



На рис. 2 зліва можна побачити вихідний код, в якому задаються координати та розмір тривимірних кубів – носіїв інформаційних бітів. Праворуч наведено створену тривимірну модель інформаційного повідомлення, яка відповідає всім заданим вхідним параметрам.

Таким чином, в результаті стеганографічного кодування інформаційне повідомлення спочатку перетворюється у трьохвимірну булеву матрицю, яка, в свою чергу, перетворюєть- ся в комп'ютерну модель фізичного об'єкту. Сформована комп'ютерна модель булевої мат- риці розміщується у середині основної моделі контейнеру так, щоб її краї не виходили за межі зовнішнього тіла, як це схематично наведено на рис. 3. При цьому застосовувалося спе- ціалізоване програмне забезпечення MakerBot Desktop з технологій 3D-друку.

Розмістити таку матрицю в середині іншої моделі можна різними способами, наприклад:

- всі заповнені куби під час друку на 3D принтері заповнювати іншим кольором;
- всі заповнені куби під час друку на 3D принтері залишати порожніми.

Недоліком другого способу є зменшення кінцевої ваги тіла, що при детальному аналізі може видати факт наявності таємного повідомлення. Заповнення бітів іншим кольором (або, наприклад, іншим матеріалом) зменшує ймовірність виявлення прихованого повідомлення, але збільшує складність його

зчитування.

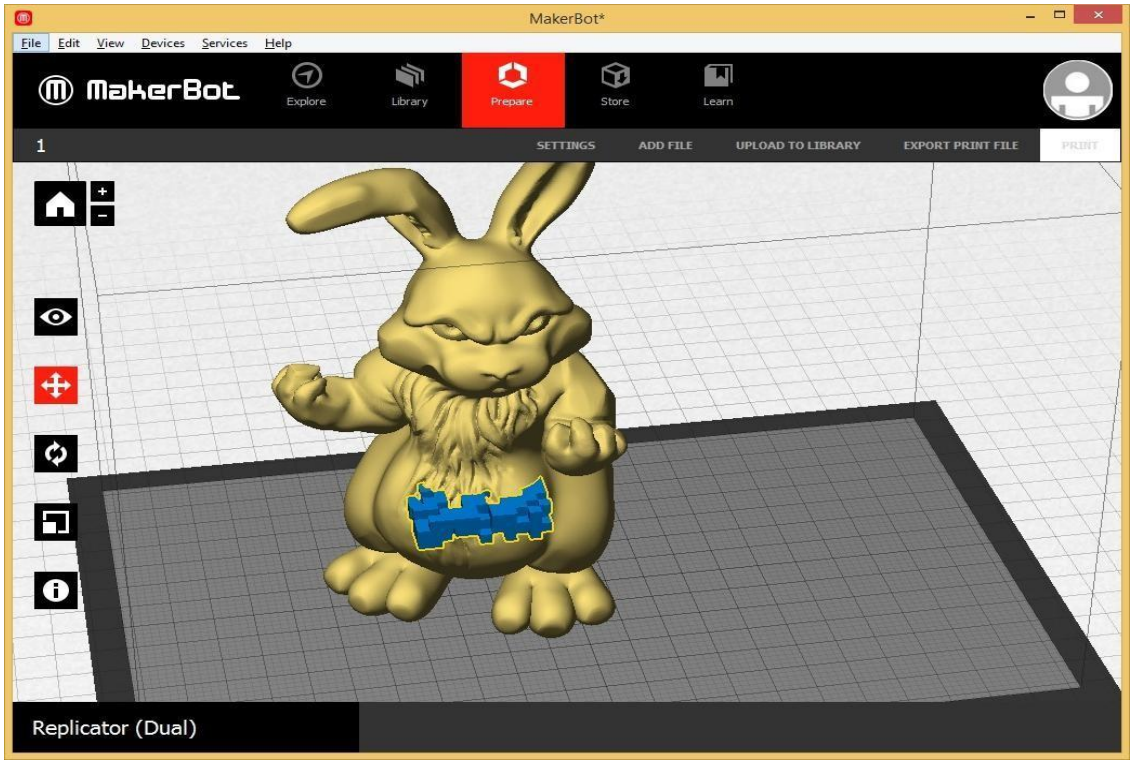


Рис. 3. Розміщення тривимірної моделі інформаційного повідомлення у середині основної моделі контейнеру

На рис. 4 показаний процес пошарового створення твердотільного об'єкту-контейнеру із вбудованим інформаційним повідомленням. Ліворуч на рисунку показана схематична візу- алізація процесу друку, праворуч – фотографія реального процесу на 68 шарі 3D-друку, який було виконано із застосуванням 3D принтеру «Flashforge Creator Dual». На рис. 5 показано завершення друку 3D-моделі та готовий виріб із вбудованим повідомленням.

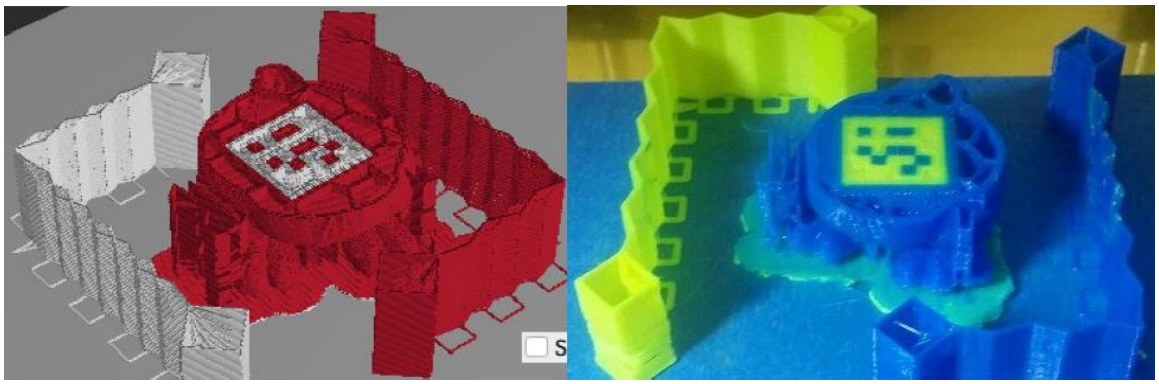


Рис. 4. Пошарове створення твердотільного об'єкту-контейнеру із вбудованим інформаційним повідомленням

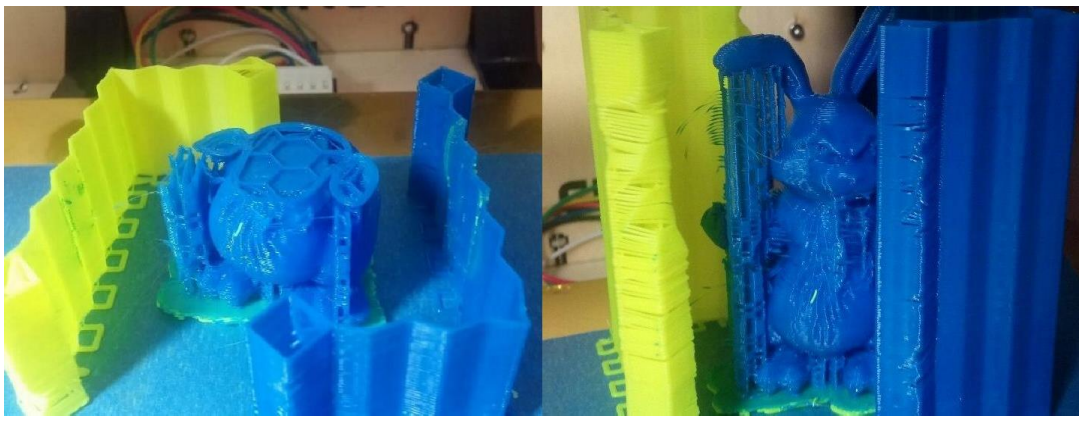


Рис. 5. Завершення друку та готовий виріб із вбудованим повідомленням

2.*Вилучення інформаційних даних*

Процес вилучення вбудованих даних здійснюється за допомогою сканування отримано- го твердотільного об’єкту. Витягнуті сканером дані піддаються стеганографічному декоду- ванню з використанням секретних ключових даних. На цьому етапі забезпечуються різні послуги безпеки, наприклад, цілісність, автентичність, причетність, конфіденційність, тощо. Для підвищення достовірності (завадостійкості) вбудовані дані додатково піддаються надмі- рному кодуванню, яке дозволяє з заданою вірогідністю виявляти і/або виправляти помилки, що виниклі в процесі пошарового друку/сканування. Пропонований комплекс може використ- товувати в різних областях: для прихованої передачі інформаційних повідомлень із забезпеченням різних послуг безпеки (цілісності, автентичності, причетності, конфіденційності та ін.). Видалення, спотворення або модифікація вбудованих даних неможливі без фізичного руйнування готового виробу, тобто пропонований комплекс ідеально підходить для забезпе- чення достовірності пошарово вирощених виробів, захисту їх від несанкціонованого копію- вання та недобросовісних підробок, забезпечення авторського права, тощо [1, 2].

Слід відмітити, що на сьогодні день ще не розроблено надійних засобів вилучення інфо- рмаційних даних [15 – 17]. Саме невизначеність конкретної процедури вилучення вбудова- них даних за допомогою сканування отриманого твердого тіла є головним невирішеним пи- танням з приводу практичного застосування запропонованого комплексу 3D-стеганографії. Зокрема, система може комплектуватися різними периферійними пристроями 3D-друку, які застосовують різні технології пошарового вирощування та різний за своїми фізичними влас- тивостями вихідній матеріал. Відповідні процедури сканування отриманого твердого тіла повинні враховувати ці особливості і, по можливісті, забезпечувати надійне та безпомилкове вилучення прихованих даних.

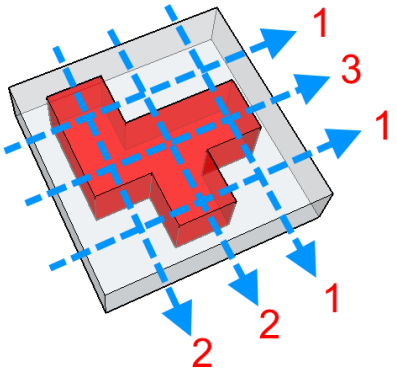
Одним із можливих напрямків у вирішенні зазначених проблем є застосування лазерних сканерів, в яких потік когерентного, монохроматичного, поляризованого і вузьконаправленого потоку випромінювання, що утворює паралельний пучок, зменшується в результаті поглинання в середовищі в деяку заздалегідь обумовлену кількість разів. Для встановлення принципової можливості зчитування прихованого повідомлення з 3D-моделі, що пошарово створена (надрукована) на 3D-принтері без пошкодження самої моделі або повідомлення,

було проведено наступні експериментальні дослідження.

2.1. *Опис лабораторної установки та умов проведення експериментальних досліджень*

Головна ідея проведення експерименту полягає в вузьконаправленому опромінюванні готового виробу (із вбудованим повідомленням) за різними кутами та напрямками, достатніми для однозначного визначення внутрішньої структури виробу. При цьому як вихідні дані враховуються значення інтенсивності випромінювання, що зменшуються в результаті поглинання.

При кодуванні інформаційних бітів пустими та заповненими кубами схема опромінення готового виробу може бути подана у спрощеному вигляді як на рис. 6 (ліворуч). В кінці стрілок вказане умовне значення результату вимірювання зменшення інтенсивності випроміню- вання (пропорційно до товщини заповненого матеріалом об’єкту). Праворуч на цьому ж рисунку подано значення інформаційних бітів, які, як очікується, буде вилучено із твердотільного об’єкту.



1	0	0
1	1	1
0	1	0

Рис. 6. Спрощена схема опромінення готового виробу (ліворуч) та очікуваний результат вилучення даних (праворуч)

Оскільки ніяких інших відомостей щодо внутрішньої структури виробу немає, розміщення заповнених фрагментів (і відповідних бітів) повинне враховувати однозначність вилучення тільки за результатами вимірювання (зображені на рисунку ліворуч результати вимірювання мають два можливі рішення, одне з яких не співпадає із наведеним праворуч). Таке розміщення, фактично, є номограмою, яку застосовують при формуванні японських кросвордів.

Для спрощення умов проведення експерименту було виготовлено просту фізичну модель у формі сходинок із ABS-пластика жовтого та синього кольорів. Така форма дозволяє швидко змінювати товщину заповненого матеріалом об’єкту (рис. 7). Фактично, маємо шість різних значень, які умовно відповідають наступним інформаційним бітовим послідовностям:

- без заповнення – бітова послідовність (00000);
- одне заповнення (перша сходинка) – бітова послідовність (10000);
- два заповнення (друга сходинка) – бітова послідовність (11000);
- три заповнення (третя сходинка) – бітова послідовність (11100);
- чотири заповнення (четверта сходинка) – бітова послідовність (11110);
- п’ять заповнень (п’ята сходинка) – бітова послідовність (11111).

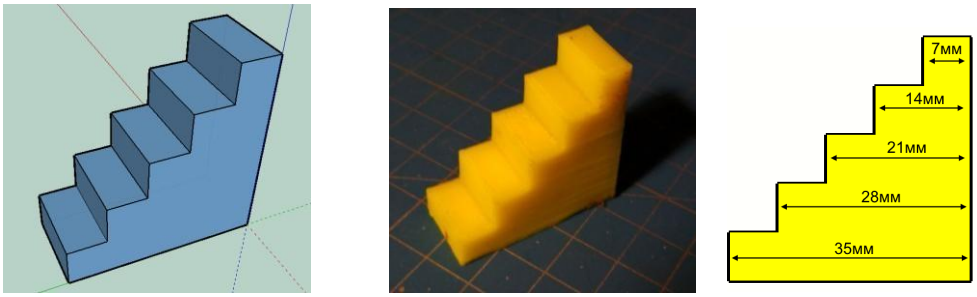


Рис. 7. Спрощена фізична модель інформаційних даних

Для проведення досліджень було застосовано оптичні прилади з лабораторії кафедри фізичної оптики фізичного факультету. Відомо, що кожен матеріал має свій показник поглинання – величина, зворотня відстані, на якому потік монохроматичного випромінюван- ня, що утворює паралельний пучок, зменшується в результаті поглинання в середовищі в деяку заздалегідь обумовлену кількість разів. Показник поглинання визначається властивостями речовини і в загальному випадку залежить від довжини хвилі λ світла, що поглинаєть ся. Ця залежність є спектром поглинання речовини.

В якості монохроматичного випромінювання використовувалися наявні у лабораторії лазери видимого спектру, що відрізнялися довжиною хвилі та потужністю випромінювання. Пучок лазерного світла проходив через досліджуване тіло. Випромінювання, що не поглиналося пластиком, потрапляло на закріплений з іншої сторони фоторезистор – фотоелектричний напівпровідниковий приймач випромінювання, принцип дії якого ґрунтується на ефекті фотопровідності (явищі зменшення опору напівпровідника у разі збудження носіїв заряду світлом). Для зчитування і подальшої обробки даних був використаний мікроконтролер «Arduino UNO». На фоторезистор подавалася напруга 5 В. В залежності від степені збудження фотоелементу змінювався його опір. Мікроконтролер робив заміри зміни напруги кожні 40 мс, оцифровував їх та відправляв на персональний комп’ютер.

Схематично лабораторну установку зображено на рис. 8. Вона включає досліджуване тіло із пластику у вигляді сходинок (рис. 7), лазер як джерело вузьконаправленого опромі- нювання готового виробу, фоторезистор та мікроконтролер, для зчитування розсіяного випромінювання. На рис. 9 наведено фотографію зібраної лабораторної установки та збільшену фотографію процесу оптичного опромінювання.

Для прийому та відображення поточного значення фоторезистора, а також розрахунку середнього арифметичного із виконаних замірів застосовувалося розроблене програмне забезпечення. Оскільки спектр поглинання речовини був невідомий для виготовленого зразка, у досліді використовувалися всі наявні в лабораторії лазери із різними характеристиками (див. табл. 1).

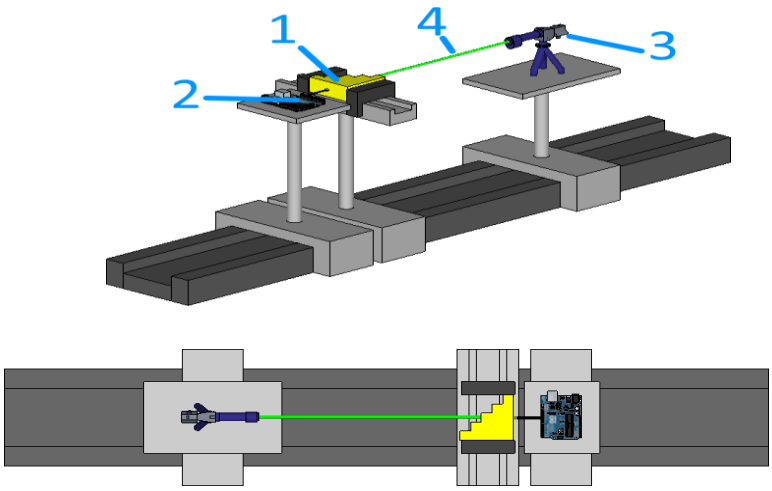


Рис. 8. Схема лабораторної установка: 1 – досліджуване тіло із пластику у вигляді сходинок; 2 – фоторезистор та мікроконтролер, що зчитує дані; 3 – лазер; 4 – лазерне випромінювання

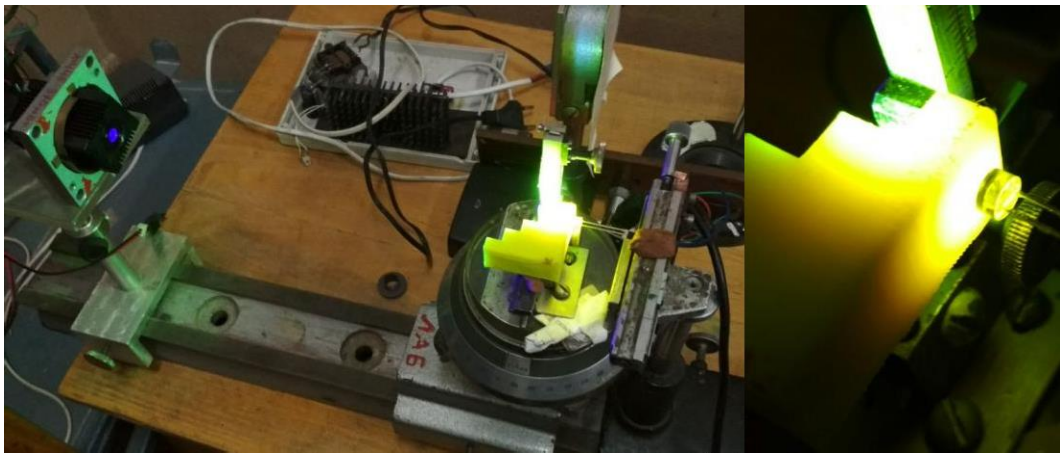


Рис. 9. Фотографія зібраної лабораторної установки (ліворуч) та збільшена фотографія процесу опромінювання (праворуч)

Таблиця 1

Характеристики лазерів, які застосовувалися в експерименті

Номер	Довжина хвилі, нм	Потужність, мВт	Видимий колір
1	532	100	Зелений
2	650	25	Червоний
3	405	90	Фіолетовий
4	445	160	Синій
5	650	25	Червоний

Кожним лазером просвічувалися різні товщини досліджуваного тіла та робились заміри відсотку світла, що пройшов крізь дану ділянку тіла. Експеримент проводився за відсутності будь-яких інших ввімкнених джерел світла, тобто у темряві. Крок зміни товщини досліджуваного тіла 7 мм був обраний враховуючи товщину лазерного пучка, товщина якого знаходиться у межах 5-6 мм. Для

коректності досліду, пучок лазерного випромінювання повинен повністю потрапляти на ділянку із однією товщиною. Мікроконтролер має вольтметр, що виявляє зміну напруги з кроком 5/1024 вольта, тому під час оцифровки аналогового значення отримуємо число від 0 (світло не потрапляє взагалі) до 1024 (максимальна кількість світла, яку може розпізнати фоторезистор).

2.2.*Результати експерименту та їх інтерпретація*

Отримані результати експериментальних досліджень (усереднені за виконаними вимірюваннями) зведено у табл. 2.

Таблиця 2

Результати вимірювань

Зразок жовтого кольору						
Номер лазера	Товщина ділянки, мм					
	0	7	14	21	28	35
1	1024	1001	775	162	33	4
2	1024	995	426	65	6	0
3	1024	995	97	5	1	0
4	1024	998	500	59	5	0
5	1024	995	336	57	4	0
Зразок синього кольору						
Номер лазера	Товщина ділянки, мм					
	0	7	14	21	28	35
1	1024	0	0	0	0	0
2	1024	0	0	0	0	0
3	1024	0	0	0	0	0
4	1024	0	0	0	0	0
5	1024	0	0	0	0	0

За наведеними у таблиці даними можна зробити висновок, що зразок із жовтого пластику найменше поглинає зелене лазерне випромінювання із довжиною хвилі λ=532 нм. Хоч обидва зразки виготовлені з однакового виду пластику, із-за різниці кольору вони мають зовсім різні показники поглинання. Тіло, що виготовлено з синього пластику, має значно більший показник поглинання. Навіть на мінімальній товщині тіло з синього пластику поглинуло світло з кожного лазера, якого б вистачило для визначення найменшої товщини.

Отримані результати для зразка матеріалу жовтого кольору свідчать, що для різної товщини матеріалу маємо різні значення інтенсивності випромінюванні і ці різниці досить суттєві. Отже, за результатами вимірювань принципово можливо встановити товщину матеріалу, та, відповідно, визначити вміст прихованих інформаційних бітів.

Висновки

В роботі досліджено новий напрямок технічної стеганографії, який пов'язаний із прихо- ванням інформаційних даних в процесі пошарового

створення (вирощування) твердотіль- ного об'єкта при використанні різних технологій 3D-друку. Інформаційні дані перетворю- ються в цифрову 3D-модель елементарних фізичних об’єктів, які розміщуються всередині 3D-моделі виробу-контейнеру. Після роздрукування твердий об'єкт фізично містить прихо- вану інформацію, яку неможливо видалити або спотворити без пошкодження контейнеру. Крім того, застосовані методи не знижують експлуатаційних, естетичних та будь-яких інших властивостей готового виробу, оскільки технології, що застосовуються для нанесення шарів, не модифікуються, приховування є інваріантним способу пошарового вирощування, тобто можуть застосовуватися різні пристрої 3D-друку з будь-якими матеріалами і принципами пошарового створення.

Процес вилучення вбудованих даних здійснюється за допомогою сканування отримано- го твердотільного об’єкту. Саме невизначеність конкретної процедури сканування отримано- го твердого тіла є головним невирішеним питанням з приводу практичного застосування за- пропонованого комплексу 3D-стеганографії.

За результатами експериментальних досліджень встановлено принципову можливість зчитування прихованого повідомлення з 3D-моделі із застосуванням лазерних сканерів, в яких потік когерентного, монохроматичного, поляризованого і вузьконаправленого потоку випромінювання, що утворює паралельний пучок, зменшується в результаті поглинання в середовищі в деяку заздалегідь обумовлену кількість разів. Отримані результати для зразка матеріалу жовтого кольору свідчать, що для різної товщини маємо різні значення інтенсив- ності випромінюванні і ці різниці досить суттєві. Отже, за результатами вимірювань принци- пово можливо встановити товщину матеріалу, та, відповідно, визначити вміст прихованих інформаційних бітів.

Наведені результати експериментальних досліджень не є остаточними та потребують подальшого уточнення та відтворення. Зокрема, невирішеними є питання обрання типу і характеристик лазеру, погодженість цих характеристик із властивостями матеріалів твердотільного об’єкту, налаштування фоторезисторів, тощо. Крім того, перспективним, на нашу думку, є проведення експериментальних досліджень із іншими видами випромінюван- ня, видами та кольорами пластику.

Використані джерела:

1. Katzenbeisser S., Petitcolas F. A. Information Hiding Techniques for Steganography and Digital Watermarking. – Norwood, MA, USA: Artech House, 2000. – 220 p.
2. Petitcolas F. A. P., Anderson R. J. and Kuhn M. G. Information hiding-a survey // Proceedings of the IEEE. – vol. 87, no. 7. – pp. 1062-1078. – Jul 1999.
3. Mazurczyk W., Smolarczyk M., Szczypiorski K. Retransmission steganography and its detection // Soft Computing, vol. 15, no. 3, pp. 505-515, 2011.
4. Nair A. S., Kumar A., Sur A. and Nandi S. Length based network steganography using UDP protocol // IEEE 3rd International Conference on Communication Software and Networks, Xi'an, 2011, pp. 726-730.
5. Ahsan K. and Kundur D. Practical data hiding in TCP Lip // ACM

Workshop on Multimedia and Security, 2002, [On-line]. Internet: http://ee.tamu.edu/deepalpdf/ acm02.pdf.

6. S. H. Sellke, C. Wang, S. Bagchi and N. B. Shroff, "TCP/IP Timing Channels: Theory to Implementation", pp. 2204-2212, 2009.

7.Khan H., Javed M., Khayam S.A., Mirza F. Designing a cluster-based covert channel to evade disk investigation and forensics // Computers & Security. – Volume 30, Issue 1. – January 2011. [On-line]. Internet: https://www.sciencedirect.com/science/article/pii/ S016740481000088X

8. Khan H., Javed M., Khayam S.A., Mirza F. Evading Disk Investigation and Forensics using a Cluster-Based Covert Channel / National University of Science & Technology (NUST). – Islamabad 44000, Pakistan. [On-line]. Inter- net: https://www.sigsac.org/ccs/CCS2009/pd/abstract_17.pdf

9. Morkevičius N., Petraitis G., Venčkauskas A., Čeponis J. Covert Channel for Cluster-based File Systems Using Multiple Cover Files // Information Technology and Control, 2013, Vol.42, No.3. pp. 32. [On-line]. Internet: http://itc.ktu.lt/index.php/ITC/article/ view/3328

10. Rani R. and Deep G. Digital 3D barcode image as a container for data hiding using steganography // 4th Inter- national Conference on Signal Processing, Computing and Control (ISPCC), Solan, 2017. – P. 325-330.

11. Sun Z. , Z. m. Lu and Z. Li. Reversible Data Hiding for 3D Meshes in the PVQ-Compressed Domain // International Conference on Intelligent Information Hiding and Multimedia, Pasadena, CA, USA, 2006, pp. 593-596.

12. Wang K., Lavoué G., Denis F., Baskurt A. and He X. A Benchmark for 3D Mesh Watermarking // Shape Modeling International Conference, Aix-en-Provence, 2010. – P. 231-235.

13. Motwani M. C., Bryant B. D., Dascalu S. M. and F. C. Harris Jr. 3D Multimedia Protection Using Artificial Neural Network // 7th IEEE Consumer Communications and Networking Conference, Las Vegas, NV, 2010. – P. 1-5.

14. Vasić B. Annotation of cultural heritage 3-D models by robust data embedding in the object mesh // 22nd Telecommunications Forum Telfor (TELFOR), Belgrade, 2014. – P. 842-849.

15. Кузнецов А.А., Коваленко О.Ю. Стеганографическая защита информации с использованием 3D-печати // Інформаційна безпека держави, суспільства та особистості : зб. тез доповідей Всеукр. наук.-практ. конф., 16 квітня 2015 р. – Кіровоград : КНТУ, 2015. – С. 91-92.

16. Кузнецов О.О. Лекція 12: Технічна стеганографія. Приховування даних в твердотільних об'єктах за допомогою 3D-друку : Електронний конспект лекцій за дисципліною «Стеганографія». – Харків : Харк. нац. ун-т ім. Каразіна, 2016. – 14 с.

17.Коваленко О.Ю. Розробка лабораторного комплексу технічної стеганографії з використанням тривимірного друку : Пояснювальна записка до дипломної роботи бакалавра (Керівник О.О. Кузнецов). – Харків : Харк. нац. ун-т ім. Каразіна, 2015. – 47 с.

Форос Г.В., доцент кафедри кібербезпеки та інформаційного забезпечення ОДУВС, к.ю.н., доцент

СТРАТЕГІЯ КІБЕРБЕЗПЕКИ ЯК ОСНОВА ІНФОРМАЦІЙНОГО ПРАВОПОРЯДКУ В УКРАЇНІ

Відкритий та вільний кіберпростір розширює свободу і можливості людей, збагачує суспільство, створює новий глобальний інтерактивний ринок ідей, досліджень та інновацій, стимулює відповідальну та ефективну роботу влади і активне залучення громадян до управління державою та вирішення питань місцевого значення, забезпечує публічність та прозорість влади. За сучасних умов в Україні, як і в інших країнах світу, при створенні нових інформаційних технологій, у результаті інтелектуальної діяльності виникають насичені найрізноманітнішими відомостями інформаційні об'єкти, що характеризуються національним значенням. Це можуть бути методики робіт, перспективні технічні рішення, результати маркетингових досліджень тощо. На цей час інформація стала першоосновою життя сучасного суспільства, предметом та продуктом його діяльності, а процес створення, накопичення, збереження, передачі та обробки інформації, у свою чергу, стимулює прогрес в інформаційній сфері.

Проблема належного забезпечення інформаційного правопорядку має дуже багато аспектів, серед яких найважливішими є визначення правового положення інформаційної сфери як соціального ресурсу, специфіка регулювання відносин, які виникають в інформаційній сфері, юридичне закріплення права на захист об'єктів інформаційної сфери та створення правових гарантій реалізації цього права. На сучасному етапі розвитку нашої держави існує певна правова база для практичної реалізації громадянами наданого їм Конституцією права як на інформацію, так і на її належний захист. Саме Конституція України проголошує принцип верховенства права та визначає, що людина, її життя і здоров‘я, честь і гідність, недоторканність і безпека визнаються в Україні вищою соціальною цінністю. Згідно норм ст. 17 Конституції захист інформаційної безпеки визначається однією з найважливіших функцій держави, справою всього Українського народу. Вся інформація, яка знаходиться в обігу, та інформаційні процеси, які відбуваються, формалізуються у вигляді нормативно-правових актів і впливають на процес прийняття управлінських рішень.

Аналіз чинного законодавства України з питань забезпечення інформаційного правопорядку показує, що він потребує системності, що може бути досягнута його узгодженістю з Конституцією та іншими законодавчими актами. Так, Закон України «Про інформацію» [1] застосовується не тільки до відносин між громадянами і органами державної влади, але й до відносин громадських організацій, приватних підприємств, тобто, до відносин між недержавними суб'єктами інформаційного права. Така ситуація певною мірою не відповідає Конституції України, оскільки вищезазначені правовідносини регулюються положеннями цивільного або господарського, а не адміністративного (інформаційного) права, і в разі виникнення

спорів між ними рішення приймаються судами у порядку цивільного судочинства.

Важливим напрямом оновлення законодавства з питань забезпечення інформаційного правопорядку є чітке визначення видів інформації з обмеженим доступом та відповідне їх правове регулювання шляхом віднесенім до відповідного законодавчого акту. Так, визначення поняття службової та таємної інформації, ми розглядаємо згідно Закону України «Про доступ до публічної інформації», а поняття конфіденційної згідно Закону України «Про інформацію».

На наш погляд, потребує змін законодавство з питань забезпечення інформаційного правопорядку з метою уникнення неоднозначного тлумачення інформаційно-правових норм, особливо тих, що регулюють провадження у справах про порушення інформаційного правопорядку, а також стосуються визначення об'єкта адміністративних правопорушень у сфері інформаційного правопорядку.

За дослідженнями В.Я. Настюка, з метою належного забезпечення інформаційного правопорядку необхідно у законотворчій діяльності зосередити увагу на:

- на відповідності законів міжнародним нормам захисту інформаційних прав людини, які забезпечували б надійний захист інформації;
- на законах, які не повинні бути перевантажені декларативними положеннями, яким притаманний суто інформаційний характер та які не мають нормативного навантаження, тобто не визначають конкретних прав та обов'язків учасників інформаційних відносин;
- на розроблені механізму відновлення порушених інформаційних прав громадянина, людини, юридичних осіб;
- на розкритті поняття «порушення інформаційного правопорядку» як об'єкту адміністративно-правових відносин тощо. [2, с. 121-122]:

Таким чином, ми можемо стверджувати, що за сучасних умов розвитку саме розвиток інформаційного законодавства може стати основою для успішного удосконалення інформаційної інфраструктури і подальшого поліпшення системи інформаційного правопорядку. Сьогодні немає формальних вимог до забезпечення інформаційного правопорядку, оскільки не існує такого юридичного поняття. Труднощі у захисті інформаційного правопорядку полягають не стільки у технічній площині (як захистити), скільки в організаційно-правовій.

Використані джерела:

1. Закон України «Про інформацію» від 02.10.1992 № 2657-12. URL: http://zakon.rada.gov.ua/laws/show/2657-12

2. Настюк В.Я., Бєлєвцева В.В. Адміністративно-правовий захист інформації: проблеми та шляхи вирішення : монографія. К.: Ред. журн. «Право України»; Х.: Право, 2013. 128 с.

Берназ П.В. - проректор Одеського державного університету внутрішніх справ, к.ю.н.

ПРОРАХУНКИ В ІНФОРМАЦІЙНО-ПРАВОВІЙ ПІДГОТОВЦІ ФАХІВЦІВ

Україна сьогодні в медійному секторі суспільних відносин дедалі все більше актуалізують питання інформаційної культури взагалі, та інформаційно-правової підготовленості фахівців багатьох спеціальностей і спеціалізацій, зокрема.

Підготовка у вищих навчальних закладах України фахівців з юриспруденції, спеціалістів з громадських зв'язків та зв'язків з засобами масової інформації, майбутніх представників журналістського корпусу, а також спеціалістів із захисту інформації передбачають їх значну, не абияку обізнаність у питаннях нормативно-правового регулювання інформаційних відносин. Втім, в реаліях вищої освіти України означена форма правової підготовки переживає, м'яко кажучи, не найкращі часи. І проблема зовсім не в тому, що не вистачає методичного, чи наукового матеріалу, або відповідних науковців-викладачів, які б могли забезпечити організацію такої форми навчання. Не є проблемою наявність і самого обсягу нормативно-правового матеріалу, що утворює фундамент галузевого законодавства і інформаційної галузі права в Україні. Однак, не зважаючи на те що в офіційному кваліфікаційному переліку юридичних спеціальностей вже 15 років передбачено «Інформаційне право» (спеціальність 12.00.07), тим не менш, в абсолютній більшості ВНЗ України, по жодній з вище перелічених спеціальностей така підготовка здійснюється не належному рівні. Тобто, чотирьох-п'яти-річні навчальні програми підготовки бакалаврів і магістрів (юристів, журналістів, фахівців із захисту інформації, соціологів, психологів, управлінців усіх рівнів та спеціалізацій), увесь цей час, не передбачає відповідного рівня опанування знаннями в сфері правового режиму інформаційного обороту. Можливо не представляє навчального інтересу питання правильного забезпечення політики прозорості в управлінській сфері, або опанування навичок роботи з конфіденційною, персональною, чи таємною інформацією без порушення чинного законодавства. Вірогідно, що мабуть перестали бути актуальними сьогодні питання захисту журналістської діяльності і саме тому в українських судах сьогодні майже немає жодного прецеденту захисту порушених прав на отримання, розповсюдження інформації представниками медіа, або перешкоджання їм при виконанні професійної діяльності. Це при тому, що тільки за останні три-чотири роки від утисків з боку влади всіх можливих рівнів в України постраждало більш 200 представників ЗМІ. Не можна не згадати і питання про доступ та захист інформації в автоматизованих інформаційних мережах, не кажучи про кібербезпеку країни взагалі. Знов таки, вірогідно перестали бути актуальними ці питання, бо інакше важко пояснити, чому відповідній підготовці фахівців не приділяється належної уваги.

Проведеними дослідженнями науковців України у цій сфері було виявлено декілька дуже актуальних для України секторів питань, що потребують значних зусиль відповідного напрямку підготовки фахівців-професіоналів. Зокрема, йдеться,

про захист інформаційного суверенітету держави, про розвиток сучасних правових, технічних, організаційних та інших заходів забезпечення захисту інформації. Йдеться і про втілення в реалії багато разів нормативно декларовані концепції інформаційного суспільства в Україні.

Наприклад, в сусідній ворожій Російській Федерації така наукова і навчальна робота здійснювалась активно на протязі останніх 10-ти років, то можемо бачити, що у північного сусіда в інформаційно-правовій сфері створено наукові групи інформаційно-правового спрямування, кафедри інформаційного права та інститути права і інформації. Видаються інформаційно-правові наукові фахові періодичні видання, працюють науково-дослідні лабораторії. Як наслідок – активна інформаційна пропагандистська політика у світовому масштабі, що здатна проводити інформаційну експансію у всьому світі по дискредитації сусідніх держав, втручання в виборчий процес та нав'язуванні світовій спільноті «новітніх стандартів «Руського миру». І хоча в даному випадку йдеться про негативний приклад використання інформаційної зброї, однак, це, водночас і показник того, що ця держава володіє цілою армією відповідно навчених фахівців. А де такий «людський арсенал» в Україні? Так тільки зараз Департамент кіберполіції Національної поліції проходить свій шлях становлення, організовуються управління в областях та набирається особовий склад зі специфічними знаннями, але існує значний дефіцит кадрів.

За останні декілька років система вищих навчальних закладів переживає вже третій чи четвертий етап масового скорочення науково-педагогічних працівників. І якщо реформаторськими ідейними підставами у сфері вищої освіти це обумовлено прагненням позбутися несправжніх, слабких за рівнем підготовки фахівців навчальних установ, то в реаліях це відбивається в позбавленні вишів найбільш кваліфікованого корпусу – професорсько-викладацького складу національних університетів. Також відбувається скорочення обсягу навчальних годин для аудиторної роботи по всіх навчальних напрямках. Саме тому сьогодні були внесенні зміни до Закону України «Про вищу освіту» щодо формування штатного розпису вищих навчальних закладів. Законодавці, хоч і з запізненням та затвердили положення за яким: «При зменшенні чисельності осіб, які навчаються за кожною освітньою програмою, у межах 20 відсотків чисельності, визначеної на початок навчання за цією програмою, штатна чисельність науково-педагогічних працівників не скорочується» [1, п. 5 ст. 32].

Та повертаючись до питання інформаційної культури і інформаційно-правової освіти в Україні, все ж таки, слід акцентувати увагу на тому, що найповажніші в сфері юриспруденції навчальні заклади України не приділяють належної уваги програмам підготовки фахівців за інформаційно-правовим напрямом. Науковцями з професорсько-викладацького складу неодноразово пропонувалися означені програми Вченим і методичним радам вишів Львова, Харкова, Києва, Одеси та інших міст, де розташовані такі заклади. Це відбувалося у період0, що за нашими підрахунками охоплюється часом з 1995 по 2018 роки включно. Тобто існують документи розгляду вченими радами означених питань ще з 1995 року, коли в офіційних кваліфікаційних переліках спеціальності «правознавство» не було такого

напряму, як «Інформаційне право». Такі спроби здійснювались на протязі означеного часу такими науковцями як: А.А. Письменицький [2], А.І. Марущак [3], В.Д. Гапотій, В.С. Цимбалюк, В.Д. Гавловський, В.В. Гриценко [4] та ін. Завдяки таким зусиллям сучасна теорія інформаційного права збагатилася концепціями «інформаційного суверенітету», «особливого суб'єкта інформаційних правовідносин», «розширеного тлумачення права на інформацію», «специфічності об'єкта інформаційних правовідносин», «сучасного інформаційного громадянського суспільства», «інформаційної юридичної відповідальності» [5].

Офіційними рішеннями відповідних рад ці програми затверджувались і передавались до методичних рад і комісій, а потім ректоратами ВНЗ приймалося рішення про можливість впровадження цих напрацювань в навчальний процес. Зрозуміло, що це впровадження має певні перепони, такі як: неможливість введення в навчальний план по причинах гострої нестачі навчального часу; перенавантаженістю планів навчальними дисциплінами та іншими штучними перепони, але все ж такі інформаційно-правова підготовка здійснюється в декількох вишах України. Серед таких ВНЗ можна назвати Одеський державний університет внутрішніх справ, Харківський національний університет внутрішніх справ, Харківський національний університет імені В.Н. Каразіна, Харківський національний педагогічний університет імені Г.С. Сковороди, Київська державна академія служби безпеки України.

Окрім означених адміністративних перепон мали місце ще і ідеологічні. Йдеться про поширеність серед керівництва більшості навчальних закладів України прихильників нормативістського погляду на сучасне право і його систему. За такими тлумаченнями в класичній юридичній освіті не має місця усіляким, на їх думку, псевдонауковим напрямкам на кшталт інформаційного права, медичного права, транспортного права, страхового права і іншим. Підсумовуючи все вище викладене, доцільно визначити, що і на сьогодні ми маємо тверду негативну тенденцію до вихолощеної і невідповідної сучасним реаліям навчально-наукової підготовки кадрів у вишах в напрямку загальної високої інформаційної культури та професійної інформаційно-правової спеціалізованої підготовки.

Використані джерела:

1. Про вищу освіту. Верховна Рада України. Закон України від 01.07.2014 № 1556-VI // Відомості Верховної Ради (ВВР), 2014, № 37-38, ст. 2004.

2. Письменицький А.А., Гапотій В.Д. Загальна теорія інформаційного права: монографія. Мелітополь: ТОВ «Видавничий будинок ММД», 2012. 300 с.

3. Марущак А.І. Інформаційне право: Доступ до інформації: Навчальний посібник. К.: КНТ, 2007. 532 с.

4. Основи інформаційного права України: Навч. посіб. В.С. Цимбалюк, В.Д. Гавловський, В.В. Гриценко та ін.; за ред. М.Я. Швеця, Р.А. Калюжного та П.В. Мельника. К.: Знання, 2004. 274 с.

5. Письменицький А.А. До питання про теорію інформаційно-правової відповідальності. *Часопис з юридичних наук*. Харків: ХНУ імені В.Н. Каразіна, 2014 р. URL: http://periodicals.karazin.ua/jls/article/view/1654/1398

Кулешник Я.Ф., доцент кафедри
інформаційного та аналітичного забезпечення
діяльності правоохоронних органів Львівського
державного університету внутрішніх справ,
к.т.н., доцент

ДЕЯКІ СКЛАДОВІ КОМПОНЕНТИ АРХІТЕКТУРИ УПРАВЛІННЯ ІНФОРМАЦІЄЮ В ДІЯЛЬНОСТІ ПОЛІЦІЇ

Актуальна інформація є ключовою в управлінні, що сприяє можливому підвищенню ефективності і продуктивності поліцейських сил. Щоб усвідомити важливість інформації, поліція повинна прикласти зусилля які дозволять ефективний і безпечний збір, зберігання, обмін та використання інформації.

Для досягнення ефективного управління інформацією поліцейські сили повинні розробити консолідовану архітектуру управління інформацією – прошарок процесів, функцій, політики та рішень, які забезпечують ефективне та безпечне створення, збір, зберігання, зв’язок, оцінку, обмін та використання інформації. Ефективні архітектури управління інформацією інтегрують розрізнені можливості інформації, безпеки, контролю доступу та управління вмістом та включають в себе робочі потоки з питань охорони праці, адміністративних та технологічних питань.

Структура управління інформацією для поліцейських служб повинна забезпечувати якісну модель управління інформаціє і створюється, щоб допомогти поліцейським силам розробити ефективніші моделі управління інформацією [1]. Архітектура управління інформацією – це сукупність процесів, функцій, політики та рішень, які забезпечують ефективне та безпечне створення, збір, зберігання, зв’язок, оцінку, обмін та використання інформації.

Спираючись на досвід впровадження інформаційних систем у всьому світі, можна розділити управління інформацією на п'ять високо взаємопов'язаних складових: з**астосування** (трансформація інформації в практичну інформацію та розвідку для поліпшення стратегічних, оперативних та економічних рішень); д**оступність** (забезпечення гарантованого та ефективного доступу до інформації, що зберігається у високорозподілених середовищах у різних системах).

Кожна галузь має декілька компонентів – найважливіші з них процеси, функції та технології, необхідні для підтвердження цінності інформації.

Застосування.

Сили поліції мають доступ до величезної кількості накопиченої інформації. Завдання полягає в перетворенні цієї інформації в діючу розвідку для вдосконалення стратегічних, оперативних та обґрунтованих рішень.

Щоб досягти максимальної цінності аналітичного розуміння, поліцейські сили повинні забезпечити тих, хто приймає рішення, своєчасним доступом до відповідної інформації в момент необхідності. Для забезпечення ефективного використання даних архітектури управління інформацією повинні включати чотири компоненти:

– ***аналітика*** – рішення, які використовують кількісний, статистичний і дослідницький аналіз та прогнозне моделювання для створення однозначного та

корисного розуміння даних, які можуть бути неструктуровані або збережені в різних місцях;

– ***візуалізація даних*** – рішення, які представляють дані графічно, тому великі обсяги інформації можна передавати, інтерпретувати та діяти ефективно. Засоби візуалізації даних можуть використовуватися для виявлення зв'язків між людьми, об'єктами, місцями та подіями. Вони допомагають складати схеми злочинності, повідомляти та аналізувати ефективність роботи та оцінювати ефективність процесів та розподіл ресурсів;

– ***оптимізація інформаційного потоку*** – це програми реінжинірингу процесів, які визначають, де і коли потрібна інформація в поліцейських та адміністративних процесах щоб забезпечити точну, цільову інформацію, котра повинна бути доступною тим, хто її своєчасно потребує;

– ***мобільний та віддалений доступ введення даних*** – мобільні та віддалені рішення, що дозволяють незалежно від місця доступу до корпоративних систем вводити та отримувати доступ до даних у ході процесу.

Доступність.

Інформація про поліцейські дії, як правило, зберігається в різних системах, якими керується цілий ряд організацій. До них належать організації кримінальної юстиції, національної безпеки, місцевої та центральної влади, а також інших міжнародних організацій поліції. Створення безпечного та ефективного доступу до цієї інформації вимагає від корпоративних IT-систем та процесів, які надають дозволи користувачам, забезпечити запобігання несанкціонованому доступу до даних у складних середовищах.

Для забезпечення надійного та ефективного доступу до даних архітектура управління інформацією повинна включати три компоненти:

– ***контроль доступу*** – це рольові моделі контролю доступу, які надають дозволи користувачам на основі функцій реального завдання та рішення, що запобігають несанкціонованому доступу до даних.

– ***виявлення даних*** – рішення, які знаходять і впорядковують дані, щоб організації знали, де зберігаються активи даних, і лише тоді вони зможуть краще контролювати, управляти, захищати та отримувати доступ до них.

– ***ділові пошуки*** – рішення, які дозволяють користувачам шукати інформацію, що зберігається в різних місцях. Ефективні рішення для пошуку інформації дозволять отримати дані з широкого спектру джерел, також вводити складні пошукові запити та повертати консолідований список інформаційних ресурсів, класифікованих за релевантністю.

Використані джерела:

1. Information Management in Policing. Improving efficiency and performance by unlocking the value of information. [Електронний ресурс]. – Режим доступу: https://www.accenture.com/_acnmedia/accenture/conversion-assets/landingpage/documents/1/accenture-information-management-in-policing.pdf

Рибальченко Л.В.
доцент кафедри економічної та інформаційної безпеки ДДУВС, к.е.н.

СУЧАСНІ ТЕНДЕНЦІЇ ЗЛОЧИННОСТІ В УКРАЇНІ ТА СВІТІ

За офіційною статистикою щодо рівня злочинності в різних країнах світу (*Crime Index for Country*), країни, індекс злочинності в яких, нижче 20, вказує на незначні випадки злочинів, від 20 до 40 – це середній рівень, від 40 до 60 – помірний, від 60 до 80 – високий та від 80 до 100 найвищий.

Україна за рівнем злочинності у 2020 році знаходиться на 46 місці (48,85) із 129 країн світу, а рівень безпеки становить 51,15. Серед 40 країн Європи Україна займає 1 місце за рівнем злочинності. Далі йде Швеція, Франція, Ірландія та Молдова. Польща займає 28 місце за рівнем злочинності (28,5) та 13 місце за рівнем безпеки (71,5). Найнижчій рівень злочинності 40 місце (21,07) та найвищий рівень безпеки 1 місце (78,93) в Словенії (табл. 1).

Таблиця 1

Рівень злочинності в країнах Європи

Місце	Країна	Рівень злочинності	Рівень безпеки
1	Україна	48,85	51,15
2	Швеція	47,07	52,93
3	Франція	46,79	53,21
8	Велика Британія	43,71	56,29
21	Німеччина	34,81	65,19
28	Польща	28,5	71,5
33	Білорусь	24,99	75,01
34	Хорватія	24,67	75,33
35	Австрія	24,43	75,57
36	Ісландія	23,7	76,3
38	Естонія	23,14	76,86
39	Швейцарія	21,6	78,4
40	Словенія	21,07	78,93

На рис. 1 наведено найнижчий рівень злочинності в країнах Америки у 2020 році. Найвищий рівень безпеки в Кубі (70,98 - 1 місце), далі йде Канада (59,36 – 2 місце), Нікарагуа (54,46 – 3 місце), Панама (53,8 – 4 місце), США (52,3 – 5 місце).

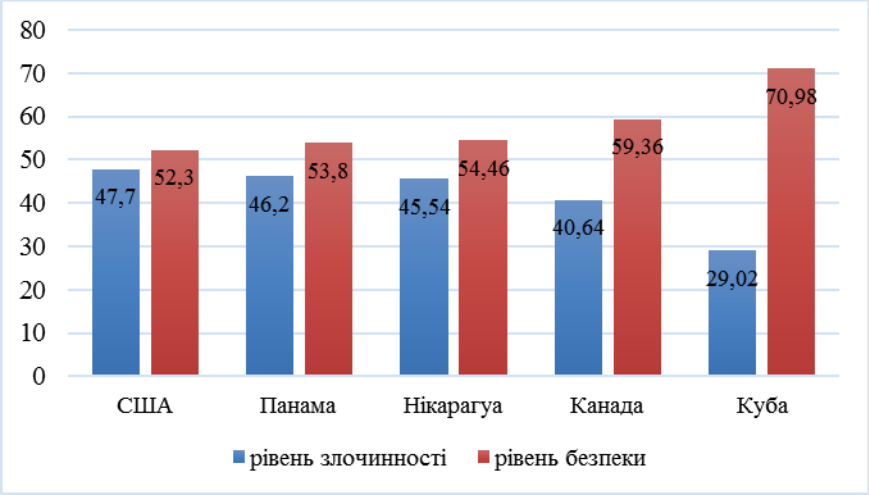


Рис. 1. Рейтинг країн Америки з найнижчим рівнем злочинності у 2020 році

Протягом останніх трьох років (з 2018 по 2020 рр), Україна покращила позиції у рейтингу злочинності і піднялася на десять сходинок вгору з 36 до 46 місця, США піднялися на три сходинки із 47 на 50 місце, Велика Британія із 47 (2018 р) на 65 (2020 р), Німеччина із 87 на 90 місце та Польща із 90 на 105 місце. Серед інших країн, що досліджено, Україна займає найнижчі позиції у рейтингу (рис. 2).

Сучасний стан злочинності в США характеризується тенденціями щодо зменшення рівня злочинності близько до 30%. Влада Великої Британії вживає заходи та приділяє увагу для зменшення рівня злочинності в країні через високу активність громадськості та підданих щодо партнерства з офіційними державними органами із запобігання злочинності. Основним засобом для досягнення цієї мети є децентралізація управління поліцейською системою. Політика орієнтування на громади є основним вектором розвитку британської правоохоронної стратегії, на запровадження якої виділяються чималі кошти із державного, місцевого бюджетів та із спонсорських джерел.

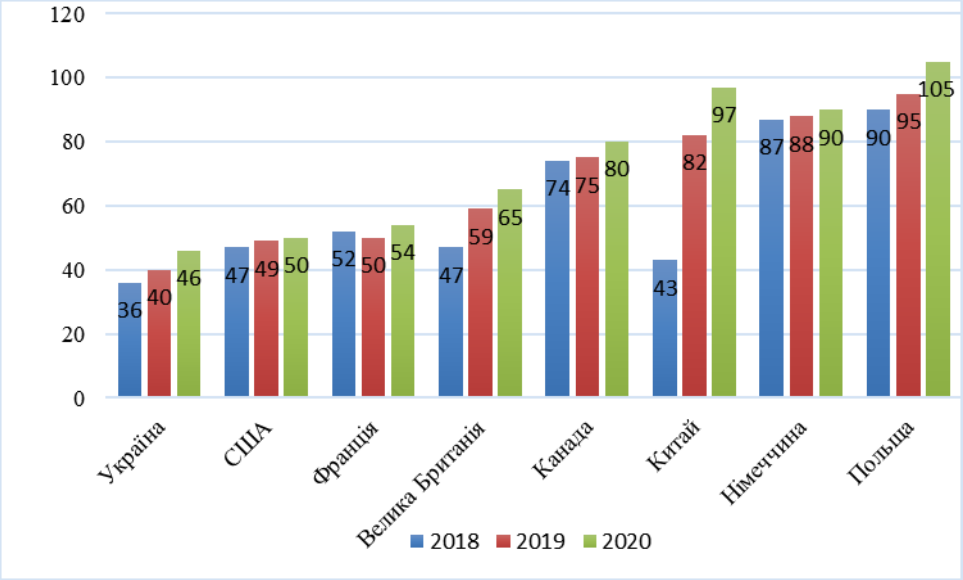


Рис. 2. Місце країн світу за рівнем злочинності у 2018-2020 роках

За рейтингом самих безпечних країн світу виступають: Швеція, Австрія,

Швейцарія, Німеччина, Норвегія, Данія, Ісландія, Японія, Люксембург та Сінгапур. Комфортна та безпечна атмосфера існує у Новій Зеландії, Сінгапурі та и Японії. В цих державах влада кілька десятиліть тому провела радикальні реформи в правозахисних сферах, реформувала суди, запровадила великі штрафи за порушення громадського порядку та законів.

Тому на державного і регіональному рівнях виникає необхідність постійного моніторингу рівня злочинності в країні, вживати заходи боротьби із злочинністю, забезпечувати високий рівня безпеки в Україні шляхом вдосконалення досвіду високорозвинених країн світу [2], використання їх досягнень, удосконалення прогалин у вітчизняній законодавчій та правовій базі, а також підвищувати рівень кваліфікації працівників та підрозділів правоохоронних органів для ефективної протидії економічній злочинності.

Використані джерела:

1. Рівень злочинності у світі. [Електронний ресурс]. – Режим доступу: - https://visasam.ru/emigration/vybor/prestupnost-v-mire.html

2. Rubalchenko L., Ryzhkov E. Ensuring enterprise economic security. SCIENTIFIC BULLETIN OF THE DNIPROPETROVSK STATE UNIVERSITY OF INTERNAL AFFAIRS. 2019. SPECIAL ISSUE №1.- P.268-271

Синиціна Ю.П. доцент кафедри економічної та інформаційної безпеки, к.т.н., доцент (Дніпропетровський державний університет внутрішніх справ, м. Дніпро)

СУЧАСНІ ПІДХОДИ ДО БЕЗПЕКИ ОПЕРАЦІЙНИХ СИСТЕМ

В області безпеки операційних систем в останні роки відбуваються помітні зміни. Все почалося з того, що в спільнотах розробників і в компаніях, що створюють операційні системи, поступово зміцнилося розуміння неможливості виправити все до однієї помилки в програмному коді. Розроблення питань захисту інформації, зокрема реалізації механізмів захисту сучасних операційних систем, займаються зарубіжні науковці В.Г. Проскурин, С.В. Крутов, І.В. Мацкевич [2], П.Б. Хорев [3], О.В. Казарін [4], проте стрімкий розвиток інформаційних технологій у сфері створення нових операційних систем безупинно дає матеріал для наукових досліджень. З урахуванням зазначеного більшість сучасних універсальних ОС не виконують у повному обсязі вимоги до захисту автоматизованих систем для оброблення конфіденційної інформації. Тому, вони не можуть без використання додаткових засобів захисту застосовуватися для захисту навіть конфіденційної

інформації. Утім, основні проблеми захисту тут викликані не тим, що не виконані окремі вимоги до механізмів захисту в ОС, а недосконалістю реалізованої в ОС концепції захисту, розроблення якої потребує подальшого наукового дослідження.

Операційна система є спеціально організованою сукупністю програм, яка управляє ресурсами системи (електронно-обчислювальної машини (ЕОМ), обчислювальної системи, інших компонентів інформаційно-обчислювальної мережі) з метою найбільш ефективного їх використання і забезпечує інтерфейс користувача з ресурсами.

Нажаль, проблеми з безпекою є майже у всіх операційних системах. Зробити щось ідеально — просто неможливо. Проте, іноді кількість «дірок» у безпеці виходить за всі допустимі рамки. Такі проблеми можуть як існувати з моменту створення ОС, так і з'являтися після деяких оновлень. За результатами аналізу, проведеної командою The Best VPN [4], сформовано своєрідний ТОП ОС, які мали найбільшу кількість таких «дірок» (рис. 1).

№№	Назва ОС	К-сть «дірок»
1	Android	414
2	Debian Linux	360
3	Windows Server 2016	357
4	Windows 10	357
5	Windows Server 2019	351
6	Adobe Acrobat Reader DC	342
7	Adobe Acrobat DC	342
8	cPanel	321
9	Windows 7	250
10	Windows Server 2008	248
11	Windows Server 2012	246
12	Windows 8.1	242
13	Windows RT 8.1	235
14	Ubuntu	190
15	Fedora	184

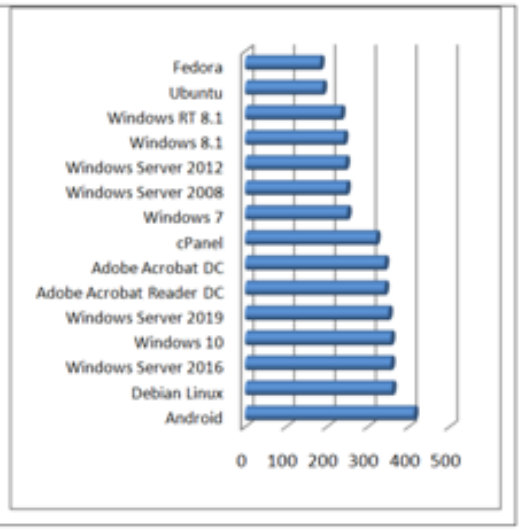


Рис. 1. Рейтинг ОС за кількістю виявлених «фейлів» за 2019 р.

У 2019-му безсумнівним лідером за кількістю фейлів стала Android. На другому місці розташувалася Debian Linux, а за нею — серверна Windows Server 2016 та Windows 10. Незважаючи на всі зусилля, у коді операційних систем, який стає все складніше, нові помилки додаються швидше, ніж виправляються старі. Частина з цих помилок призводить до вразливості інформаційної безпеки, що є серйозною проблемою. Щоб її вирішити, в галузі з'явилося два взаємодоповнюючих підходи, які почали покращувати ситуацію з безпекою операційних систем.

Перший підхід: ядро операційної системи має володіти засобами самозахисту. Іншими словами, в разі помилки або атаки система повинна безпечно обробити цю ситуацію. Існує популярна аналогія, де розробка операційних систем наших днів порівнюється з автомобільною індустрією 60-х років XX століття: тоді через величезну травматизму в ДТП автовиробники почали розробляти засоби безпеки для пасажирів, щоб автомобіль був не тільки надійний в звичайній ситуації, а й безпечний в разі аварії. Аналогічні технології розробляються в наші дні для

операційних систем. Зокрема, в цьому році фахівці Microsoft Security Response Center представили детальний огляд типів вразливостей і способів боротьби з ними в ядрі Windows. Також розроблена карта засобів захисту ядра Linux, яка відображає взаємозв'язки між типами вразливостей, методами їх експлуатації та наявними механізмами захисту.

Однак на практиці впровадження засобів самозахисту ядра операційної системи не буває безкоштовним. За підвищення безпеки зазвичай доводиться платити падінням продуктивності і додатковими складнощами для розробників системи. Наочним прикладом цього служать спроби усунення апаратних вразливостей Spectre, Meltdown, MDS на рівні операційних систем.

Другий підхід до вирішення проблеми помилок в операційних системах - це безперервне використання автоматичних засобів динамічного і статичного аналізу. Наші операційні системи написані на низькорівневих мовах програмування за цілою низкою причин. Такі мови дають розробнику більшу потужність і при цьому вимагають від нього великої уважності та професіоналізму. А людям властиво помилятися, тому на допомогу приходять автоматизовані засоби перевірки. Це і різноманітні методи статичного аналізу, включаючи пошук помилок по паттернам, і технології динамічного аналізу, однією з найпопулярніших серед яких став фаззинга (методика тестування ПО випадковими даними). Прикладом проекту, що вносить значний вклад в безпеку багатьох операційних систем, є фаззер syzkaller.

При цьому у розвитку автоматизованих засобів пошуку вразливостей є важливий побічний ефект: вони доступні не тільки захисникам, а й атакуючим.

Слід зазначити, що не існує одного стандарту захисту, а захист не є бінарним вибором. Те, наскільки захищена оперативна система, потрібно розглядати в контексті потреби організації. Саме тому найбільш результативним сьогодні вважається комплексний підхід. Виділивши окремо найбільш важливі елементи ОС можна добитися повноцінного захисту системи із повноцінним захистом, найбільш наближеним до ідеального.

Використані джерела:

1. Проскурин В.Г. Защита в операционных системах / В.Г. Проскурин, С.В. Крутов, И.В.Мацкевич. – М. : Радио и связь, 2000. – 168 с.

2. Хореев П.Б. Методы и средства защиты информации в компьютерных системах / П.Б. Хорев. – М. : Академия, 2005. – 256 с.

3. Казарин О.В. Безопасность программного обеспечения компьютерных систем / О.В. Казарин. – М. : МГУЛ, 2003. – 212 с.

4. ТОП ОС за визначенням команди The Best VPN. Електронний ресурс. URL: https://9to5google.com/2020/03/06/android-vulnerabilities-report-2019/

Проценко О.В.
науковий співробітник відділу організації
наукової роботи ДДУВС

ДУАЛЬНА ОСВІТА ЯК ЕФЕКТИВНИЙ ІНСТРУМЕНТ ІНФОРМАЦІЙНОЇ ПІДГОТОВКИ ФАХІВЦІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Законом України «Про освіту» передбачаються наступні форми здобуття освіти: інституційна (очна (денна, вечірня), заочна, дистанційна, мережева); індивідуальна (екстернатна, сімейна (домашня), педагогічний патронаж, на робочому місці (на виробництві); дуальна [1].

Дуальна форма здобуття освіти – це спосіб здобуття освіти, що передбачає поєднання навчання осіб у закладах освіти з навчанням на робочих місцях на підприємствах, в установах та організаціях для набуття певної кваліфікації [2].

Розпорядженням Кабінету Міністрів від 19 вересня 2018 р. № 660-р. затверджено Концепцію підготовки фахівців за дуальною формою здобуття освіти [2]. Ця Концепція ґрунтується на німецькому досвіді дуальної форми здобуття освіти.

Підготовка співробітників правоохоронних органів у Німеччині здійснюється, як правило, в поліцейських школах (центрах підготовки співробітників поліції). Незважаючи на те, що програми підготовки поліцейських можуть відрізнятися в кожному окрузі, принцип дуальності є спільним для всіх.

В середньому практична складова навчання в Німеччині за програмами підготовки фахівців 1-го базового рівня за три роки становить близько 40 %. У Німеччині з фахівцями, які досягають високих показників у службовій діяльності, а також є найбільш підготовленими і здатними до педагогічної діяльності співробітниками, укладають контракт на чотири роки. Після цього він повертається до підрозділу, з якого був направлений в навчальний центр. Тобто викладач розуміє, що через певний період йому необхідно буде повернутися в той підрозділ, з якого він прибув, і перебувати в освітній організації до закінчення своєї служби він не зможе [3]. В таких умовах педагогічні кадри постійно підвищують рівень майстерності.

Отже, маючи інформацію про позитивний досвід впровадження дуальної освіти в провідних країнах світу, вважаємо, що в українських закладах вищої освіти є всі підстави для проведення відповідних реформ в освіті. Вважаємо, що саме дуальна освіта є засобом професійної соціалізації молоді, оскільки надає їй найкращі можливості для отримання кваліфікації.

Безумовно, навчання поліцейських повинно тривати постійно.

Так, згідно із п. 5 Положення про організацію службової підготовки працівників Національної поліції України від 26.01.2016 р. №50 (із змінами, внесеними згідно з Наказом Міністерства внутрішніх справ №51 від 21.01.2020), основними завданнями службової підготовки є [4]:

підвищення рівня знань, умінь, навичок та професійних якостей поліцейських з метою забезпечення їх здатності до виконання завдань з охорони прав і свобод

людини, протидії злочинності, підтримання публічного (громадського) порядку та безпеки;

вивчення нормативно-правових актів, які регламентують діяльність Національної поліції України;

удосконалення керівним складом органів (підрозділів) поліції, закладів, установ поліції навичок управління поліцейськими.

При цьому згідно із п. 7 цього ж Положення, орієнтовними формами службової підготовки є: навчальні заняття в групах за місцем служби; навчальні збори; дистанційна підготовка або самостійне навчання (проводиться впродовж усього строку служби поліцейського з метою безперервного, систематичного поповнення та поглиблення знань, умінь і навичок, необхідних для успішного виконання службових завдань).

Вважаємо за доцільне в удосконаленні методичного забезпечення інформаційної підготовки фахівців Національної поліції України введення в освітній процес більшої кількості практичної частини навчання починаючи з першого курсу. Знання потрібно використовувати та вміти оперувати ними у своїй службі. Для досконального закріплення пройденого матеріалу пропонується дуальна освіта майбутніх поліцейських. Окрім отримання можливості застосувати отримані за час навчання знання, з'являється можливість інформаційного обміну між майбутніми фахівцями та практиками. Так студент, який став безпосереднім учасником внутрішньої роботи поліції, може вносити свої пропозиції з удосконалення методичного забезпечення до наукових лабораторій після проходження практики, а також надавати оновлену, отриману під час навчання інформацію до поліцейських підрозділів. Враховуючи те, що законодавство постійно змінюється та оновлюється, інформаційна підготовка повинна бути постійною та невід'ємною частиною не тільки в підготовці фахівців Національної поліції України, а й для діючих співробітників поліцейських підрозділів. Для цього пропонуємо створити спеціальний мобільний додаток з алгоритмами дій, законами, наказами та інш., який буде постійно оновлюватись. Пропозиції до якого будуть вносити як студенти, так і діючі співробітники. Пропонується створити спеціальні анкети для визначення проблемних питань з обох сторін. В Україні популярним серед поліцейських є мобільний додаток «Патруль», але проблема в тому, що оновлення цієї програми не є постійним. Актуальність деяких нормативних документів вже давно втратила чинність, що вводить в оману як діючих працівників, так і студентів. Тому за рахунок введення дуальної освіти для підготовки фахівців Національної поліції України збільшиться рівень професійних знань та удосконалення інформаційного обміну стане результатом підвищення інформаційної обізнаності як студентів так і діючих працівників поліції. Дана система допоможе вирішувати проблемні питання сьогодення, закріплювати знання майбутніх фахівців, чим виведе інформаційне забезпечення на вищий рівень.

Використані джерела:

1. Закон України «Про освіту». [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2145-19

2. Розпорядження Кабінету Міністрів України «Про схвалення Концепції підготовки фахівців за дуальною формою здобуття освіти» від 19 вересня 2018 р. № 660-р. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/660-2018-р

3. Наказ від 26.01.2016 № 50 «Про затвердження Положення про організацію службової підготовки працівників Національної поліції України». [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua/laws/show/z0260-16#Text

Панченко Л.В.
Науковий співробітник відділу організації наукової роботи ДДУВС, викладач вищої категорії, викладач-методист

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ПРАВООХОРОННІЙ ТА ЮРИДИЧНІЙ ДІЯЛЬНОСТІ: МІЖНАРОДНИЙ ДОСВІД

В умовах розвитку сучасного суспільства на тлі загострення криміногенної ситуації в Україні надзвичайно актуальною є проблема правильного розроблення, впровадження та застосування нормативно–правових актів для забезпечення оптимального розвитку інформаційних технологій в Україні.

В Стратегії **національної безпеки України затвердженої** Указом Президента України від 14 вересня 2020 року № 392/2020. п.9 вказано, про стрімке зростання ролі інформаційних технологій у всіх сферах суспільного життя. В п.п. 51-52 розкрито основне завдання розвитку системи кібербезпеки, яке гарантується через кіберстійкість та кібербезпеку національної інформаційної інфраструктури, важливим завданням, окрім іншого є поширення цифрової грамотності серед населення України [10].

У Окінавській хартії глобального інформаційного суспільства, від 2000 року було закріплено, що «всі люди повсюдно, без винятку повинні мати можливість користуватися перевагами глобального інформаційного суспільства», на думку міжнародної спільноти країн Великої вісімки, які підписали хартію, «Права, закріплені у Загальній декларації прав людини, повинні бути реалізовані в інформаційну епоху, перебувати під захистом держави і суспільства незалежно від розвитку і впровадження нових технологічних досягнень»[6; с.74].

Наразі в Україні існує проблема недосконалості законодавчої бази, тому окрім удосконалення технічної сторони питання інформаційних технологій необхідно в першу чергу заповнити прогалини законодавчої бази в правоохоронній та юридичній діяльності.

Роль держави полягає в розробці законів та створенні компетентних правоохоронних та судових органів для забезпечення діяльності осіб, які надають

кваліфіковану юридичну допомогу. Для цього, необхідна якісна комплексна система правового забезпечення, що було вимогою викладеною в принципах та керівних положеннях ООН, 2012 року (резолюція 67/1872). [2; 9].

Одним з аргементів, який виступає на необхідність упорядочення та удосконалення правового забезпечення в інформаційній та юридичній діяльності є дані Лаабораторії Касперського, згідно яких, за останні 12 місяців, кожна друга промислова компанія пережила кіберінциденти в інформаційного характеру на усунення яких, було витрачено близько 497 тісяч доларів США[11].

Проблеми правового забезпечення інформаційних технологій розглядали в своїх працях Голубев В.А, Касперский Е., Вайман Г., Каплан Є., Коллін Б., та інші.

Бубницька О.П. в своїх працях дає таке визначення: «Правове забезпечення - сукупність правових норм, що визначають створення, юридичний статус і функціонування інформаційних систем, що регламентують порядок одержання, перетворення й використання відомостей».

Доступ до справедливого правосуддя на всіх рівнях має безапеляційне значення для всіх категорій населення в кожній країні.

Юридична допомога є важливим елементоми системи яка надає доступ до системи правосуддя кожної особи в державі.

Право на безоплатну юридичну допомогу викладено та вперише закріплено в Міжнародному пакті про громадянські та політичні права 8 , в с. 14(3)(d) [2; с.13].

Експертами Венеціанської комісії створено матеріали в яких відображено досвід судочинства країни Азії, що буде корисним в юридиній діяльності. [3; с.40-45].

Орієнтуючись на інтеграцію України до ЄС необхідно орієнтуватися на стратегію розвитку країн-учасниць ЄС та НАТО в інформаційній сфер, дотримуючись всіх вимог правового забезпечення в првоохоронній та юридичній діяльності [4;62].

Тому важливим є міжнародний досвід в становленні розвитку та адаптації законодавчої бази стосовно інформаційного забезпечення, оскільки події останніх років доводять, що Україна не готова до інформаційних війн, які ведуться на сьогодні в інтернет просторі.

На країни, які є членами Північноатлантичного Альянсу та Європейського Союзу. поширюються стандарти міжнародних організацій щодо інформаційної політики та забезпечення інформаційної безпеки.

Серед основних загроз в інформаційній сфері виділяють три складові: ведення інформаційної війни, інформаційний тероризм, інформаційні злочини.

Головними є стандарти НАТО щодо захисту інформації, викладені у Документі СМ (2002)49 “Безпека в організації Північноатлантичного договору (НАТО)”, офіційна політика НАТО у сфері кіберзахисту , стратегічна концепція кібербезпеки, сформульована за результатами Лісабонського саміту й уточнена за результатами Варшавського саміту. [4; с.63].

Для безпеки інформаційного простору Стратегії кібербезпеки розроблені на сьогодні в більшості є країн світу, таких як Австрія, Австралія, США, Ізраїль, Великобританія, Естонія, Іспанія, Італія, Канада, Латвія, Німеччина, Польща, Франція, Чехія таа інших [5;32-38].

Особа в інформаційному просторі наражається на небезпеку і загрози.

Інформаційне середовище не збігається зі звичною для суспільства тому необхідні норми, розроблені для регулювання інформаційно-просторових відносин, які б попереджували вчинення правопорушень та злочинів, що є особливо важливим в діяльності правоохоронних органів.

З 2018 року для Румунії та Болгарії, як і інших країн-членів ЄС, набули чинності нові правила захисту персональних даних (GDPR, важливим є введення більш суворого покарання за несвоєчасне повідомлення інформації про виток даних. Компаніям, які порушили положення та не доповіли про факт витоку або злому протягом 72 годин з моменту інциденту, загрожує штраф до 4 % річного доходу або до 20 млн. євро. [4; с.64].

У забезпеченні кібербезпеки Румунії відводиться її спеціальному контррозвідувальному органу – Румунській службі інформації, у структурі

якої створено національний центр кібербезпеки. Румунія забезпечує функціонування динамічного інформаційного середовища на основі функціональної сумісності й послуг, характерних для інформаційного суспільства, а також забезпечення відповідності основних прав і свобод громадян та інтересів національної безпеки у відповідних правових рамках. [4; с.64-65].

У квітні 2016 року в Болгарії розроблено проект Національної стратегії кібербезпеки під назвою "Стійка до кібератак Болгарія 2020", серед інших в якій ініціювання законодавчі зміни щодо забезпечення високого загального рівня мережної й інформаційної безпеки , а також для захисту політичних і виборчих прав громадян і в кіберпросторі; реалізації мережної моделі обміну інформацією й координації між організаціями, відповідальними за кібербезпеку у Болгарії.

В законодавстві Молдови в січні 2010 року прийнято Закон "Про попередження та боротьбу зі злочинністю у сфері комп'ютерної інформації". Згідно із яким генпрокуратура Молдови наділена повноваженнями координувати й здійснювати кримінальне переслідування осіб, що вчинили кіберзлочини. [4; с.67].

В Білорусії діє державна система спостереження (СОРМ), яка здійснює повний он-лайн-нагляд у всій країні, що регламентується значною кількістю нормативно-правових актів. Тут немає спеціальних законів, присвячених протидії кіберзлочинності, але деякі аспекти регулюються Кримінальним кодексом і законами, що стосуються регламентації діяльності глобальної інформаційної мережі Інтернет, що є достатньо ефективним, для інформаційної держави.[4; с.71].

У 2000 році в КНР створено «Проект С219» «електронної стіни» навколо національної зони мережі Інтернет. Китай є одніє з 20 країн , яка суворо регулює, доступ своїх громадян до інформаційної мережі. З 2011 року проголошено, про стоворення онлайн-армії «Блакитні мундири», для попередження кіберзагроз. Правилами регулюється діяльність блогерів, яких в країні понад 180 млн. Для доступу до мережі існує віковий ценз та триступенева система ідентифікації. Широко публікується інформація про арешти блогерів –дисидентів,тощо. Окрім того існує система матеріальних заохочень про повідомлення за інформаційні загрози. Так, приміром, за сигнал про поширення порно контенту винагорода від 60 - 241 дол. США. Та інші. .[12; с.96].

В Законі «Про кібербезпеку КНР», від 2016 року вказано на захист від випадкового чи навмисного витоку даних.[9; с.406].

В 2009 році в США затверджена «Комплексна національна ініціатива з кібербезпеки», яка спрямована на захист громадянських свобод особи . Кіберзагрози проти країни прирівнюються до інформаційної війни.

Для заборони поширення недостовірної інформації у Франції не потрібно дозвіл суду, лише рішення правоохоронних органів. [7; с.20].

Отже, для вирішення проблеми правового забезпечення інформаційної безпеки в правоохоронній та юридичній діяльності, суспільства, держави, Україна має співпрацювати з іншими країнами орієнтуючись на стандарти ЄС та НАТО. Для України є важливим досвід країн Східної Європи, щодо приведення національного законодавства у відповідність до вимог міжнародних організацій, щодо забезпечення балансу між свободою й безпекою в інформаційній сфері на законодавчому рівні.

Використані джерела:

1.Паспорт информационнной безопасности. Режим доступа: https://digital. gov.ru/uploaded/files/pasport-federalnogo-proekta-informatsionnaya-bezopasnost. pdf

2. Справочник по обеспечению качества юридической помощи в процессах уголовного правосудия: Практическое руководство и перспективная практика. Организация Объединенных Наций, февраль 2020 года.

3. Judicial systems of Central Asia a comparative overview Edited by G. Dikov Moscow Jurisprudence 2015,-328 c.

4. Ткачук Т.Ю., Забезпечення інформаційної безпеки: досвід окремих країн Східної Європи (ст. 62-72).//Журнал "Інформація і право" № 4(23)/2017.

5. Законодавство та стратегії у сфері кібербезпеки країн європейського союзу сша, канади та інших. Режим доступу: https://parlament.org.ua/wp-content/uploads/2016/11/INFODOVIDKA-ZAKONODAVSTVO-TA-STRATEGIYI-KIBERBEZPEKA.pdf

6. Ольга Золотар.Інформаційна безпека людини: теорія і практика. Монографія.-Київ 2018.

7. Сардарова Валерия Анатольевна. Вопросы кибербезопасности в американо-Китайском взаимодействии Cybersecurity in the US-China Interaction. Санкт-Петербург, 2018.

8. Кучмій О.П. Стратегія інформаційної безпеки в структурі внутрішньої й зовнішньої політики КНР.

9. Н.О. Піпченко. Здійснення політичної комунікації в китаї засобами мережі інтернет. Режим доступу: //http://vmv.kymu.edu.ua/v/p05/ar401414.pdf.

10. Указ Президента України , №392/2020 Про рішення Ради національної безпеки і оборони України від 14.09. 2020 року «Про Стратегію національної безпеки України».Режим доступу: https://www.president. gov.ua /documents /3922020-35037.

11. Офіційна інформація про дані Лабораторії Кассперського. Режим доступу: https://genproc.gov.ru

12. Дубцов Д. Політика Укитаю, щодо регулювання внутрішнього інфопростору.// Політичний менеджмент.№4, 2010.

Железняк О.Г.
завідувач сектору дактилоскопічного обліку відділу криміналістичних видів досліджень Донецького НДЕКЦ МВС
Баранова Н.О.
головний судовий експерт сектору дактилоскопічних досліджень відділу криміналістичних видів досліджень Донецького НДЕКЦ МВС

ПРОБЛЕМНІ ПИТАННЯ ДАКТИЛОСКОПІЧНОГО ОБЛІКУ

Все в світі зазнає змін, розвитку та науково-технічного прогресу. Це торкнулось і науково-технічного розвитку дактилоскопії в експертній практиці. Впровадження в роботу експертних підрозділів автоматизованих дактилоскопічних інформаційних системи (АДІС), за допомогою яких почав вестись облік і перевірка слідів рук, вилучених з місць нерозкритих злочинів (в тому числі минулих років, за які були накопичені значні масиви дактилоскопічної інформації), в свій час стало свого роду «проривом» в даній сфері діяльності. Значна кількість злочинів, розкритих за допомогою дактилокартотек, привела до зміщення акцентів в сторону інформаційно-пошукової діяльності та ідентифікаційних дактилоскопічних досліджень [1].

Так, введення в роботу експертних підрозділів МВС АДІС дало великий прогрес в розкриті злочинів, але час йде і виникають нові проблемні питання в роботі дактилоскопічного обліку, а це, перш за все, оновлення версій АДІС «Дакто-2000»; матеріально-технічне забезпечення; вирішення прогалин в нормативно-правовій базі щодо функціонування дактилоскопічного обліку та взаємодії досудових органів з Експертною службою з цього питання; якість і кількість об’єктів дактилоскопічного характеру, тощо.

На сьогоднішній день в експертних підрозділах МВС використовується автоматизована дактилоскопічна ідентифікаційна система «Дакто-2000», яка призначена для автоматизації дактилоскопічних обліків. АДІС «Дакто-2000» реалізує наступні функції: - Введення в базу даних відбитків пальців рук (дактилокарт) і демографічних даних; - Введення в базу даних слідів пальців рук, вилучених з місць нерозкритих злочинів; - Зберігання і керування базою даних відбитків пальців рук (дактилокарт); - Зберігання і керування базою даних неідентифікованих слідів пальців рук; - Проведення та аналіз пошуків «дактилокарта - база даних дактилокарт»; - Проведення та аналіз пошуків «дактилокарта - база даних неідентифікованих слідів пальців рук»; - Проведення та аналіз пошуків «слід - база даних дактилокарт»; - Проведення та аналіз пошуків «слід - база даних неідентифікованих слідів пальців рук»; - Підготовка та друк результатів пошуку; - Створення статистичних звітів; - Проведення пошуків за демографічними даними і їх комбінацій (П.І.Б., дата народження і т.д.) [2].

Саме після проведення реформи правоохоронної системи в Україні, яка розпочалась в 2014 році, знизився рівень якості і кількість вилучених об’єктів дактилоскопічного

характеру.

Аналізуючи сучасний стан нормативного регулювання порядку функціонування дактилоскопічного обліку Експертної служби МВС України [3], а також процесу взаємодії органів досудового розслідування зі співробітниками підрозділів експертної служби [4], констатуємо, що його рівень, на жаль, поки що не є достатнім. В Інструкції про порядок функціонування дактилоскопічного обліку експертної служби МВС України взагалі останні зміни були в 2011 році. Нормативні й організаційні проблеми взаємодії органів досудового розслідування з працівниками Експертної служби МВС України не набули належної теоретичної розробки, що призводить і до суттєвих труднощів у практичній діяльності. Низка питань правового й організаційного характеру залишається не вирішеною, що стримує більш повне використання можливостей сумісної діяльності цих суб'єктів, підвищення її результативності.

Для вирішення вищевикладених проблем пропонуємо проводити спільні семінари, заняття з залученням працівників органів досудового розслідування поліції та Експертної служби Міністерства внутрішніх справ України, під час яких обговорювати проблемні питання та шляхи їх вирішення. Розробляти інформаційні листи, пам'ятки, рекомендації, тощо, для працівників органів досудового розслідування поліції, що сприятиме покращенню взаємодії органів та якісній роботі для розкриття злочинів.

Дактилоскопічні дослідження та обліки повинні розвиватись на базі сучасної науково обґрунтованої методичної бази, адаптованої до можливостей прогресивного розвитку технічного і правового забезпечення усіх етапів дослідження слідів рук, в тому числі подальшого розвитку АДІС.

Використані джерела:

1. Мамайчук Г.С. Дактилоскопічне дослідження: роль і місце в судові й експертизі, ефективність і перспективи розвитку Криминалистика и судебная экспертиза. 2014. Вып. 59. С. 271-278. Режим доступу: http://nbuv.gov.ua/UJRN/krise_2014_59_35 (дата звернення: 08.11.2020)

2. АДІС «Дакто-2000» Автоматизована дактилоскопічна ідентифікаційна система [Електронний ресурс]. – Режим доступу: URL:http://es-trade.kiev.ua/uk/afis-dakto-2000-automated-fingerprint-identification-system.6X6MHT/ (дата звернення: 08.11.2020).

3. Про затвердження Інструкції про порядок функціонування дактилоскопічного обліку експертної служби МВС України: Наказ Міністерства Внутрішніх Справ України від 11.09.2001 №785. [Електронний ресурс]. – Режим доступу: URL:https://zakon.rada.gov.ua/laws/show/z1066-01#Text (дата звернення: 08.11.2020).

4. Про затвердження Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні : Наказ Міністерства Внутрішніх Справ України від 07.07.2017 № 575. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/z0937-17#Text (дата звернення: 08.11.2020).

Станіна О.Д. – старший викладач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ, к. т. н.

НЕЙРОННІ МЕРЕЖІ: МОЖЛИВОСТІ ТА ПРОБЛЕМИ ВИКОРИСТАННЯ

Нейронні мережі (НМ) з кожним днем стають все більш розповсюдженими в нашому сьогоденні. Більшість з нас не задумується над тим, що використовує їх кожен день: під час взаємодії з голосовим асистентом Siri, розпізнавання обличчя для розблокування мобільного телефону, при побудові маршруту до найближчої кав'ярні, пошуку фільму тощо. Потенціал НМ дуже високий, тому можна зробити припущення, що їх розповсюдження надалі буде лише збільшуватися. І цьому є об'єктивна причина: НМ – це універсальні апроксиматори функцій. Тобто за використання НМ з великою ємністю можна апроксимувати будь-яку нелінійну функцію.

Проте, вони не бездоганні та мають свої недоліки. І це добре було показано Яном Гудфеллоу в його статті [1], у якій він продемонстрував, що при додаванні шуму до початкового знімку панди НМ розпізнавала остаточну картинку як гібона, хоча з початковим зображенням таких проблем не було. Це здається кумедною особливістю НМ, але в реальності може мати досить суттєві негативні наслідки для поліції, медицини, банківської сфери тощо.

Всі атаки на НМ, в залежності від усвідомленості зловмисника, можна умовно поділити на атаки білої та чорної скриньок. Атаки білої скриньки виникають тоді, коли зловмисник має доступ до базової мережі, а отже - до архітектури. А коли архітектура мережі йому відома, він може керувати окремими нейронами, а отже - привести НМ до помилкового висновку. Атака чорної скриньки виникає в тому випадку, коли зловмисник нічого не знає про будову архітектури мережі. Хоча така атака є більш складною, велика кількість злочинців вдається до неї також.

Найбільш розповсюдженим типом атак, в залежності від способу впливу на мережу, є так звані атаки в обхід (evasion attack), сутність яких полягає в тому, що зловмисник, використовуючи початкові дані та шум, створює змагальні приклади - вхідні умови, які модифіковані таким чином, щоб ввести НМ в оману (наприклад, спуффінг-атаки на біометричні системи, які набувають широке розповсюдження [2]).

Найбільш небезпечною вважається так звана отруйна атака (poisoning attack), сутність якої полягає в порушенні процесу навчання НМ завдяки спеціально згенерованим зразкам. Найчастіше такі атаки виникають у випадку наявності онлайн-навчання мережі і лише у виключних випадках - через отримання інсайдерської інформації. Слід зазначити, що зловмисник, який використовує даний тип атак повинен мати високий рівень компетенції в Data Science.

Всі зазначені вище атаки відносяться до програмного типу, але науковці також виділяють фізичний різновид нападу на НМ. Прикладом таких атак можуть виступати так звані «змагальні стікери», певне розташування яких на фізичному

об’єкті призводить до хибного висновку [3].

Зараз вже існує досить велика різноманітність методів навчання НМ, які дозволяють запобігти атакам різних типів. Крім того, розроблено ряд методів для захисту нейронних мереж; найбільш розповсюдженими серед них є:

- Змагальна підготовка – передбачає самостійне створення змагальних прикладів для навчання НМ. Такий метод захисту можна вважати найкращим способом протидії зловмиснику, адже він робить мережу більш стійкою до кібератак.
- Регулізація – допомагає згладжувати границі прийняття рішень між класами та спрощує класифікацію мереж.
- Змішування – дозволяє збільшувати навчальний набір, а отже - знижує залежність класифікації від невеликої кількості нейронів.
- Тестування на проникнення – комбінує усі вищезгадані методи та передбачає залучення спеціалістів з кібербезпеки для виявлення уразливості мережі та розміру можливих збитків.

Отже, виявлення та запобігання вторгнень є однією з найважливіших задач в області інформаційної безпеки. З ростом зацікавленості світу до глибокого навчання, популяризації біометричних систем та автономних машин, повсюдного впровадження штучного інтелекту та НМ у житті сучасної людини все гостріше стає питання інформаційної безпеки та важливості протистоянню кібератакам. Слід пам’ятати, що світ не стоїть на місці, та разом з виникненням нових можливостей постають проблеми щодо їх використання.

Використані джерела:

1. Goodfellow, Ian & Shlens, Jonathon & Szegedy, Christian. Explaining and Harnessing Adversarial Examples. 2014, URL: https://arxiv.org/abs/1412.6572

2. Мирошниченко В.О. Біометрічна ідентифікація клієнтів в банківській сфері. Міжнародна та національна безпека: теоретичні і прикладні аспекти. Матер III Міжнар. наук-практ. конф. (м. Дніпро, 15 бер.2019 р.) Дніпро: Дніпроп. держ. ун-т внутр. справ, 2019, с. 263 - 265.

3. Kevin Eykholt, Ivan Evtimov, Earlence Fernandes, Bo Li, Amir Rahmati, Chaowei Xiao, Atul Prakash, Tadayoshi Kohno, Dawn Song, Robust Physical-World Attacks on Deep Learning Models, 2017 URL: https://arxiv.org/abs/1707.08945

Гребенюк А.М.
доцент кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ,
канд. техн.наук, доцент

ОПЕРАТИВНЕ РОЗПІЗНАВАННЯ ВІДЕОДАНИХ З ВИКОРИСТАННЯМ СИСТЕМИ ИНТЕЛЛЕКТУАЛЬНОГО ВИДЕОАНАЛІЗУ

Відеоспостереження існує вже дуже довгий час, ймовірно, набагато довше ніж багато хто може собі уявити. Системи відеоспостереження на основі технології телебачення замкнутого контуру (CCTV) застосовуються з середини 1960-х років. Ключова подія сталася в 1969 році, коли на урядовій будівлі Нью-Йорка були встановлені відеокамери. У той час як дані системи набували все більшого поширення, користувачі ймовірно швидко зрозуміли, що відеоспостереження - нелегке завдання.

Дослідження показують, що при збільшенні кількості камер, які повинен обслуговувати оператор, їх ефективність зменшується. Таким чином, хоча відеоспостереження могло забезпечити всебічний огляд території, ця інформація не використовувалася в повній мірі. Нарешті, з'явилося рішення даної проблеми - технологія аналізу відеоданих (VCA), зараз більш відома як «відеоаналітика».

Використовуючи комбінацію алгоритмів, система відеоаналітики аналізує отримуване відео в режимі реального часу і оповіщає про будь-яку подію, на ідентифікацію якого налаштоване програмне забезпечення.

Технологія відеоаналітики пройшла довгий шлях. За останні 10 років ця технологія досягла в своєму розвитку рівня інших технологій і знаходиться зараз в четвертому поколінні. Сучасні відеоаналітичні додатки здатні робити набагато більше, ніж просто виявляти рух, а кількість помилкових тривог зведено до незначного рівня.

Більшість базових систем відеоаналітики просто виявляють рухомі об'єкти, але не розпізнають їх природу. Використовуючи технологію класифікації об'єктів, сучасне відеоаналітичне програмне забезпечення здатне розрізняти типи рухомих об'єктів, наприклад, людей або машини. Також дане програмне забезпечення здатне фільтрувати деякі рухомі об'єкти, такі як рухома рослинність, хиткий паркан, тіні, світло автомобільних фар.

В теперішній час встановлюють новітні PTZ камери які здатні повертатися слідом за об'єктом, який рухається по території, і збільшувати певні сцени, щоб отримати більш велике і чітке зображення. Не менш важливою є здатність PTZ камери збільшувати відстежуваний об'єкт, щоб отримати більш деталізоване зображення. Це робить автоматичне PTZ стеження вкрай корисним не тільки для подій реального часу, але також для цілей ідентифікації і для аналізу відеоматеріалу постфактум.

Програмне забезпечення для аналізу відеоконтенту — це технологічне рішення на основі штучного інтелекту, яке пропонує спектр аналітичних

можливостей для покращення систем відеоспостереження, що дозволяє користувачам вкладати інвестиції для:

- Пошуку та фільтрації по переважній кількості відеоматеріалів, для дієвої безпеки;
- Запуску сповіщень в режимі реального часу, щоб підвищити ситуаційну обізнаність та прискорити реагування при виникненні загроз або надзвичайних ситуацій;
- Кількісної оцінки відеоданих та використання метрик для планування, розробки та оптимізації операцій. [1]

Це все дало можливість впроваджувати в м. Дніпро програму "Безпечне місто" яка працює з 2016 року та була затверджена рішенням міської ради від 30.03.2016 № 14/5. В рамках реалізації заходів Програми були реалізовані вже три етапи створення Системи відеоспостереження.

На І етапі у 2017 році було встановлено 350 оглядових камер та створена основа Системи - Центр обробки даних та були створені 2 центри моніторингу – в Головному управлінні національної поліції в Дніпропетровській області та в Дніпропетровському обласному управлінні СБУ.

На другому етапі будівництва у 2018 році до Системи були підключені ще 399 камер, більша частина яких «навчена» виконувати спеціалізовані аналітичні функції ,вперше у нашому місті були задіяні камери нового типу:

- 15 керованих (роботизованих) камер, які дозволяють оператору Системи скерувати камеру на ту чи іншу частину зображення, приблизити його до необхідного рівня;
- 5 панорамних (оглядових) камер, які дозволяють водночас проводити огляд значної частини міста та крім того цими камерами також можливо керувати.
- 10 мобільних комплексів, для встановлення у місцях де немає можливості підключення до мережі постійного електроживлення та комунікаційних мереж.

При реалізації третього етапу створення Системи у 2019 році було встановлено ще 471 камера, в т.ч.

-100 керованих (роботизованих) камер, які добре себе зарекомендували в роботі;
-близько 200 LPR (аналітичних) камер, у т.ч з розширеними аналітичними функціями: визначення кольору та марки автомобіля, підрахунок кількості транспорту та ін. [2].

Широке застосування аналітики відеоконтенту дозволяє користувачам використовувати ці відео, без серйозних витрат часу та робочої сили. Завдяки легкому пошуку, дії та кількісній оцінці відео, ресурси можуть бути перерозподілені між різними службами.

Розвиток інтелектуальної відеоаналітики відбувається за двома основними технологіями - це трекінг і ідентифікація. На основі правил, закладених в алгоритм відеоаналізу, будується весь функціонал системи, який вкрай необхідний для побудови сучасних систем відеоспостереження.

Трекінг - це коли алгоритм обробки відео шукає в кадрі рух, визначає і класифікує об'єкт, що рухається, описує його характеристики (розмір, колір, швидкість). Варіантів трекінгу (відеодетектора) може бути досить багато.

Ситуаційні детектори - це коли, об’єкт спостереження перетинає уявні лінії в кадрі, після чого система видає сигнал тривоги:

- перетин об'єктом прямої лінії в заданому напрямку;
- рух в зоні;
- вихід об'єкта із зони;
- зупинка об'єкта в зоні;
- залишений в зоні предмет.

Сервісні детектори - це функціонал (програмне забезпечення), який виробники вже вбудовують в свої IP камери:

- детектор перекриття об'єктиву;
- детектор засвічування камери;
- детектор переміщення, відхилення камери;
- детектор зміни фону;
- детектор відсутності фокусування.

Також, до трекінгу відносять інтелектуальний пошук в архівах. Це пошук, який допомагає оператору швидко знаходити потрібний матеріал за фактом спрацювання детектора, коли точний час події не відомо.

Особливо важливим це стало для поліції міста та дало можливість:

- Оперативного цілодобового контролю ситуації на вулицях і об’єктах міста в режимі реального часу;
- Ведення відео і аудіоархіву;
- Автоматичне оповіщення про виникнення надзвичайних ситуацій відповідних служб і організацій, надання візуальної інформації з місць установки телекамер;
- Відновлення ходу подій на основі записаних відеоматеріалів;
- Інтеграція відеоінформації з інформацією інших автоматизованих систем міської інфраструктури.

Відеоспостереження сьогодні стало не лише потужним інструментом в сфері безпеки, але також і ефективним рішенням в галузі експлуатації. За чотири десятиліття, з того моменту як відеоспостереження вперше з'явилося на сцені, воно дало нам очі і вуха в тих місцях, де в іншому випадку у нас їх не було. Зараз, завдяки відеоаналітичним додаткам четвертого покоління, відеоспостереження є більш точним, з більш високим рівнем позитивних відгуків, більш інтелектуальним і може застосовуватися для більш широкого кола цілей і об'єктів, ніж будь-коли раніше.

Використані джерела:

1. Еволюція відеоаналітики [Електронний ресурс]. – Режим доступу: https://worldvision.com.ua/ua/articles/evolyutsiya-videoanalitiki
2. Безпечне місто [Електронний ресурс]. – Режим доступу: https://dniprorada.gov.ua/uk/page/-62
3. Інтелектуальна відеоаналітика [Електронний ресурс]. – Режим доступу: https://cutt.ly/vhMYtXh
4. Система інтелектуального відеоаналізу [Електронний ресурс]. – Режим доступу: https://cutt.ly/mhMYulq

Рижкова С.А.
старший викладач кафедри адміністративного права, процесу та адміністративної діяльності Дніпропетровський державний університет внутрішніх справ

ВИКОРИСТАННЯ ЧАТ – БОТІВ У ПРОФІЛАКТИЦІ ПРАВОПОРУШЕНЬ

З розвитком інформаційно-комунікаційних технологій практично всі сфери суспільних відносин інтегрувались в он-лайн комунікацію. В умовах обмежувальних карантинних заходів з метою запобігання поширенню на території України гострої респіраторної хвороби COVID-19, спричиненої коронавірусом SARS-CoV-2, потреби в такій комунікації стали найбільш актуальними та стали невід'ємною частиною повсякденного життя трудової сфери. Комунікаційні функції Інтернет набувають нових форм, які пов'язані з сучасними технічними можливостями. Особливої актуальності останнім часом набули технології комунікацій, засновані на месенджерах і чат-ботах. Месенджери – це програми, які дозволяють передавати повідомлення в реальному часі через Інтернет. Еволюція месенджерів привела до того, що в даний час вони можуть відправляти як текстову інформацію, так аудіо і відео повідомлення. Дослідження показали, що мобільні телефони зараз використовуються для обміну повідомленнями частіше ніж для інших цілей. Тому компанії прагнуть завоювати увагу онлайн-користувачів і створюють чат-боти, щоб вбудуватися в месенджери. Крім того, за даними BI Intelligence, сукупний обсяг користувальницької аудиторії чотирьох провідних месенджерів WhatsApp, WeChat, Messenger, Viber перевищив аудиторію чотирьох найбільших соціальних мереж Facebook, Instagram, Twitter, Linkedin [1].

За статичними даними в Україні понад 70% громадян від 18 до 60 років користуються месенджерами. Найбільшою популярністю у жителів України користуються два месенджера — Viber(56%) і Facebook (41%), за ними з істотним відривом за частотою згадок слідують Телеграм (17%), Skype (14%), WhatsApp (12%) і ряд інших. У віці від 18 до 29 років 95% українців переписуються в призначених для цієї справи додатках. Також використовують месенджери 89% відсотків громадян країни від 30 до 40 років, у віці від 40 до 50 років - 79%. А ось після 50 років українці набагато рідше переписуються, відповідно 50-60-річні українці лише у 57% випадках користуються мессенджерами, і тільки 21% громадян України задіює відповідні додатки віком від 60 і більше років [2].

На підставі вищезазначеного, з огляду на практику використання месенджерів, та впровадження чат-ботів серед користувачів, набуває актуальності використання чат-ботів у протидії та профілактиці правопорушень органами та підрозділами Національної поліції та іншими суб'єктами, уповноваженими вести право просвітницьку діяльність серед населення.

Чат-бот — це спеціальна программа, яка працює в додатках – месенджерах та соціальних мережах. Боти допомагають вирішувати типові задачі: ставлять користувачам питання та відповідають, шукають інформацію, виконують прості

доручення тощо.

Інтеграція суб'єктів, які уповноважені здійснювати повсякденну діяльність з протидії та профілактиці правопорушень серед населення в он-лайн простір за допомогою чат-ботів має певні переваги: можливість цілодобової роботи 24/7; оперативність, користувач отримує відповідь на ситуацію в найкоротший термін; спрощена комунікація тощо.

Зупинимось на деяких позитивних прикладах використання чат–ботів у профілактиці правопорушень. Дуже актуальним та ефективним, особливо в умовах обмежувальних карантинних заходів, є створений МВС України у месенджері Telegram чат-бот #ДійПротиНасильства, який допомагає запобігти домашньому насильству. Окрім правової консультації, що є ознаками домашнього насильства, чат-бот може допомогти викликати служби допомоги (поліцію, швидку медичну допомогу), переадресувати на спеціалістів безоплатної правової допомоги, які нададуть юридичну консультацію в онлайн-режимі. Також чат-бот може надати контакти інших служб допомоги, роз'яснити, що таке домашнє насильство та як йому протидіяти, розповісти про повноваження органів і установ, котрі здійснюють заходи для запобігання домашньому насильству [3].

Ще одним позитивним прикладом у профілактиці правопорушень є впроваджений МВС України, чат-бот #Вибори-2020 для забезпечення прозорого виборчого процесу. Чат-бот #Вибори2020 створено для захисту волевиявлення громадян і реагування на факти порушення виборчого процесу [4].

Слід зазначити, що обмежувальні карантинні заходи вплинули на учасників освітнього процесу. Спілкування учнівської молоді з однолітками частіше відбувається у соціальних мережах та месенджерах. У зв'язку з цим почастішали випадки кібербулінгу серед учнівської молоді.

Кібербулінг – це новітня форма протиправної поведінки, яка виявляється в агресивних, жорстоких діях з метою дошкулити, нашкодити, принизити людину, використовуючи інформаційно-комунікаційні засоби: мобільні телефони, електронну пошту, соціальні мережі тощо. В українській мові поняттям кібербулінгу позначають процес лютого завзятого нападу, який характеризують дієсловами «роз'ятрювати», «задирати», «прискіпуватися», «провокувати», «дошкуляти», «тероризувати», «цькувати» тощо [5, с. 277].

Важливе місце цьому негативному явищу та профілактиці кібербулінгу серед учнівської молоді належить створений Міністерством цифрової трансформації у співпраці з ЮНІСЕФ та за інформаційної підтримки Міністерства освіти і науки України, Координаційного центру з надання правової допомоги та Міністерства юстиції України чат-бот #Кіберпес. Чат-бот #Кіберпес [6], надає певний правовий алгоритм дій, учасникам освітнього процесу щодо протидії проявам кібербулінгу.

Чат-бот у Telegram і Viber допоможе дізнатись, як визначити кібербулінг, як самостійно видалити образливі матеріали з соціальних мереж, а також куди звертатись за допомогою, тощо.

На підставі вищезазначеного, слід визнати, що впровадження чат-ботів суб'єктами які уповноважені здійснювати профілактичні функції у правоохоронній

сфері, є новим інструментом комунікації з населенням, здатним не тільки підвищувати правосвідомість громадян, підвищувати рівень правового виховання серед населення, а також бути дієвим помічником у протидії правопорушенням.

Використані джерела:

1. Ушакова І.О. Підходи до створення інтелектуальних чат-ботів / І.О. Ушакова // Системи обробки інформації. – 2019. – № 2 (157).

2. Понад 70% повнолітніх українців користуються месенджерами URL: https://ua.112.ua/suspilstvo/v-ukraini-ponad-70-povnolitnikh-hromadian-do-60-rokiv-korystuiutsia-messendzheramy-516252.html

3. МВС запустило у Telegram чат-бот для протидії домашньому насильству URL: https://www.ukrinform.ua/rubric-technology/3002636-mvs-zapustilo-u-telegram-catbot-dla-protidii-domasnomu-nasilstvu.html

4. МВС запустило чат-бот «Вибори-2020» для забезпечення прозорого виборчого процесу URL: https://www.kmu.gov.ua/news/mvs-zapustilo-chat-bot-vibori-2020-dlya-zabezpechennya-prozorogo-viborchogo-procesu

5. Кібербулінг в Україні – соціально небезпечне явище чи злочин: визначення та протидія / Т. В. Миронюк, А. К. Запорожець // Юридичний часопис Національної академії внутрішніх справ. - 2018. - № 2. - С. 275-284. - Режим доступу: http://nbuv.gov.ua/UJRN/aymvs_2018_2_25

6. Кіберпес: в Україні розробили чат-бот для боротьби з кібербулінгом. Режим доступу: https://nus.org.ua/news/kiberpes-v-ukrayini-rozrobyly-chat-bot-dlya-borotby-z-kiberbuling

Рижкова С.А.
старший викладач кафедри адміністративного права, процесу та адміністративної діяльності
Романенко П.П.
курсант факультету підготовки фахівців для підрозділів кримінальної поліції
Дніпропетровський державний університет внутрішніх справ

ЗАРУБІЖНИЙ ДОСВІД ВИКРИСТАННЯ ВІРТУАЛЬНОЇ РЕАЛЬНОСТІ ПРИ ПІДГОТОВКИ ПОЛІЦЕЙСЬКИХ

Поліцейський в силу покладених на нього завдань є суб’єктом державно-владних повноважень, що в свою чергу вимагає від нього підвищення свого професійного розвитку, розуміння ступеню відповідальності під час виконання своїх

обов’язків.

Важливе значення в цьому контексті відводиться навчанню та професійній підготовці за різними напрямами діяльності останніх. Актуальним в цьому напрямі є використання та впровадження методів інтерактивного навчання, використання навчально-тренувальних полігонів, інтерактивних кімнат, тощо.

Крім того, з швидким розвитком інноваційних технологій, науковий та практичний інтерес представляє використання віртуальної реальності при підготовці та навчанні поліцейських. Така практика може бути розглянута на прикладі зарубіжних країн.

Справді дуже гарним винаходом, ще до 1900 року був стереоскоп. Чарльз Уітстоун винайшов перші форми стереоскопу у 1838 році, який використовував можливості здібностей мозку поєднувати два слабких та різних зображення в одне, ізолюючи змішану картинку над кожним оком, створюючи трьохвимірний ефект. Відмічається, що стереоскоп, це зовсім не кінець винаходів людства. Досить багато проектів та задумів було реалізовано у реальність, але прорив був помітний у 2007 році. Google запустив програму Street View, яка дозволяє реалістично представляти карти по всьому світу, а в 2010 році в цей сервіс був застосований стереоскопічний 3D-режим. Перегляд вулиць був одним із перших широкомасштабних засобів масової інформації на 360 градусів, і те, що VR стає дедалі більше пов’язаним із поточним ландшафтом галузі [1].

Зазначимо, що під віртуальною реальністю розуміють (VR) – створене комп’ютером тривимірне середовище, з яким може взаємодіяти людина. Якщо говорити простою мовою – завданням окулярів віртуальної реальності є перехитрити мозок таким чином, щоб він сприймав видиме за реальне за допомогою спеціальних технологій [2].

Науковий та практичний інтерес підготовки поліцейських представляє програмне забезпечення Apex Officer (VR-симулятор). Завдяки такому програмному забезпеченню моделюються ситуації, які мали місце в реальному житті (вбивство, грабіж, крадіжка, озброєний напад на поліцейського тощо). Спеціаліст завантажує програму і обирає персонажа з бібліотеки, в яку входять люди всіх рас, віку і статі. Потім він дає їм додаткові пристрої, наприклад, зброю або мобільні телефони, а також встановлює психологічний стан, наприклад, занепокоєння або гіперактивність, яке впливає на їх поведінку (поведінку правопорушника фахівець моделює окремо). Далі визначається місце віртуального світу, де з'явиться персонаж. Це можуть бути вулиці, провулки, школи, будинки, магазини, тощо. Стажер-поліцейський бере відповідну екіпіровку, яка може включати в себе ліхтарик, гвинтівку, електрошокер, рушницю або пістолет. Фахівець грає роль підозрюваного, реагуючи на слова і дії поліцейського.

Програма віртуальної реальності пропонує безліч варіантів для відстеження прогресу у навчанні офіцерів поліції. Їх навчають за допомогою окулярів аби дослідити точність траєкторії польоту кулі, а також відпрацьовуються навички переговорів при деескалації конфліктів з громадянами. Супервайзери стежать за офіцерами, які проходять навчання під час симуляції, використовуючи програмне забезпечення, щоб відстежувати, куди направляються їх погляди, і виявляти будь-

які проблеми [3]

Переваги використання VR-симулятора надають можливість аналізувати та відпрацьовувати всі тактичні прийоми, виробити певні алгоритми дій, завдяки яким є можливість запобігти застосування певних примусових заходів з боку поліцейського, або навпаки допомогти поліцейському зняти психологічні бар'єри, застосування зброї в обстановці, яка склалася. VR-симулятор може бути особливо корисний на тренуваннях, присвячених виявленню не завжди очевидних злочинів, таких як торгівля людьми або сексуальне насильство. За допомогою цієї технології поліцейські в Нью-Йорку тренуються стріляти, а в Чикаго - спілкуватися з аутичними підозрюваними. У Х'юстоні, штат Техас, завдяки спеціальному симулятору поліцейські мають можливість спостерігати, наприклад, як торговець людьми може заманювати жертв. За даними виробника програми Apex Officer, її затосовують 12 поліцейських ділянок в шести штатах.

VR-тренінги для поліцейських обходяться дешевше, ніж постановки з акторами. Apex Officer стягує одноразову плату приблизно в $ 15 тисяч, в той час як Guardian Center, майданчик в Джорджії площею 350 тисяч кв. футів (більше 32 тисяч кв. м), бере близько $ 15 тисяч за курс для 12 осіб. У Міннесоті навчальні центри просять $ 700 за співробітника [4].

Злочинність на території України не має стійкої тенденції до зменшення. Це стосується крадіжок, вбивств, розбійних нападів та ін. На етапі прийняття рішень суду було б доречним впровадити технологію віртуальної реальності. Мова безпосередньо йде про фотографії з місця злочину, відео з відеокамер, відео з машини відеореєстратора. Потрібно аби суддя, присяжні, адвокат, прокурор мали можливість побачити всі докази, які мають відношення до відео у віртуальній реальності аби зануритись у ту подію яка сталася [5].

На підставі вищезазначеного, з урахуванням ефективного досвіду підготовки поліцейських з використанням віртуальної реальності на прикладі зарубіжних країн, вважаємо, це інноваційним проривом в цьому напрямі, яке надає переваги не тільки при підготовці висококваліфікованих поліцейських, а також допомагає набути відповідних навичок поліцейськими, які здатні мінімізувати право на помилку у реальному житті. За такими новаціями майбутнє, такий досвід є корисним в тому числі й при підготовці поліцейських органів та підрозділів Національної поліції.

Використані джерела:

1. Історія віртуальної реальності//URL: https://medium.com/gwaramedia (дата звернення 28.11.2020)
2. Можливості технологій віртуальної реальності в різних сферах//URL: https://www.radiosvoboda.org/a/28903722.html (дата звернення 28.11.2020)
3. Поліція Нью-Йорка використовує VR для навчання//URL: https://mvr.technology/policija-nju-jorka-ispolzuet-vr-dlja-obuchenija/ (дата звернення 29.11.2020)

4. Поліцейські навчаються ловити торговців людьми за допомогою VR-симулятора//URL: https://rb.ru/story/police-vr/ (дата звернення 29.11.2020);

Тренажер виртуальної реальності //URL https://www.apexofficer.com/ Apex Officer; Тренинг по виртуальной реальности готовит будущих сотрудников правоохранительных органов в Вашингтоне //URL https://www.policetechnews.com/post/virtual-reality-training-preparing-future-law-enforcement-officers-in-washington; Обучение сотрудников полиции Аляски виртуальной реальности//URL https://www.policetechnews.com/post/alaska-police-officers-training-in-virtual-realit

5. Як поліція використовує 360 фотографій та віртуальну реальність у кримінальних сценках?//URL: https://www.eyespy360.com/uk-ua/blog/How_Police_Are_Using_360_Photography_and_Virtual_Reality_in_Crime_Scenes.html (дата звернення 29.11.2020)

Богучарова О. І.
професор кафедри юридичної лінгвістики
та практичної психології
доктор психологічних наук, доцент
Костенко К.О., Лусік Я.В. курсанти
Луганський державний університет внутрішніх
справ імені Е.О. Дідоренка

OSINT ЯК ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ДИСТАНЦІЙНОГО НАВЧАННЯ КУРСАНТІВ ЗВО

Абревіатура OSINT (Open Source Intelligence, скор. – OSINT) у міжнародному та національному контексті означає «відкриті джерела» та включає пошук, реєстрацію, облік та отримання оперативної інформації, її аналіз, синтез, адміністрування, а також відслідковування шляхів її розповсюдження, напрацювання системи заходів з безпеки її збереження. Джерелами OSINT можуть бути різні комп'ютерні «продукти», додатки або програми: мас-медіа, онлайн-публікації, блоги, дискусійні групи, інші відео-хостинги, вікі-довідники, YouTube та веб-сайти соціальних медіа (Facebook, Twitter, Instagram), чат-боти тощо. Деякі з цих продуктів вміщують відеоролики, графічну інформацію, складні системи обробки людської мови та є свідченням скоєних правопорушень. Велика кількість та різноманітність відеопродукції OSINT дозволяє використовувати її не лише як джерело, що може свідчити про вчинене правопорушення, а й як зразки навчальної комп'ютерної технології. Актуалізація питання використання OSINT як

універсальної освітньої технології перш за все пов’язана з тим, що в системі вищої поліцейської освіти з’явилися нові предметні цикли і дисципліни, які потребують діалогового, взаємодіючого навчання в умовах дистанційної освіти. Зокрема, курс бакалаврату «Протидія насильству в сім'ї», пропагуючи європейські цінності, тим не менш, є важким для засвоєння, хоча і є складовою правосвідомості сучасного правоохоронця. Зокрема, засвоєння підвалин змісту цього курсу в системі вищої поліцейської освіти має враховувати не тільки те, що специфіка службової діяльності змушує сьогодні працівників правоохоронних органів використовувати з різних джерел інформацію про вчинення кримінальних правопорушень, особливо щодо домашнього насильства, а і необхідність обміну інформацією, спільного вирішення оперативних завдань, комунікації та співробітництва різних підрозділів, а на додаток високого рівня розвитку моральної свідомості. У цьому плані слід зазначити, що окремі навчальні модулі (курси, блоки) навчальної програми курсу «Протидія насильству в сім'ї» мають потужну аналітику моральної складової поведінки жертви та кривдника. Звертаючись до гуманітарних засад поліцейської освіти в частині засвоєння нових дисциплін європейського циклу, підкреслимо, що освітній процес у ЗВО зі специфічними умовами навчання має забезпечувати формування у курсантів не лише теоретичних знань, навичок вирішення практичних завдань, а також компетенцій у сфері долання насильства, прогнозування, фіксації.

Тобто ще у стінах ЗВО курсанти мають зрозуміти, що відбулась «технологізація» оперативного пошуку інформації, а разом з тим йде постійне удосконалення схем скоєння злочинів, у тому числі насильницьких з боку самих злочинців, невпинно зростає анонімність осіб, які вчиняють правопорушення, зокрема й актів насилля. Недарма кривдники опановують технологічні пристрої, які спрямовані на контроль поведінки і підтримку страхів жертви; шифрують свої повідомлення, видаючи себе за іншу особу; діють через проксі-, VPN-сервери, Darknet, які приховують справжню IP-адресу користувача. Іншими словами, трансляція знань про домашнє насильство в освітніх інтеракціях ЗВО вимагає ретельного огляду особливих моделей дій особистості кривдника, пояснення алгоритму його поведінки примусу, тиску й контролювання постраждалої особи, що вміщує в собі дії фізичного, психологічного, економічного сексуального, а останнім часом, навіть, інформаційного характеру на реальних прикладах відеороликів з YouTube, веб-сайтів соціальних медіа (Facebook, Twitter, Instagram). Ураховуючи складні питання викладу подібних практико-орієнтованих курсів з вмістом ціннісно-моральної складової, варто наголосити, що курсанти і курсантки іноді не готові надати чітку моральну оцінку діям кривдника; все ще вважають, що у актах насилля винна сама жертва (45, 6%). Тому під час викладу базових відомостей курсу має ініціюватися активна взаємодія всіх курсантів. Притому наголошувалося, що насильницькі злочини мають дуже високу латентність; їх протоколювання є складною процедурою; законодавча база розслідування цих злочинів, попри те, що напрацьована, але організаційно-розпорядчі процедури виконання приписів і постанов залишають багато питань. Звідти в курсі, з одного боку, важливою є та частина модулів, яка передбачає перевірку практичних навичок, знань і компетенцій (практичні завдання, тести, контрольні запитання тощо), а з іншого, та, яка

спрямована на тестування морально-ціннісного рівня свідомості самих курсантів і курсанток. Як відомо, свого часу О. Негодченко, досліджуючи методологічні основи діяльності поліції щодо побудови інформаційно-аналітичних систем, розглядав ці явища з позиції кібернетики (науки про загальні закони існування інформації) [1, с. 31]. Проте, сьогодні, у наш час заняття, зокрема з курсу «Протидія насильству в сім'ї» мають поєднувати інформаційні й психологічні аспекти аналізу інформації щодо помилок, колізій, казусів досудового розслідування групи насильницьких злочинів на підставі відкритих джерел OSINT.

Результати опитування за методом семантичного диференціалу для розрізнення ставлення до кривдника і фактів насилля продемонстрували позитивну динаміку. Цікаво, що оцінки "легких" ситуацій насилля потрапили у «позитивну» частину спектру. А ось терміни, які описували складні випадки насилля, що найбільш адекватно визначають сутність курсу «Протидія насильству в сім'ї», отримали найнижчі бали та виявилися в «негативній» частині спектру. Отже, OSINT-технології є спеціальна форма, яка успішно забезпечує взаємодію викладача і курсантів ЗВО.

Використані джерела:

1. Негодченко О.В. Завдання та функції штабів органів внутрішніх справ щодо інформаційно-аналітичного забезпечення діяльності органів внутрішніх справ. Наук. вісник Херсон. держ. ун-ту. – 2015. – Вип. 3. – Т 5. – С. 31–35.

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

НОВІТНІ ПІДСИСТЕМИ ІНФОРМАЦІЙНОГО ПОРТАЛУ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

Виконання функціональних обов’язків працівниками Національної поліції можливе лише за умов використання ефективної інформаційної підтримки. Основу інформаційного забезпечення діяльності поліцейських складають відомчі бази даних. З моменту створення Інформаційного порталу Національної поліції він вже налічує біля шести десятків підсистем. Час бурхливого розвитку порталу закінчився і керівництво Національної поліції поставило завдання щодо ефективного використання працівниками Національної поліції усіх підсистем ІПНП. Тому у цій доповіді хочу приділити увагу детальному вивченню можливостей однієї з новітніх підсистем Інформаційного порталу Національної поліції «Точки інтересів».

В інформаційній підсистемі «Точки інтересів» ведеться облік кримінологічно значимих об’єктів (церкви, ломбарди, питні заклади тощо) із застосуванням інтерактивної карти їх розміщення [1].

Ведення цієї підсистеми ІПНП регламентується дорученням НПУ від 29.01.2019 № 137/02/14-2019 «Про віднесення об’єктів транспортної інфраструктури до підсистеми «Точки інтересів» інформаційно-телекомунікаційної системи ІПНП».

Розглянемо роботу з інформаційною підсистемою «Точки інтересів» ІТС ІПНП через мобільний додаток Lis-M [2].

Запускаємо мобільний додаток (рис. 1). Після цього з’явиться запрошення для входу до системи, де працівнику необхідно ввести логін та пароль користувача (рис. 2).

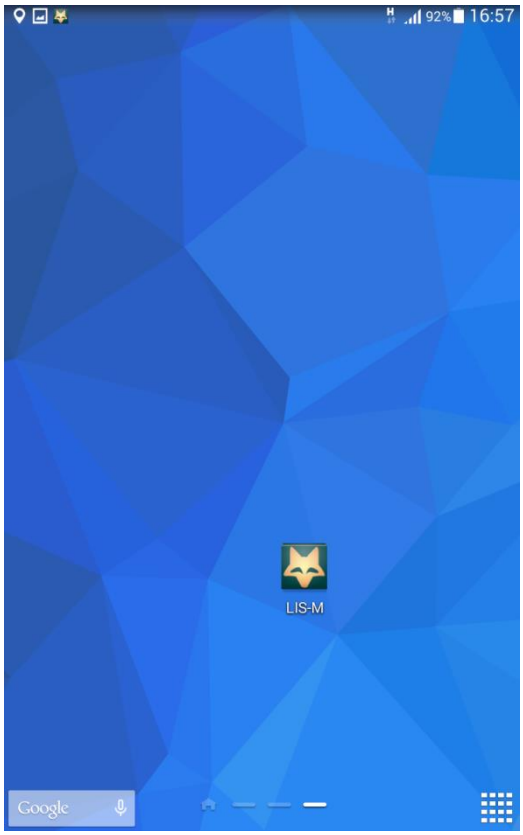


Рис. 1

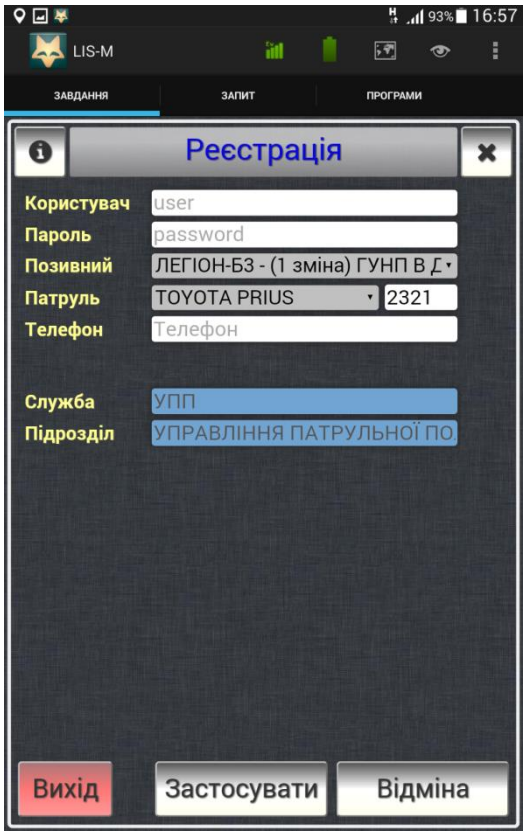


Рис. 2

Після входу до ІТС ІПНП на екрані відкриється вкладка с завданнями користувача (рис.3). Далі переходимо на вкладку «Запит» (рис.4).

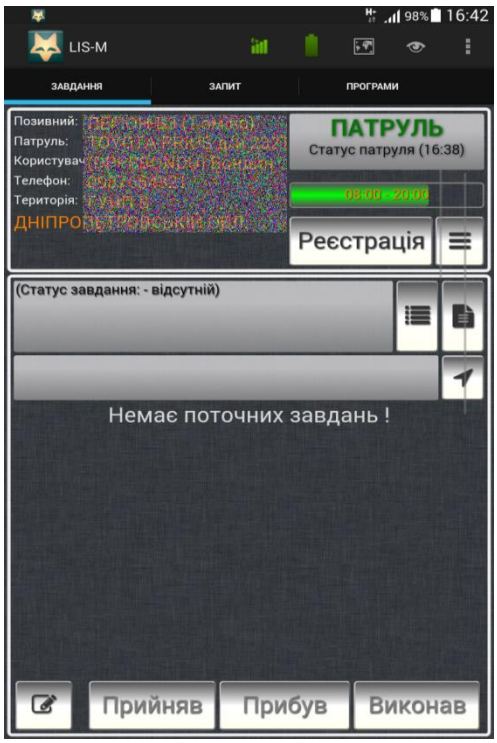


Рис. 3

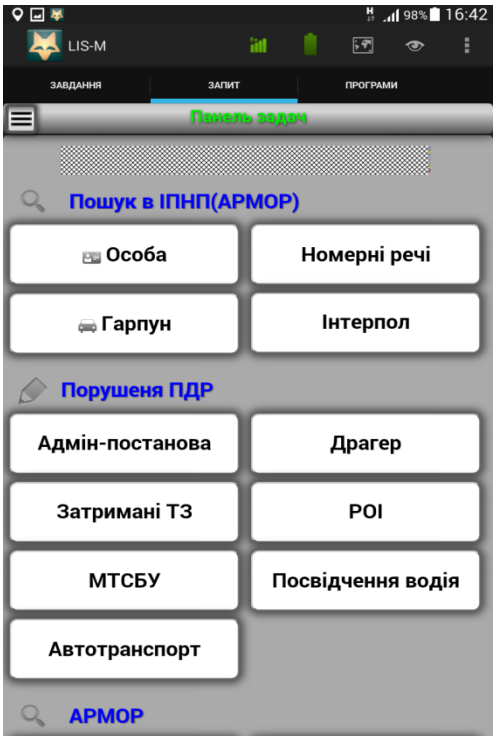


Рис. 4

Для введення та пошуку по ІП «Точки інтересів», треба перейти на панелі задач в «POI» (рис. 4). Далі відкриється меню підсистеми «Точки інтересів» (рис. 5)

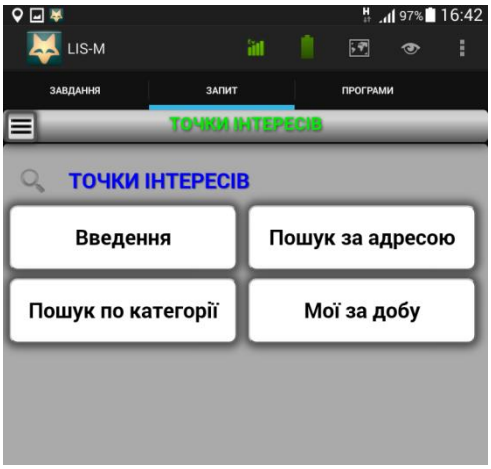
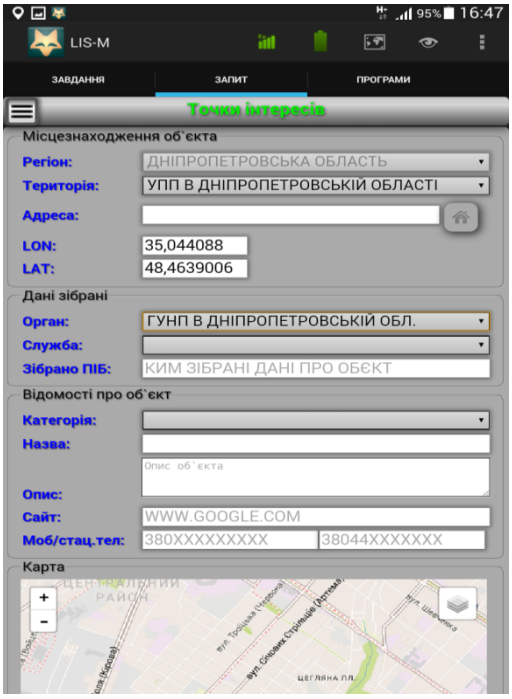


Рис. 5

Для заповнення нової електронної картки натискаємо на «Введення», після чого відкриється картка нової точки з незаповненими полями та картою. (рис. 6, 7). Після заповнення відповідних полів та зазначенням місця знаходження на карті, натискаємо «Зберегти». У разі наявності фотозображення об’єкта передбачено можливість додавання фотозображення до картки «Додати фото».



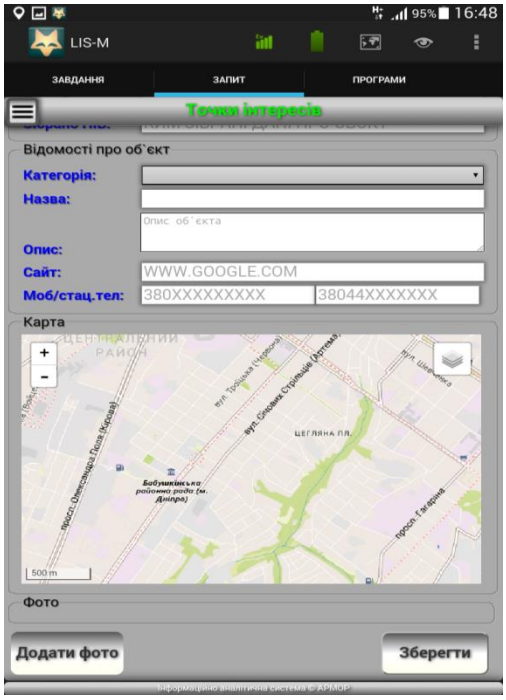
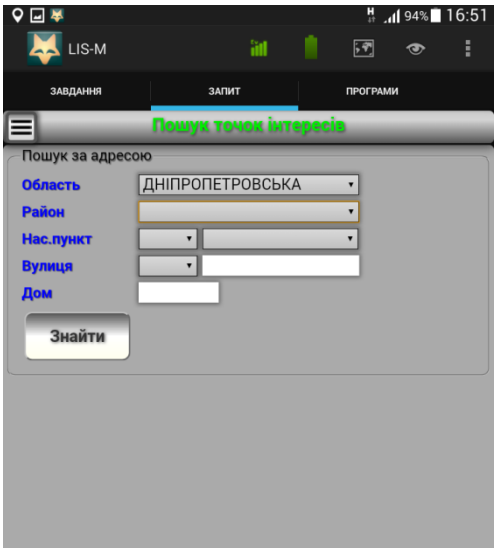


Рис. 6 Рис. 7

Для пошуку за адресою (рис. 8) та по категорії (рис. 9) електронної картки ІП «Точки інтересів» ІТС ІПНП, потрібно вибрати відповідний пункт меню.



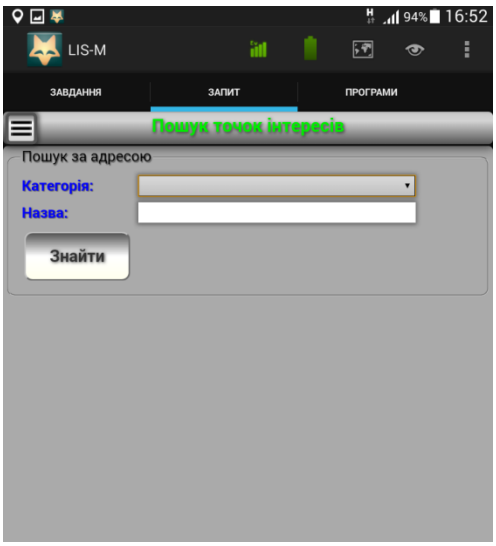


Рис. 8 Рис. 9

Детальне вивчення можливостей підсистеми «Точки інтересів» інформаційно-телекомунікаційної системи Інформаційний портал Національної поліції курсантами, викладачами та практичними працівниками, надасть можливість

більш ефективного використання цього новітнього інформаційного ресурсу в поліцейській діяльності.

Бібліографічні посилання:

1. Доручення НПУ від 29.01.2019 № 137/02/14-2019 «Про віднесення об’єктів транспортної інфраструктури до підсистеми «Точки інтересів» інформаційно-телекомунікаційної системи ІПНП»
2. Інформаційне забезпечення професійної діяльності: навч. посіб. / І.В.Краснобрижий, С.О. Прокопов, Е.В. Рижков – Дніпро : ДДУВС, 2018. – 218 с.

Махницький О. В.
старший викладач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ

МОБІЛЬНІ ДОДАТКИ ДЛЯ БОРОТЬБИ З COVID 19. ЗАРУБІЖНИЙ ДОСВІД

У даній статті представлений огляд додатка eRouška - Part of Smart Quarantine, розробленого урядом Чехії для контролю і попередження поширення COVID19.
eRouška - це офіційний чеський додаток з повідомленнями про вплив, розроблене Міністерством охорони здоров'я і NAKIT (Національним агентством інформаційних і комунікаційних технологій). Для боротьби з епідемією COVID-19, додаток направлено на повідомлення користувачів, які піддаються ризику передачі вірусу. Грунтуючись на історії контактів з іншими потенційно заразними користувачами, додаток дає інструкції, як діяти, щоб мінімізувати поширення епідемії. Однак програма не є діагностичним або медичним інструментом.

У додатку використовується технологія Bluetooth Low Energy , яка зводить до мінімуму споживання енергії, і воно не збирає дані про геолокації , включаючи дані GPS. Додаток розроблено і випущено в повній відповідності з вимогами « Політики API » повідомлень про розкриття інформації, повністю відповідає GDPR і не збирає і не обробляє будь-які особисті дані, які можуть ідентифікувати користувача або його мобільний пристрій, такі як його ім'я, адреса або номер телефону. eRouška може визначити, що два користувача були в контакті, не знаючи, хто ці користувачі і де сталася зустріч.

Що б не перевантажувати огляд технічними термінами не аналізуватимемо вихідний код і обмін додатки з сервером. Практично вся робота відбувається на сервері Google, через сервіси Google Play. Сервер чеського МОЗ задіюється тільки в тому випадку, якщо є позитивний результат тесту на COVID-19.

Використання технології Bluetooth. Система побудована на базі «маяків» BLE (Bluetooth Low Energy Beacon). Спочатку ця технологія проектувалася для захисту предметів від втрати-крадіжки, а також для навігації в приміщеннях. У 2013 році

Apple представила свою технологію iBeacon , а в 2019, з релізом iOS 13, задіяла ці маяки для пошуку пристроїв через Find My . Рік тому ніхто не думав, що ці маяки будуть використовувати для боротьби з вірусом. Bluetooth пристрій при цьому працює в broadcast режимі, передаючи в ефір певні дані. Пристрої, що знаходяться поруч, можуть ці дані прочитати і якось використовувати, в тому числі і передати далі. Ось такими віртуальними рукостисканнями і обмінюються пристрої, відстежуючи контакти з зараженими COVID-19.

Як забезпечується приватність. Звичайно ж, в новому додатку вже немає номера телефону і SMS- ки для активації. Все, що потрібно зробити, це запустити додаток і дозволяти пристрою використовувати API Exposure Notifications . У будь-який момент додаток можна поставити на паузу. Кожен день на пристрої генерується Temporary Exposure Key (TEK) - абсолютно випадковий набір з 16 байт. Але і він не передається в ефір, щоб виключити атаку з перехопленням коду і його емуляцією на іншому пристрої. В ефір передається Rolling Proximity Identifier (RPI). Цей ідентифікатор змінюється кожні 10 хвилин, що робить перехоплення трафіку безглуздим. Спочатку з TEK за допомогою алгоритму HKDF генеруються два ключі, шифрування: RPI Key і AEM Key . Ключем RPI ми шифруємо поточний час, що вимірюється в 10-хвилинних інтервалах. А ключем AEM шифруємо метадані. metadata у цьому процесі поки не використовується і є резервним параметром для майбутніх версій. Далі програма бере поточний час, додає до нього ще кілька байт padding -а і шифрує його нашим RPI ключем. Провести зворотне перетворення з RPI в TEK практично неможливо, теоретично це займе багато мільйонів років навіть з використанням всіх комп'ютерних потужностей на планеті. TEK залишається секретним до того моменту, коли потрібно повідомити про те, що людина заражена COVID19. Після цього, за згодою користувача, його ключ публікується в базі. Ця база зберігається на серверах Google Play і додаток робить запити для її отримання Рис.1:

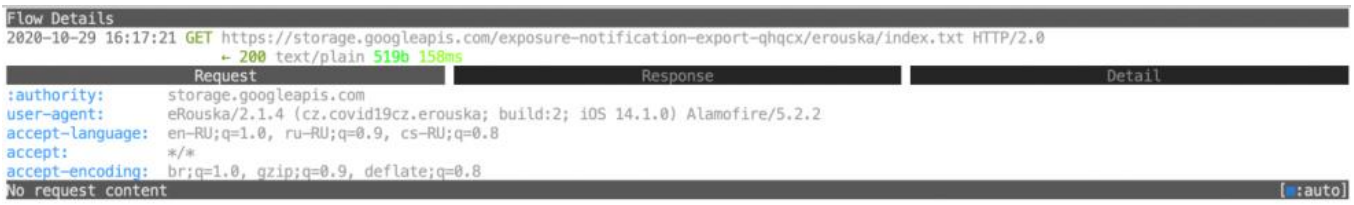


Рис. 1

Ім’я Файлу - це часовий проміжок, рівний однієї доби. Усередині зіп архіву знаходяться два файли: export.bin і export.sig . Перший файл містить protobuf зі структурою, в яку входить трохи службової інформації і, власне, список ключів TEK. Для кожної людини тут буде до 14 ключів, так як мається на увазі, що за 2 тижні до позитивного тесту він міг бути носієм зарази. Аналіз структури показав, що кожен ключ займає 31 байт, тому за розміром файлу можна приблизно прикинути, скільки заражених система виявила за день.

У разі визначення контакту з зараженим виконуються наступні дії. На пристрої у нас є свіжі бази TEK, а також величезна колекція RPI разом з інформацією про рівень сигналу Bluetooth , за яким приблизно можна визначити

відстань. Ці дані, до речі, інтерпретуються так, як вибере МОЗ тієї країни, в якій запроваджено систему. Наприклад, автори програми eRouška стверджують, що в Чехії небезпечним вважається контакт тривалістю більше 15 хвилин на відстані менше, ніж 2 метри. В інших країнах це може бути по-іншому. Перевірка контактів здійснюється виключно в самому додатку і ці дані нікуди не передаються. Додаток просто повідомляє користувачеві про можливий контакт з зараженим . Для перевірки додаток бере все викачані TEK і повторює для них ту ж процедуру, яку я описував в розділі «Як здійснюється приватність». Тобто, ми беремо TEK, час, метадані та заново вважаємо все RPI, які міг передати в ефір телефон зараженого . Далі проста процедура порівняння і фільтрація по часу контакту і відстані.

Користувач ставить додаток і забуває про нього. Все працює в фоновому режимі. До тих пір, поки не виникне дві ситуації:
Система виявила можливий контакт з зараженим. Буде просто попередження від програми. Додаток нікому про це не повідомляє, крім користувача. Далі вже користувач сам вирішує, що йому робити. Він може піти здати тест, може обмежити на час контакти з іншими людьми, може взагалі нічого не робити. Це його соціальна відповідальність.

Користувач з якої-небудь причини здав тест, і він виявився позитивним. У цьому випадку на телефон користувача приходить два SMS повідомлення: про те, що тест позитивний, і код верифікації для додатка eRouška . Далі знову ж рішення за користувачем. Він може просто проігнорувати цей код і нічого за це не буде. Або може опублікувати свої анонімні ключі в базі. Для цього він просто вводить отриманий код в додаток, і воно передає ключі на сервер.

Висновки

Система зроблена дуже грамотно і дійсно забезпечує анонімність. Поставити додаток нескладно, і воно абсолютно ні до чого не зобов'язує. Використання BLE маяків не призводить до істотного витрати батареї. І можливо, комусь буде спокійніше психологічно бачити, що контактів з зараженими не було. Але, з іншого боку, доведеться понервувати, якщо з'ясується, що контакт був.

Згідно з даними Google Play , додаток для Андроїда скачали більше мільйона жителів Чехії. Для iOS таких даних немає. Таким чином, програма встановлена приблизно у 12-15% чехів. Звичайно ж, дуже цікаво, скільки в базі заражених. Отже, в день, коли офіційна статистика говорила про 15664 позитивних тестах, в базу потрапило близько 500 ключів користувачів. З цього складно зробити якийсь висновок, але видно, що далеко не всі користувачі програми публікують свої ключі.

А тепер подивимося на цей додаток з точки зору подвійного призначення. А саме як теоретично можна використовувати цю систему для розслідувань. Ну або як це можуть використовувати «погані хлопці». В системі все добре до тих пір, поки в наших руках не виявилося сам пристрій. Або, ще краще, два пристрої від двох підозрюваних. Наприклад, вони кажуть, що взагалі один одного не знають і ніколи не бачили. Але на пристрої є маса інформації, яка може довести, що це не так. Як відомо, iPhone зберігає внутрішню базу координат, з якої можна визначити місце розташування телефону в певний момент часу. Більш того, наш підозрюваний може ще користуватися фітнес трекера , які визначають навіть кількість кроків. Але GPS координати не так точні, щоб зробити висновок, що люди перебували поруч один з

одним. А ось ті самі RPI, отримані через BLE beacons , скажуть нам, що люди були дуже близько один до одного. Плюс, ми самі можемо визначити, чи були у підозрюваного контакти із зараженими COVID19 , хоча для криміналістики це не така суттєва інформація. Звичайно ж, на всіх сучасних пристроях інформація захищена від несанкціонованого доступу. Але є дуже багато вразливостей, якими успішно користуються як експерти-криміналісти, так і кримінал. Більш того, користувач може сам залишити свій пристрій відкритим, достатньо не встановити на нього пароль доступу. І навіть якщо він стоїть, пристрій може бути вилучено у розлоченому вигляді.

Тому бережіть свої дані. Користуйтеся сучасними пристроями, ставте стійкі паролі, не залишайте розблокувати пристрій без нагляду. Ця рада універсальний і стане в нагоді в будь-якій ситуації.

Мельнікова О.О. кандидат юридичних наук, викладач кафедри кібербезпеки та інформаційного забезпечення факультету підготовки фахівців для підрозділів кримінальної поліції Одеського державного університету внутрішніх справ
Гагауз В.Ф. студент 3 курсу 4 групи факультету №1 ННІПКБ Одеського державного університету внутрішніх справ

ЗАГАЛЬНА ХАРАКТЕРИСТИКА ЗЛОЧИНІВ У СФЕРІ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Стрімкий розвиток інформаційних технологій в Україні, який спостерігається останнє десятиріччя, супроводжується динамічним розвитком злочинів у сфері інформаційних технологій .

«Кіберзлочинність», «хакери», «комп'ютерний злом» – ці терміни вже перестали бути новелою в нас час. На сьогодні кіберзлочини – це одна з динамічних груп суспільно небезпечних посягань. Швидко збільшуються показники поширеності даних злочинів, а також постійно зростає їх суспільна небезпечність [4].

З розвитком технологій стрімко зростає кількість злочинів у цій сфері, а тому з впевненістю можна стверджувати, що саме «кіберзлочини» у XXI столітті є одними з найчисельніших.

Інформаційний злочин(кіберзлочин) — це незаконні дії спрямовані на розкрадання або руйнування інформації в інформаційних системах і мережах, які виходять з корисливих або хуліганських спонукань.

Правове підґрунтя інформаційної безпеки України створюють: Конституція України, Кримінальний кодекс України, закони України "Про основні засади

забезпечення кібербезпеки України", "Про інформацію", "Про захист інформації в інформаційно-телекомунікаційних системах", "Про національну безпеку України" та інші закони, Доктрина інформаційної безпеки України, Конвенція Ради Європи про кіберзлочинність та інші міжнародні договори, згоду на обов'язковість яких надала Верховна Рада України.

Відповідно до Закону України "Про основні засади забезпечення кібербезпеки України" кіберзлочин (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 [2].

Щодо класифікації кіберзлочинів, то в Конвенції Ради Європи про кіберзлочинність, яку Верховна Рада України ратифікувала й імплементувала до українського законодавства починаючи з 11.10.2005, 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 (контентом), що полягає у здійсненні умисних незаконних дій щодо вироблення, пропонування або надання доступу, розповсюдження дитячої порнографії, а також володіння такими файлами у своїй системі. (правопорушення, пов'язані з дитячою порнографією);

• правопорушення, пов'язані з порушенням авторських і суміжних прав [3].

Найпоширеніші види кіберзлочинів

Кардинг – шахрайські операції з кредитними картками (реквізитами кредитних карток), які не погоджені власником картки. Це може бути крадіжка чи незаконне отримання кредитної картки, викопіювання даних картки для подальшого її підроблення, викопіювання реквізитів картки для здійснення покупок через Інтернет без участі власника картки. У будь-якому разі основною метою злочинців є отримання доступу до чужих грошових коштів. Для досягнення цієї мети зловмисники вигадують різноманітні способи отримання потрібної інформації в неуважних і легковірних громадян. Одним із таких способів є фішинг.

Фішинг – шахрайські дії, спрямовані на виманювання реквізитів картки у її власника. Зазвичай власник кредитної картки сам добровільно повідомляє шахраям потрібну інформацію.

Фішинг буває кількох видів:

• *СМС-фішинг*, коли потенційна жертва шахраїв отримує повідомлення про те, що її кредитну картку заблокував банк, а для розблокування необхідно надати реквізити, або ж про те, що власник картки отримав виграш, але потрібно заплатити за його доставку. Варіацій СМС-повідомлень безліч, тому потрібно бути особливо уважними й обачними, якщо ви отримуєте повідомлення.

• *Інтернет-фішинг*, коли шахраї створюють фішингові (підроблені) сторінки, які імітують офіційні сторінки банків, платіжних сервісів, інтернет-магазинів тощо. На жаль, не всі уважно перевіряють назву сайта, уводячи дані кредитної картки, що

на руку кібершахраям.

• *Вішинг* – це майже той самий фішинг, однак виманювання реквізитів картки зловмисники здійснюють за допомогою телефонних дзвінків (шахраї часто представляються працівниками банку й намагаються вивідати у власника картки ПІН-код чи примусити здійснити якісь дії зі своїм рахунком).

• *Скімінг* – копіювання даних платіжної картки за допомогою спеціального пристрою (скімера). Зазвичай відбувається під час здійснення карткових операцій із банкоматами. Для отримання даних злочинці використовують міні-камери або змінні клавіатури.

• *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.

• *Злом* – це умисна дія, спрямована на несанкціоноване проникнення у ПЗ або систему шляхом обходу механізму безпеки, з метою отримання несанкціонованого доступу до певного ПЗ або системи.

• *Протиправний контент* – контент, який пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості й насильства.

• *Рефайлінг* – незаконна підміна телефонного трафіку.

• *Кард-шарінг* – надання незаконного доступу до перегляду супутникового та кабельного TV.

• *Соціальна інженерія* – технологія управління людьми в Інтернет-просторі. [5, с. 361 - 362]

Головними статтями Кримінального кодексу України, за якими розслідуються кіберзлочини в Україні:

- ст. 176 «Порушення авторського права і суміжних прав»;

- ст. 190 «Шахрайство»;

-ст.361 «Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку»;

- ст. 361^{-1} «Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут»;

- ст. 361^{-2} «Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп’ютерів), автоматизованих системах, комп’ютерних мережах або на носіях такої інформації»;

- ст. 362 «Викрадання, привласнення, вимагання комп'ютерної інформації або заволодіння нею шляхом шахрайства чи зловживання службовим становищем»;

- ст. 363 «Порушення правил експлуатації автоматизованих електронно-обчислювальних систем»;

- ст. 363^{1} «Перешкоджання роботі електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку шляхом масового розповсюдження повідомлень електрозв’язку» [1].

Як захистити себе від кіберзлочинів?

Звісно, викладений вище перелік шахрайських дій не є виключним, але, дотримуючись кількох простих правил, можливо суттєво полегшити своє життя, зберігши і нерви, і гроші.

1. Зберігати ПІН-код кредитки, паролі, дані для входу в інтернет-банкінг у надійному місці, найкраще – у власній пам'яті.

2. У жодному разі не повідомляти третім особам паролі й реквізити картки.

3. Бути дуже обережними, здійснюючи інтернет-покупки. Користуватися лише офіційними й перевіреними сайтами.

4. Користуватися банкоматами, розміщеними у відділеннях банків або в місцях із відеонаглядом.

5. Не використовувати неліцензійне програмне забезпечення та не завантажувати його безкоштовно з підозрілих сайтів.

6. Не відкривати підозрілі листа та не переходити за незрозумілими посиланнями.

7. Обов'язково встановити антивірусні програми.

8. Здійснювати резервне копіювання важливих файлів і не надавати доступу стороннім особам до свого комп'ютера та/або телефону.

Указані заходи не убезпечать від усіх можливих загроз, які є в Інтернеті, однак дають змогу значно мінімізувати ризики втрати важливої інформації.

Отже, стрімкий розвиток інформаційних технологій, незважаючи на позитивний вплив на всі сфери людського життя, спричинив неабияке зростання й поширення кіберзлочинів. З упевненістю можна сказати, що кіберзлочини – це одна з основних проблем XXI ст., вирішення якої потребує сучасних методів, активних, рішучих заходів і своєчасного нормативного реагування. Світ живе в еру інформаційних технологій, коли можливості мережі є не лише приємним джерелом можливостей, знань та спілкування, але й джерелом підвищеної небезпеки бути «відкритою книгою», якщо вами зацікавляться певні особи.

Використані джерела:

1. Кримінальний кодекс України: Закон: від 05.04.2001 № 2341-III. Режим доступу : http://zakon2.rada.gov.ua/laws/show/2341-14

2. Закон України «Про основні засади забезпечення кібербезпеки України» від 21.06.2018. Режим доступу : https://zakon.rada.gov.ua/laws/show/2163-19#Text

3. Про ратифікацію Конвенції Ради Європи про кіберзлочинність : Закон України: від 07.09.2005 № 2824-IV. Режим доступу: http:// zakon2.rada.gov.ua/laws/show/2824-15

4. Гриців М. І., В. В. Антощук Узагальнення судової практики розгляду справ про злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), автоматизованих систем та комп’ютерних мереж і мереж електрозв’язку. Офіційний сайт Верховного Суду України. Режим доступу: http://www.scourt.gov.ua/

5. Марків С. І. Кіберзлочинність. Нова кримінальна загроза. Режим доступу: http://gurt.org.ua/articles/34602/ С 361 - 362

Форос Г.В., доцент кафедри кібербезпеки та інформаційного забезпечення, к.ю.н., доцент Одеського державного університету внутрішніх справ
Узюм П.А., курсантка 401 взводу факультету підготовки фахівців для підрозділів кримінальної поліції ОДУВС

ЗАСОБИ ПОШУКУ ІНФОРМАЦІЇ З ВІДКРИТИХ ДЖЕРЕЛ

Сьогодні практично неможливо уявити собі комфортне життя без інноваційних технологій. Ми звикли до того, що в смартфоні та у комп'ютері можна знайти рішення будь-якої проблеми. Там міститься майже все наша життя. Посилки більше не приходять до нас з голубом - їх привозить кур'єр, а оплатити їх можна через термінал, або просто приклавши до них свій смартфон чи розумний годинник. В сучасності існує досить мало систем, які можна назвати надійно захищеними.

Спочатку розглянемо що таке OSINT. Розвідка відкритих джерел (англ. Open source intelligence, OSINT) - концепція, методологія і технологія добування і використання військової, політичної, економічної та іншої інформації з відкритих джерел, без порушення законів. Використовується для прийняття рішень у сфері національної оборони, безпеки, розслідувань тощо[1, С. 81].

У практиці працівника поліції важливо вміти дістати розвіддані, коли мова заходить про збір інформації про людей. Це може бути розслідування зараження і пошук винуватця або ідентифікація особистості для уточнення поверхні атаки.

Зараз розглянемо декілька способів отримання інформації тоді, коли збір з відкритих джерел не дає потрібного результату. Зараз більш 80 відсотків користуються соціальними мережами. До всього іншого більшість людей просто на просто не усвідомлює, що викладає свою інформацію про себе у відкритий джерело доступу, після чого в інтернеті можна знайти особисті дані починаючи від ПІБ, закінчуючи номером карти і де вона проживає. Для пошуку в соціальних мережах потрібно визначитися з інтересами нашого об’єкту і де він вважає за краще проводити час в інтернет-мережі (ВК, Twitter, Instagram, Facebook, навіть Однокласники і багато іншого).

Всім відома сторінка «Вконтакті» пропонує викласти на загальний огляд всі свої дані ще при реєстрації. День народження, місто, номер телефону, місце роботи, інші соцмережі, місце роботи, родинні зв’язки, освіта, захоплення і життєва позиція. Навіть фото з усіх ракурсів.

Розглянемо й інший спосіб пошуку інформації. Не так давно користування сервісу «Telegram» поширився серед людей. У «Telegram» широка функціональність для роботи з ботами. Деякі чат-боти працюють з базами даних і можуть з'ясувати інформацію про номер телефону, знайти контактні дані власника автомобіля по державному номеру транспортного засобу [2]. Всі вони виконують різні функції. Це відбувається за рахунок відмінної роботи ботів з відкритими

базами даних і телефонними довідниками. Застосування подібних програм ще не дуже поширене, але вже створені такі боти, які підключені до баз даних з телефонними номерами. Вони і будуть служити нам помічником з пошуку.

Наприклад, можна скористатися ботом @HowToFind_UA_bot (HowToFind Ukrainian Bot). У ньому можна вибирати зі списку інформацію, яка відома, і бот покаже боти або ресурси, які допоможуть обробити інформацію.

Буває, що ми стикаємося з проблемою, коли про людину зовсім нічого не відомо, окрім фото. Навіть на це знайдеться відповідь. Розробник FindClone надає послуги пошуку схожих зображень, видає у відповіді посилання на сторонні сайти і гарантує, що для пошуку використовувалися тільки «дані, доступні для перегляду необмеженого кола осіб». Найчастіше пошук видає посилання на сторінки ВК.

FindClone - розумний сервіс, який може допомогти знайти вашого двійника всього по одній фотографії. Система ґрунтується на складних операціях: від звичайного розпізнавання осіб до біометричних вимірювань. Дані алгоритми знайдуть копії ваших фотографій, які використовуються Вконтакте для розсилки реклами і спаму. Детальний пошук осіб по фото (Search Face) допоможе відшукати оригінал сторінки користувача, покаже дублікати і просто схожих людей[3].

Авторизуватися в сервісі можна за номером телефону. FindClone безкоштовний перші 30 днів, за цей час сервіс дозволяє перевірити 25 знімків. Після доведеться вибирати платний тариф. З тієї ж аналогії діють FindFace.ru і Findface.me.

Слід зазначити, що люди самі збирають на себе досьє. Вся інформація знаходиться у відкритому доступі та база даних збільшується щодня з кожним новим зареєстрованим користувачем у соцмережі, відповідно до популярності користування мережі Інтернет.

У висновку можна виділити, що одна з найсильніших сторін нашого сучасного розвиненого суспільства є також одним з найголовніших його недоліків. У нинішньому світі розвинені і високотехнологічні соціуми сильно залежать від роботи ряду служб і сервісів, які в даний час стали життєво необхідними.

Використані джерела:

1. Минько О. В. Використання технологій OSINT для отримання розвідувальної інформації / О. В. Минько, О. Ю. Іохов, В. Т. Оленченко, К. В. Власов // Системи управління, навігації та зв'язку., 2016., Вип. 4. -184 с.

2. Бойовий OSINT. Режим доступу: https://xakep.ru/2019/09/06/real-osint (дата звернення: 03.11.2020)

3. Інтернет-новини village. Режим доступу: https://www.the-village.ru/business/news/363567-findclone (дата звернення: 03.11.2020)

Глушаченко В.В.
курсант 2 курсу ФПФОДР Дніпропетровського державного університету внутрішніх справ
Науковий керівник: Рижков Е.В.
завідувач кафедри, кандидат юридичних наук, доцент кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Однією з важливих умов підвищення рівня боротьби зі злочинністю є широке використання сучасних досягнень науково-технічного прогресу, які за останні роки зробили прорив у галузі інформаційних технологій.

Україна посідає 56-те місце у світі за рівнем розвитку інформаційних технологій (2016; Світовий економічний форум у своєму шостому щорічному звіті). У попередньому рейтингу Україна посіла 71 місце. Єдиною конкурентною перевагою, яку наша країна має в цьому аспекті, є традиційно сильний IT-персонал, тобто в Україні дуже високий рівень підготовки програмістів.

Сьогодні важко уявити роботу будь-якого з підрозділів Національної поліції України без інформаційного забезпечення та інформаційного забезпечення, накопичення та систематизації інформації в базах даних. Це явне підтвердження загальновідомої тези "хто володіє інформацією, той володіє світом" [1, 202].

Інформаційне забезпечення органів поліції - це сукупність методів, заходів, засобів різного характеру, які забезпечують створення та функціонування інформаційних технологій, а також їх ефективне використання для вирішення завдань, покладених на міліцію. Інформаційні підсистеми як компоненти систем інформаційного забезпечення призначені для збору, накопичення, зберігання та обробки інформації з певних областей бухгалтерського обліку і орієнтовані на використання в діяльності більшості правоохоронних органів, мають загальний характер і належать до загальних інформаційних систем.

Сучасні інформаційні технології - це сукупність методів, виробничих процесів та програмно-апаратних засобів, інтегрованих для збору, обробки, зберігання, розповсюдження, відтворення та використання інформації в інтересах своїх користувачів.

Типи сучасних інформаційних технологій:

- інформаційні технології обробки даних;
- технологія управління інформацією;

- інформаційні технології для підтримки прийняття рішень;

- інформаційні технології експертних систем [2, 396-397].

Основними тенденціями розвитку інформаційних технологій у правоохоронних органах є: 1) вдосконалення форм і методів управління системами інформаційного забезпечення; 2) централізація та інтеграція комп'ютерних банків даних; 3) впровадження новітніх комп'ютерних інформаційних технологій для ведення кримінологічних та кримінологічних записів; 4) розвиток та широке використання ефективних та потужних комп'ютерних мереж; 5) використання спеціалізованих засобів захисту інформації; 6) встановлення ефективного обміну кримінологічною інформацією на міждержавному рівні. Все це забезпечує значне підвищення рівня контролю за злочинністю [3, 12].

Фахівці в галузі інформаційних технологій спільно з працівниками відділу інформаційного забезпечення Головного управління Національної поліції в Харківській області розробили інноваційний підхід, реалізований на сучасних веб-технологіях у вигляді веб-порталу www.police.kh.ua , що надає можливість поліції взаємодіяти з населенням на абсолютно нових, сучасних принципах, що відповідають європейським вимогам.

Портал забезпечує три групи функцій: 1) інформування громадськості про стан злочинності в регіоні (в даному випадку - в Харківській області), 2) реалізація відгуків громадськості, 3) надання послуг.

Перша група функцій включає наступне:

- відображення на географічній карті району всіх зареєстрованих поліцією злочинів, у тому числі розкритих та нерозкритих, з можливістю вибору: а) одного або декількох видів злочинів; б) обраний район (або райони) Харкова або Харківської області; в) обраний проміжок часу (для останнього дня, тижня, місяця тощо);

- відображення на географічній карті районів концентрації всіх злочинів, зареєстрованих поліцією, з можливістю вибору: а) одного або декількох видів злочинів; б) обраний район (або райони) Харкова або Харківської області; в) обраний проміжок часу (для останнього дня, тижня, місяця тощо);

- відображення на географічній карті області всіх доступних відеокамер з можливістю перегляду в режимі реального часу ситуації в районі, що спостерігається даною відеокамерою (або декількома відеокамерами одночасно);

Ця особливість цікава тим, що дозволяє: спостерігати за розвитком ситуації під час масових заходів у режимі реального часу; зацікавленим особам (наприклад, родичам) спостерігати за ситуацією в режимі реального часу за місцем знаходження спостережуваних осіб (наприклад, дітей чи інших близьких родичів); відображати на географічній карті місцезнаходження всіх дільничних інспекторів з можливістю перегляду їх контактної інформації та районів їх обслуговування (перелік будівель); можливість переглянути список усіх злочинців, які наразі розшукуються, а також зниклих безвісти осіб.

Функції реалізації зворотного зв'язку (інтерактивна взаємодія) включають:

- можливість будь-якого громадянина надіслати в Інтернеті повідомлення про правопорушення, небезпечний предмет тощо з додаванням файлу з фотографією чи

відео описуваної події чи предмета; - можливість оцінити ефективність діяльності поліції в інтерактивному опитуванні (у майбутньому).

Сервісні функції включають одну з найбільш часто використовуваних можливостей замовлення судимості на порталі. У майбутньому розширення службових функцій шляхом додавання модуля оцінки ефективності діяльності поліції за допомогою інтерактивного опитування та розширення функції інформування громадськості шляхом додавання аналітичного модуля для аналізу динаміки злочинності в різних категоріях злочинів у часі [4, 376-377].

З розвитком нових інформаційних технологій посилилась тенденція до використання персонального комп'ютерного обладнання, сфера його застосування розширилася. В результаті спостерігаються позитивні тенденції, серед яких: загальне підвищення рівня комп'ютерної грамотності працівників правоохоронних органів, розширення переліку комп'ютерних інформаційних записів; розширення "географії" використання сучасних засобів обчислювальної техніки у всіх сферах діяльності, розвиток технологій електронної обробки інформації; створення комп'ютерної мережі для обміну інформацією.

У підсумку зазначимо, що інтеграція інформаційних технологій у діяльність Національної поліції України дозволяє вдосконалити механізми управління, забезпечує належне функціонування правоохоронних органів, а саме, швидко отримує доступ до певної інформації, необхідної для виконання своїх обов'язків, аналізує їх , використовувати досягнення науково-технічної думки для оптимізації слідчих дій. Розвиток комп'ютерних технологій дає можливість створювати нові методи роботи, підвищувати професіоналізм кожного працівника правоохоронних органів.

Використані джерела:

1. Танкушина Т. Ю. Автоматизовані інформаційні системи в структурі реєстраційної діяльності поліції: становлення, розвиток, сучасність. – Запоріжжя: Запорізький національний університет, 2011. – Ч. І. – 224 с.

2. Варенко В.М. Інформаційно-аналітична діяльністьї. – К.: Університет «Україна», 2014. – 417 с.

3. Інформаційні технології в правоохоронній діяльності.–К.:НАВСУ,2013. 82с.

4. Узлов Д.Ю., Струков В.М. Про новий підхід до взаємодії поліції з населенням на основі сучасних інформаційних технологій. – Харків, 2016. – 472 с.

Чечель А.О., курсант факультету підготовки
фахівців для органів досудового розслідування
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник: Рижков Е.В.,
завідувач кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
к.ю.н., доцент

ПОШУК ЗНИКЛИХ ДІТЕЙ ЯК ОДИН ІЗ НАПРЯМКІВ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Забезпечення національної безпеки є досить актуальною проблемою, адже у зв'язку зі стрімким процесом реформування та бурхливим розвитком інноваційних технологій інформаційні ресурси, до яких надано доступ лише державним службовцям, знаходяться у відкритому доступі, що негативно впливає на збереження важливої інформації, яка у подальшому використовується не за призначенням та взагалі втрачає свою цінність в роботі правоохоронних органів.

Досить важливу роль у всіх сферах життєдіяльності займають інформаційні технології. Важко уявити сучасне повсякдення без комп'ютерів, смартфонів, телевізорів, тощо. Інноваційні технології не лише урізноманітнили життя людей, але й набагато полегшили їх роботу.

Міністерство внутрішніх справ України не є виключенням з переліку сфер, де інформаційні технології є необхідними для забезпечення ефективної роботи всієї правоохоронної структури. Як зазначалося вище, інформаційні технології перш за все пов'язані з національною безпекою, адже колообіг інформації та даних, які використовуються правоохоронними органами кожного дня має великий об'єм та закритий доступ.

Сьогодні поліції користується низкою інформаційних систем (базами даних), в яких накопляється, обробляється та зберігається інформація.

В правоохоронній системі діє цілий комплекс науково-технічних, довідково-інформаційних, технологічних та нормативних заходів, які мають на меті забезпечити повсякденну роботу всієї правоохоронної системи.

Слід зауважити, що бази даних використовуються поліцією перш за все задля боротьби зі злочинністю. Але не лише пошук та виявлення злочинців входить до завдань поліції. Одним з таких завдань є надання допомоги особам, які цього потребують.

Також, не всі бази даних використовуються задля виявлення злочинців. Досить розповсюдженою проблемою є пошук дітей. В правоохоронній структурі також функціонує інформаційна система «Пошук дітей», яка розшукує дітей в межах від 1000-3000 метрів [1].

Очевидно, що кількість дітей, які зникали почала зростати, та постало питання про необхідність вдосконалення роботи вищезазначеної бази даних. З огляду на таку

проблему, уповноважені представники «Київстар» і Національної поліції України підписали Меморандум про співпрацю, у рамках якого впроваджується спільна соціальна послуга «Пошук дітей».

Завдяки даній співпраці за 2019-2020 роки Національній поліції вдалося розшукати 485 дітей. Специфіка роботи даної послуги полягає в тому, «Київстар» отримує від поліції запит на SMS-розсилку, що містить інформацію про зниклу дитину та місце, де її бачили востаннє, після чого дану розсилку «Київстар» розповсюджує такі повідомлення на номери абонентів, які могли бути свідками зникнення, адже вони користувалися послугами зв'язку (телефонували, писали SMS або користувалися мобільним інтернетом) у радіусі 1–3 км від місця події. [2]. У повідомленні міститься посилання на сайт Міністерства внутрішніх справ України, де знаходиться фотокартка зниклої дитини та її особливі прикмети.

На нашу думку, це досить позитивна співпраця між ПрАТ «Київстар» та представниками Національної поліції України, але слід зауважити, що не всі особи користуються послугами ПрАТ «Київстар», окрім даного тарифу є також ПрАТ «ВФ Україна» та ТОВ «ЛАЙФСЕЛЛ», тобто така співпраця повинна бути з усіма операторами мобільного зв’язку.

У підсумку варто зазначити, що завдяки впровадженню такої співпраці з усіма операторами мобільного зв’язку,а не лише з ПрАТ «Київстар», вдасться не лише збільшити відсоток можливості знайдення дитини, але й залучити якомога більше населення до допомоги правоохоронним органам.

Використані джерела:

1. Аналітично-пошукові функції сучасних інформаційних систем. Можливості використання результатів аналізу в розкритті та розслідуванні злочинів Режим доступу: https://pravo.studio/osnovyi-kriminalistiki/analitichno-poshukovi-funktsijisuchasnih_html (дата звернення: 09.11.2020).

2. Пошук дітей. ПрАТ «Київстар».: веб-сайт. Режим доступу: https://kyivstar.ua/uk/about/responsibility/kidsearch (дата звернення: 09.11.2020).

Грищенко Д. Р.
курсант 1-го курсу Сумської філії
Харківського національного
університету внутрішніх справ

МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ ПРОЗОРОСТІ І ВІДКРИТОСТІ ОРГАНІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ В КОНТЕКСТІ ВПРОВАДЖЕННЯ ЕЛЕКТРОННОГО ВРЯДУВАННЯ

Реформування сучасного інституту державної служби та місцевого самоврядування передбачає відкритість, прозорість, зростання довіри громадян до

органів державної влади, толерантність у відносинах громадян і службовців, поліпшення якості і своєчасність надаваних громадянам публічних послуг.

Публічна політика забезпечує відкритість та прозорість дій влади та можливість громадян впливати на процеси розробки і впровадження державних рішень через електронне врядування. Найважливішою умовою існування демократії є публічність політики, тобто гласність і відкритість будь-якої політичної дії. Громадяни мають право знати про дії та наміри політичних сил, органів державної влади. Вони повинні впливати на процеси створення і реалізації законів, якість роботи державного апарату, рівень освіченості і громадянської самосвідомості політиків, які приймають політичні рішення [1, с. 90-96].

Встановлення зворотного зв'язку з громадськістю, публічного діалогу, партнерських стосунків правоохоронних органів та інститутів громадянського суспільства, громадян, підвищення ефективності механізму залучення громадськості до розроблення та реалізації державної політики – питання першочергової ваги, від яких залежатимуть усі подальші дії влади [2].

Якість нормативно-правової бази та вільний доступ громадян до інформації про діяльність органів державної влади є головними чинниками відкритості. Останнім часом суттєво зросла кількість інформаційних потоків, що циркулюють у суспільстві. Зорієнтуватися у великому об'ємі інформації, визначити і знайти саме ту інформацію, яка потрібна, допомагають централізовані реєстри чинних законів та інших нормативних актів. Такі реєстри запроваджені у країнах Організації економічного співробітництва та розвитку.

Згідно з Концепцією розвитку електронного урядування в Україні, 38 затвердженої Кабінетом Міністрів України 20.09.2017 р. №649-р, «Електронне урядування» - це форма організації державного управління, яка сприяє підвищенню ефективності, прозорості та відкритості діяльності державних органів влади та органів місцевого самоврядування через використання ІКТ з метою формування нового типу держави, орієнтованої на задоволення потреб суспільства [3].

Досить часто електронне урядування державними службовцями й посадовими особами органів місцевого самоврядування на практиці зводиться тільки до електронного спілкування з громадськістю. Однак електронне урядування має сприяти вирішенню тих проблем, які існують у владі: перейти від бюрократизації на електронний документообіг; впровадити електронну форму спілкування з громадянами задля підвищення прозорості та наближення її до потреб і запитів суспільства.

Однією з існуючих проблем щодо надання адміністративних електронних послуг в Україні є недостатній рівень розвитку електронного документообігу в правоохоронних органах .

Недостатньо уваги приділяється підвищенню кваліфікації співробітників органів місцевого самоврядування у питаннях електронного урядування та особливостям функціонування системи електронного документообігу (відповідна робота ведеться тільки у 38% органів публічної влади місцевого рівня [4].

При цьому, до чинників, що ускладнюють впровадження електронного документообігу в поліції належать:

– недосконаліть українського нормативно-правового поля щодо функціонування електронного документообігу;

– неузгодженість і, навіть, відсутність єдиних національних стандартів функціонування систем електронного документообігу, вимог до програмного забезпечення цих систем, а також їх інтеграцію;

- поки що недостатній рівень захисту інформації в системах електронного документообігу правоохоронних органах;

– існування давніх традицій ведення документообігу в паперовій формі.

Подальший розвиток послуг засобами електронного урядування стримується низьким рівнем комп'ютеризації населення, недостатнім рівнем розподілу та проникнення мережі Інтернет, низьким рівнем комп'ютерної грамотності та обізнаності громадян щодо можливостей та переваг отримання послуг в електронному вигляді. Так, відповідно до результатів соціологічного дослідження, тільки половина українців (54,6%) мають комп'ютер, а до мережі Інтернет підключено лише 51% населення держави, а більшість з тих, хто не користується Інтернетом, не відчувають в цьому нагальної потреби [5].

Враховуючи наявне співвідношення кількості власників смартфонів і персональних комп'ютерів, а також існуючу тенденцію інтенсивного зростання кількості користувачів мобільних телефонів в Україні, доволі перспективним є використання мобільного зв'язку, як додаткової можливості надання електронних послуг. Адже мобільний зв'язок є найбільш доступним та поширеним засобом комунікації в країні, а забезпеченість населення України мобільним зв'язком є майже втричі більшою, ніж їх забезпеченість комп'ютерами [5].

Таким чином, можемо зробити висновки, що система електронного урядування не поширена в правоохоронних органах. Однак забезпечення принципів прозорості та відкритості правоохоронних органів в реалізації своїх функцій є важливою запорукою демократизації суспільства й держави. Саме прозорість та відкритість органів її здатність, спроможність і готовність до діалогу з громадянами через засоби електронного звязку значним чином визначають внутрішньополітичну ситуацію і впливають на процеси консолідації суспільства.

Використані джерела:

1. Кохан А. І. Державна комунікативна політика - механізм ефективної діяльності інституту публічної влади в Україні [Електронний ресурс] / А. І. Кохан. – Режим доступу : http://www.academy.gov.ua/ej/ej13/txts/zmist.htm

2. Шпортько О. Поле публічної політики / О. Шпортько // Політ. менеджмент. – 2010. – № 5 (44). – С. 90-96.

3. Про схвалення Концепції розвитку електронного урядування в Україні: Розпорядження Кабінету Міністрів України від 20 вересня 2017 року №649-р [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.

4. 100 міст – крок вперед. Моніторинг впровадження інструментів електронного урядування, як основи надання адміністративних послуг в електронному вигляді [Електронний ресурс]; за. заг. ред. І. С. Куспляк, А. О.

Серенок. – Вінниця : ГО «Подільська агенція регіонального розвитку», 2014. – 86 с. – Режим доступу: http://nc.gov.ua/news/index.php?ID=1577.

5. Сучасний стан, проблеми і перспективи розвитку в Україні електронних адміністративних послуг. [Електронний ресурс]. – Режим доступу: http://www.euroosvita.net/prog/print.php/prog/print.php?id=3808

Трень Т.О. курсант ІІ курсу факультету
підготовки фахівців для органів
досудового розслідування
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник: Рижков Е.В.
завідувач кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ, к.ю.н., доцент

ІНФОРМАЦІЙНА БЕЗПЕКА В ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ

Під інформаційною безпекою слід розуміти стан захищеності національних інтересів України в інформаційній сфері, що визначається сукупністю збалансованих інтересів особистості, суспільства і держави. Досвід останній років показує, що Україна зовсім не готова протидіяти атакам в інформаційній сфері. Водночас застосування інформаційних технологій є вимогами часу, які дозволяють швидко й точно збирати дані, оперативно вирішувати завдання щодо зміцнення правопорядку та законності, а також є запорукою протидії злочинності. Саме необхідністю створення механізмів захисту інформації, що використовуються правоохоронними органами, і зумовлена актуальність дослідження.

Сформулюємо визначення інформаційної безпеки органів внутрішніх справ (далі – ОВС) – це стан інформації щодо діяльності ОВС України, при якому з нею ознайомлені лише суб’єкти, які передбачені чинним законодавством та виключено можливість надходження інформації до третіх осіб [1, с.18]. Тобто інформаційна безпека в органах Національної поліції України має на меті збереження цілісності інформації, що циркулює в поліції, і має деякі особливості. В першу чергу це стосується інформації, що містить державну таємницю. Відзначимо, що державна таємниця – це вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці

України та які визнані державною таємницею та підлягають охороні державою [2, с.7].

Треба сказати, що захист інформації не є основною функцією правоохоронних органів України, тому їхня діяльність не спрямована на забезпечення власної інформаційної безпеки. Така ситуація складається в результаті того, що на сьогодні не існує єдиної системи служб і підрозділів, робота яких була б спрямована на забезпечення такого захисту. Вважаю за необхідне створення такої системи для захисту інформації, що використовується правоохоронними органами при здійсненні покладених на них повноважень, від несанкціонованого доступу та незаконного її використання.

Загалом політика інформаційної безпеки має бути спрямована на мінімізацію та, по можливості, уникнення існуючих чи потенційних внутрішніх або зовнішніх загроз розвитку інформаційно-аналітичного забезпечення ОВС відповідно до її цілей [3, с.9].

Пропонуємо виділити наступні форми гарантування інформаційної безпеки ОВС:

– законодавчий, що включає ухвалення нормативно-правових актів, які встановлюють правила використання й обробки інформації, доступ до якої обмежено, та визначають ступінь відповідальності за порушення цих правил;

– технічний, що полягає у регулюванні доступу до всіх ресурсів інформаційної системи (технічних, програмних, елементів баз даних), регламентації порядку роботи користувачів і персоналу.

Досвід правоохоронних органів інших країн щодо забезпечення інформаційної безпеки дозволяє виокремити два основні напрями. Один із них полягає в удосконаленні діяльності правоохоронних органів щодо гарантування власної інформаційної безпеки зсередини. Інший – у покращенні правового забезпечення інформаційної безпеки на державному рівні.

Треба відзначити, що для досягнення вищого рівня забезпечення інформаційної безпеки правоохоронних органів необхідним є не тільки вдосконалення чинного законодавства, а й наявність механізму його втілення в життя. За такого підходу, на нашу думку, можливо активізувати всі фактори, необхідні для гарантування інформаційної безпеки нашої держави.

До основних принципів органів внутрішніх справ у сфері захисту інформації належать: єдність підходів до забезпечення захисту інформації; комплексність, повнота і безперервність заходів в питаннях захисту інформації; відвертість нормативно-правових актів і нормативних документів з питань захисту інформації, які не містять відомостей, складових державної таємниці; обов’язковість захисту інженерно-технічними засобами інформації, яка складає державну та іншу, передбачену законом, таємницю; конфіденційність інформації, що є власністю держави та відомства.

Отже, треба підсумувати, що аналіз роботи органів та підрозділів Національної поліції свідчить про те, що однією з проблем попередження, виявлення та розкриття злочинів є недостатній рівень захищеності відомчих інформаційних мереж та систем, доступ до інтегрованих інформаційно-пошукових

систем і баз. Тому наразі система захисту інформації потребує вдосконалення.

Використані джерела:

1. Беззубов Д.О. Інформаційна безпека органів внутрішніх справ у системі координаії діяльності правоохоронних структур України // Міліція України: щомісяч. Інформ.-популяр. та наук.-практ. ілюстр. журн. / співзасн. МВС України та Держ. ощад. Банк України. – 2012. - №5/6. – С. 18-19

2. Інформаційна безпека правоохоронних органів: Курс лекцій / О.В. Рибальський, В.Г. Хахановський, Ю.Ю. Орлов та ін.. – К.: Нац. акад. внут. справ, 2004.-148с.

3. Бойченко О.В. Інформаційна безпека в органах внутрішніх справ України (організаційно-правові засади) : монографія / О.В. Бойченко. – Сімферополь: ВАТ «Сімферопольська міська друкарня», 2009. – 288 с.

Дума А. курсант факультету підготовки фахівців для органів досудового розслідування Дніпропетровського державного університету внутрішніх справ
Науковий керівник: Рижков Е.В.
к.ю.н. , доцент, завідувач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ

ІНФОРМАЦІЙНА БЕЗПЕКА НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

Процес інформатизації діяльності територіальних органів поліції України тягне за собою широкі можливості доступу до інформаційних ресурсів, які використовуються в діяльності поліції щодо забезпечення охорони прав і свобод людини, інтересів суспільства і держави, протидії злочинності, підтримання публічної безпеки і порядку. Тому підвищення ефективності діяльності Національна поліція України може бути вирішено через запровадження надійної системи інформаційної безпеки.

О. Красікова вважає, що інформаційну безпеку Національної поліції України можна досягти тільки за двома формами: організована котра полягає в організації роботи поліції пов’язаної з збиранням, обігом, обробкою, зберіганням та використанням інформації та взаємодії працівників; правова форма полягає у створенні інструкцій та положень, складання планів чи навіть виданні розпоряджень та наказів [1, с. 20].

Тому можна стверджувати, що інформаційна безпека Національної поліції

України полягає у її спроможності забезпечити інформаційні ресурси від несанкціонованого доступу до них.

На даний час основним напрямом протидії витоку інформації є забезпечення фізичного (технічні засоби, лінії зв'язку, персонал) та логічного (операційна система, прикладні програми, дані) захисту інформаційних ресурсів органів поліції України. При цьому безпека досягається завдяки використанню апаратних, програмних та криптографічних методів та засобів захисту, а також комплексом організаційних заходів.

Але незважаючи на значні результати в області інформатизації та запровадження новітніх інформаційних технологій в діяльність поліції кінцева ефективність забезпечення інформаційної безпеки не завжди відповідає сучасним вимогам [2]. Сучасні системи безпеки мають високі характеристики тільки по окремим напрямам забезпечення безпеки. Прямолінійне вирішення даної проблеми шляхом створення на кожну інформаційну систему власної системи безпеки не є ефективним та не забезпечує можливості практичної реалізації на всіх рівнях, а саме: фінансові обмеження, складність в експлуатації та координації дій. Логічним виходом з цієї ситуації є інтеграція окремих інформаційних систем та систем безпеки [3, с. 102].

У сфері інформаційної безпеки України вирізняються такі життєво важливі інтереси держави: недопущення інформаційної залежності та блокади України, інформаційної експансії з боку інших держав та міжнародних структур; ефективне функціонування механізму взаємодії органів державної влади та інститутів громадянського суспільства при виробленні, реалізації та коригуванні державної політики в інформаційній сфері; побудова та розвиток інформаційного суспільства як необхідної передумови конкурентоспроможності України в сучасному світі; забезпечення економічного та науково-технологічного розвитку України; формування позитивного іміджу України; організація системи захисту прав громадян на вільний і безперешкодний доступ до інформації, залучення їх формування системи інформаційної безпеки; інтеграція України у світовий інформаційний простір.

Тому розглянувши основні чинники котрі впливають на інформаційну безпеку Національної поліції України, ми сформували основні положення котра на нашу думку будуть доцільними: законодавчий чинник полягає в ухваленні нормативно-правових актів, за допомогою котрих можна встановити правила використання й обробки інформації, доступ до якої обмежено, та визначають ступінь відповідальності за порушення цих правил; технічний чинник допомагає регулювати доступ до всіх ресурсів інформаційної системи, а саме: технічної, програмної, елементів баз даних), регламентація порядку роботи користувачів і персоналу.

Таким чином, система інформаційної безпеки має бути спрямована на запобігання втрати інформації, її перекручення, несанкціонованого доступу та незаконного її використання під час проектування, впровадження та експлуатації інформаційних підсистем. Безпека та захист в інформаційних системах Національної поліції має будуватись з урахуванням комплексного підходу до побудови системи захисту, що передбачає об'єднання в єдиний комплекс необхідних

заходів та засобів захисту інформації на всіх рівнях системи інформаційного забезпечення.

Використані джерела:

1. Красіков Д.О. Правове забезпечення інформаційної безпеки в діяльності органів внутрішніх справ України: автореф. дис. ... канд. юрид. наук: 12.00.19 К., 2019. 20 с.

2. Іванець Т.М. Інформаційев безпека держави як умова для збереження національного суверенітету. [Електронний ресурс]. – Режим доступу: http://intkonf.org/ivanets-tm-informatsiyna-bezpeka-derzhavi-yak-umova-dlya-zberezhennyanatsionalnogo-suverenitetu/ (дата звернення: 12.11.2020).

3.Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 рр.: Закон України № 537V від 9 січня 2007 р. *Відомості Верховної Ради України*. 2007. № 12. Ст. 102.

Філімонов В.О. курсант 2 курсу ФПФОДР Дніпропетровського державного університету внутрішніх справ
Науковий керівник: Рижков Е.В.
завідувач кафедри, кандидат юридичних наук, доцент кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ

ВИЗНАЧЕННЯ МІСЦЕЗНАХОДЖЕННЯ ЧЕРЕЗ ГЕОІНФОРМАЦІЙНУ СИСТЕМУ

У даній роботі розглянуто поняття та сутність геоінформаційної системи, її структура та основні функції, можливості її вдосконалення шляхом прийняття певних законів та нормативно-правових актів, що будуть слугувати регулятором взаємовідносин між громадянами, їх власністю кіберполіцією України.

Сьогодні важко уявити роботу будь-якого з підрозділів Національної поліції України без інформаційного забезпечення та інформаційного забезпечення, накопичення та систематизації інформації в базах даних. Це явне підтвердження загальновідомої тези "хто володіє інформацією, той володіє світом" .

Необхідним заходом управління є наявність вичерпної, цілком достовірної, позбавленої суб'єктивних (неточних повністю та офіційно не підтверджених) слоїв інформації, яка необхідна для виконання певної конкретної задачі та допускає прийняття відповідного, добре продуманого управлінського рішення. Ця інформація повинна відображати не тільки реальний стан справ, але й тенденції,

масштаби та очікувані наслідки розвитку життєвих процесів з коротко- та довгостроковою перспективою [1, с.74].

Для України, яка перебуває на стадії всебічного розвитку соціальних мереж, інформаційних технологій, питання формування інформаційно-аналітичної бази для прийняття управлінських рішень є особливо актуальним. Тому об'єктивною вимогою є повне використання сучасних інформаційних технологій. Стратегія інформаційно-аналітичного забезпечення має полягати у формуванні єдиної системи збору, обробки, зберігання та передачі інформації в цій галузі, яку буде затверджено на державному, законодавчому рівні. ГІС має слугувати для пошуку людей як сервіс, з використанням якого користувач сервісу має можливість знайти людину, яка знаходиться поряд з нею на карті, та розпочати спілкування. Сучасні інформаційні технології - це сукупність методів, виробничих процесів та програмно-апаратних засобів, інтегрованих для збору, обробки, зберігання, розповсюдження, відтворення та використання інформації в інтересах своїх користувачів [2].

Сама геоінформаційна система (ГІС) являє собою найсучаснішу комп'ютерну технологію, яка дозволяє поєднувати модельне зображення території (електронне відображення карт, діаграм, простору, повітряних зображень земної поверхні) з інформацією табличного типу (різні статистичні дані, списки, економічні показники, тощо). Також під геоінформаційною системою розуміють систему управління просторовими даними та пов'язані з ними атрибути. Більш конкретно, це комп'ютерна система, яка дозволяє використовувати, зберігати, редагувати, аналізувати та відображати географічні дані. Вона призначена для збору, зберігання, модифікації, управління, аналізу та відображення всіх форм географічної інформації. ГІС використовується багатьма дослідниками в галузі екологічних проблем для виявлення різних показників в географічній сітці. За територіальним поділом ГІС поділяються на глобальні ГІС, субконтинентальні ГІС, національні ГІС частіше мають статус державних, регіональних ГІС, субрегіональних ГІС та локальних або місцевих ГІС. [3, с.172]

Для правильного функціонування геоінформаційної системи на території України недостатньо створити певну кількість нормативно правових актів та законів. Необхідно встановити їх таким чином, щоб вони усі нормально функціонували, та щоб один не перекривав своїми функціями (також існуванням) інші. Лише тоді вони зможуть діяти безпосередньо один від одного та на користь кіберполіції України.

Отже, зробимо висновок: головним пріоритетом для розвитку є розробка алгоритму подання інформації про користувачів. Використовуючи маркери, які є на карті, а саме тоді, коли користувач натискає на маркер, що вказує на конкретну людину, він отримає графічну та текстову інформацію про цю особу. Ця інформація дозволяє отримати доступ та записати профіль користувача. Наявність цієї інформації на маркері значно полегшує та пришвидшує процес спілкування між користувачів, що є перевагою перед аналогічними сервісами. Користувач також має можливість написати повідомлення на стіну, яке можуть бачити всі користувачі цієї послуги; ця особливість дозволяє відстежувати активність користувачів

Використані джерела:

1. Рифонова Т. А. Геоинформационные системы и дистанционное зондирование в экологических исследованиях / Т. А. Трифонова, Н. В. Мищенко, А. Н. Краснощеков. – Східна наука, № 4, 2017. - с. 74
2. Інформаційне забезпечення професійної діяльності : навч. посіб. / І.В. Краснобрижий, С.О. Прокопов, Е.В. Рижков – Дніпро : ДДУВС, 2018. – 218 с.
3. Бусигін Б.С, Гаркуша І.М., Середінін Е. С., Гаевенко А. Ю. Інструментарій геоінформаційних систем: довідковий посібник. – К.: ІРГ "СБ", 2000. – 172 с.

Пяничук М.С. курсант ІІІ курсу ФПФОДР,
Дніпропетровський державний
університет внутрішніх справ
Науковий керівник: Гребенюк А.М., доцент
кафедри економічної та інформаційної безпеки
к.т.н., доцент Дніпропетровського державного
університету внутрішніх справ,

ЗАКОРДОННИЙ ДОСВІД ЗАСТОСУВАННЯ НОВІТНІХ ТЕХНОЛОГІЙ В ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ

Наразі у світі відбувається велика кількість, можна навіть назвати це «вибухом», нових технологічних відкриттів, метою яких, безумовно, є побудова «розумного», «цифрового» суспільства і держави. У сучасному світі навряд чи залишилася хоч одна сфера людської діяльності, в яку цифрові технології не принесли кардинальних змін. Так само, не менш важливим буде застосування новітніх технологій у діяльності поліції. Цифрова трансформація відкриває нам нові можливості в поліцейській діяльності, а саме аналіз величезних масивів даних, підвищення внутрішньої ефективності системи та прискорення її роботи. Саме такі властивості цифрових технологій можуть запропонувати працівникам поліції нові інструменти впливу у протидії злочинності та підвищить якість їх роботи.

Варто розглянути це питання в аспекті аналізування досвіду зарубіжних країн, щодо впровадження нових технологій для допомоги в роботі правоохоронних органів. І так, середньорічний темп зростання загальносвітових витрат правоохоронних органів на програмні засоби та обладнання становить 9,3%. У 2018 році фінансування оцінили в $ 11,6 млрд, за 2020 рік витрачено вже понад $ 13,6 млрд, а до 2023 року, за підрахунками аналітичної компанії Markets and Markets, бюджет збільшиться до $ 18,1 млрд. Гроші витрачаються не тільки на зброю і засоби захисту, але і на високоточні інформаційні технології.[1]

Інновації наразі впроваджують по всьому світу, щоб швидше знаходити і

затримувати порушників. Ось, наприклад, у Китаї з'явилось одне із найновітніших винаходів - так зване «всевидюче око». У березні 2018 року поліцейські з Пекіна почали тестувати «розумні» окуляри для розпізнавання осіб і автомобільних номерів. Використання таких окулярів в Китаї почалося ще в лютому. Гаджет, розроблений компанією LLVision Technology, вперше протестували в китайській провінції Хенань. За допомогою «розумних» окулярів поліцейські з Хенаня затримали 7 підозрюваних і виявили 26 випадків підробки документів менш ніж за тиждень.[2] Китайська влада також сприяє розвитку технологій на основі біометричних даних для виявлення злочинців. З 2017 року Китаї збирають зразки голосів громадян і відбитки їхніх пальців для створення бази даних.

Однак інноваційність зарубіжної поліції цим не обмежується. Раніше ніхто навіть і подумати не міг, що поліцейських зможуть замінити роботи, але в Дубаї запустили роботу залізних поліцейських. Ще у березні 2018 року в аеропорту з'явився робот-митник, який здатний розпізнавати обличчя і відправляти попередження про підозрілих пасажирів. Він оснащений системами теплового і рентгенівського сканування, тому може відразу перевіряти вміст багажу.

Поліція Дубая вже прийняла в штат робота-поліцейського для патрулювання торгового центру. Робот ідентифікує підозрюваних і передає відеозаписи в поліцейську дільницю, а громадяни можуть повідомити про порушення через сенсорний екран на його грудях. До 2030 року влада ОАЕ планує замінити чверть поліцейського складу на роботів. [2]

Крім того, досить розповсюдженою є практика патрулювання на вулицях міст самоврядних дронів. Згідно даних звіту за березень 2020 року дослідницького центру з вивчення дронів Бард-коледжу близько 102 країни використовують БПЛА. Вони оснащені камерою з 360-градусним кутом огляду і здатні виявляти правопорушення та розпізнавати людей, що знаходяться в розшуку. А в США Amazon оформила патент на мініатюрні дрони, які отримали назву UAVA (Unmanned Aerial Vehicle Assistant), що перекладається як «безпілотний літальний апарат-асистент». За командою «злетіти» дрон підіймається в повітря для виконання команд, оснащений відеокамерою. Він зможе зазирнути туди, куди живому співробітнику заходити небезпечно, і тим самим позбавить поліцейських від невиправданого ризику.[3] Дрони також борються з браконьєрами і контрабандистами.

Але і в Україні з такими технологіями не баряться, так як українські поліцейські також використовують у своїй діяльності дрони. На озброєнні ЗСУ (завдяки співпраці з Туреччиною) знаходяться 6 ударних безпілотників. Втім, літали вони поки тільки на полігонах. Ангар ударних БПЛА в Україні невеликий, хоча потенціал у цій галузі є. Десятки українських операторів, техніків та інших фахівців на Bayraktar TB2 пройшли курс навчання у турецьких фахівців. Наразі Україна хоче придбати ще 48 безпілотників Bayraktar TB2, і локалізувати їх виробництво в Україні. [4]

Використання новітніх інформаційних технологій являє собою ідеальне поєднання використання актуальної інформації та сучасного програмного забезпечення, а також можливість скоординованого патрулювання території та

покращення діяльності, пов’язаної з попередженням та розкриттям злочинів.

Враховуючи вищенаведені факти ефективного використання інформаційних технологій в діяльності поліції зарубіжних країн, варто зазначити, що використання новітніх перспективних технологій значно поліпшить рівень роботи поліцейських щодо розкриття та попередження злочинів. Також не варто забувати, що необхідною умовою для підвищення дієвості поліції завжди буде залишатись якісна підготовка фахівців і підвищення кваліфікації співробітників Національної поліції України по профілях, пов'язаних з системним аналізом і автоматизованими системами.

Використані джерела:

1. Дрони та роботи [Електронний ресурс]. – Режим доступу: https://cutt.ly/bhjlvYC

2. Новітні полицейскі технології [Електронний ресурс]. – Режим доступу: https://cutt.ly/xhjlbPd

3. Якою виявиться поліція майбутнього [Електронний ресурс]. – Режим доступу: https://cutt.ly/AhjlnOA

4. Ударні безпілотники стали модною смертоносною зброєю: чи готові ВСУ до сучасної війні [Електронний ресурс]. – Режим доступу: https://cutt.ly/8hjlmhW

Голубєва Д. В. студентка І курсу
Дніпропетровський державний
університет внутрішніх справ
Науковий керівник: Гребенюк А.М.,
доцент кафедри економічної
та інформаційної безпеки к.т.н., доцент
Дніпропетровського державного
університету внутрішніх справ

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ПРАВООХОРОННІЙ ТА ЮРИДИЧНІЙ ДІЯЛЬНОСТІ

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.

В умовах сучасного світу інформація є найціннішим ресурсом людини. Економічний потенціал суспільства переважно визначається обсягом інформаційних ресурсів та рівнем розвитку інформаційної інфраструктури.

На сьогодні дуже складно уявити роботу будь-якого підрозділу Національної поліції України без інформаційної підтримки та інформаційного забезпечення.

Інформаційне забезпечення органів поліції – це комплекс методів та прийомів, заходів, які забезпечують функціонування інформаційних технологій і їх використання задля вирішення поліцейських питань [1, 2].

Основними тенденціями розвитку інформаційних технологій у правоохоронній сфері є:

1) удосконалення форм та методів управління системами інформаційного забезпечення;

2) централізація та інтеграція комп'ютерних банків даних;

3) впровадження новітніх комп'ютерних інформаційних технологій для ведення кримінологічних та криміналістичних обліків;

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

5) застосування спеціалізованих засобів захисту інформації;

6) налагодження ефективного взаємообміну кримінологічною інформацією на міждержавному рівні.

На теперішній час важливими проблемами, що постають перед правоохоронними органами, є:

- вдосконалення нормативно-правової бази;
- покращення організаційно-кадрового забезпечення, яке потребує докорінного вдосконалення;
- оснащення та переоснащення всіх галузевих підрозділів сучасною потужною комп'ютерною технікою, ліцензійним стандартним та прикладним програмним забезпеченням, а також реалізація заходів зі створення єдиної комп'ютерної мережі ОВС України;
- обмін інформацією між інтегрованими банками даних різних рівнів і забезпечення постійного зв'язку між ними, уніфікація технологічних процедур обробки документів, збору, реєстрації, накопичення й обробки інформації, що надходить у кожен з банків даних;
- вдосконалення роботи інформаційних систем та інтеграції в єдине інформаційне середовище на державному та міжнародному рівнях, що покращить рівень відповідної внутрішньої та зовнішньої;
- створення та розробка дієвої системи інформаційної безпеки ОВС, яка б визначила загальні положення, основні поняття, цілі, принципи й напрями запровадження та підтримку надійної системи інформаційної безпеки правоохоронних органів України.

Сучасні інформаційні технології – це сукупність методів, виробничих процесів і програмно-технічних засобів, інтегрованих з метою збирання, обробки, зберігання, розповсюдження, відтворення і використання інформації в інтересах її користувачів [3, 4].

Види сучасних інформаційних технологій:

- інформаційна технологія опрацювання даних;
- інформаційна технологія керування;
- інформаційна технологія підтримки прийняття рішень;
- інформаційна технологія експертних систем.

Зважаючи на умови сьогодення, для вирішення проблеми вдосконалення інформаційного забезпечення, треба внести певні зміни, уточнення та доповнення у основні завдання системи інформаційного забезпечення правоохоронних органів України – запорука підвищення ефективності діяльності ОВС щодо забезпечення правопорядку та прав і свобод громадянина [4].

Отже можна зробити *висновок*, що проблема вдосконалення інформаційного забезпечення діяльності правоохоронних органів України є багатогранною та потребує комплексного підходу до її вирішення: від нормативно-правових аспектів до матеріально-технічного та кадрового забезпечення.

Використані джерела:

1. Системна інформатизація правоохоронної діяльності: Монографія / М. Швець, В. Бур-жинський, Б. Раціборинський та ін.; За ред. В. Дурдинця, В. Євдокимова, М. Швеця; 2006. – 287 с.
2. Варенко В.М. Інформаційно-аналітична діяльність: Навч. посіб. / В. М. Варенко. – К.: Університет «Україна», 2014. – 417 с.
3. Інформаційні технології в правоохоронній діяльності : Посібник / В.А Кудінов., В.М.Смаглюк, Ю.І. Ігнатушко, Іщенко В.А. – К.: НАВС, 2013. – 82с.
4. Бойченко О.В. Герасименко К.С. Концепція інформаційної безпеки в системі інформаційного забезпечення ОВС України // Вісник Запорізького юридичного інституту. Дніпропетровського Державного університету внутрішніх справ. – 2010. – № 2. – С. 54-62.

Тарантюк А.Р. студентка юридичного факультету Дніпропетровського державного університету внутрішніх справ

Науковий керівник: Тютченко С.М.
старший викладач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ

ТЕОРЕТИЧНІ ЗАСАДИ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ ДІЯЛЬНОСТІ

На сьогоднішній день існує декілька трактувань визначення поняття «інформаційно-аналітичної діяльності». Деякі науковці вважають, що це є сфера діяльності. Інші вважають, що інформаційно-аналітична діяльність – це збір та переробка інформації, яка необхідна для якісного керівництва та управління. Існує визначення, що інформаційно- аналітична робота – це збір по суті застарілої інформації, яка згодом переходить до нової якості та використовується на сучасному

етапі [1].

Як і будь-яка діяльність, інформаційно-аналітична має свої цілі, які поділяються на стратегічні та тактичні. Стратегічною ціллю можна назвати метод збору та обробки інформації з метою надання замовнику необхідного якісного інформаційного продукту. Тактичною ціллю можна назвати питання та завдання, які ставляться замовником.

До об'єктів інформаційно-аналітичної діяльності можна віднести наступні: бази даних; апаратні засоби; інформаційно-аналітичні продукти; офісне, мережеве устаткування; засоби комунікації; програмні засоби; системне, мережеве програмне забезпечення [2].

До суб'єктів інформаційно-аналітичної діяльності відносяться, в першу чергу, особистість та держава, потім - виробники інформації, виробники вторинної інформації, виробники технічних засобів обробки інформації.

Засобами інформаційно-аналітичної діяльності є технічні та інтелектуальні засоби, які забезпечують виконання даного завдання. Інтелектуальні засоби інформаційно-аналітичної діяльності включають в себе відомості або факти, що забезпечуються можливістю зберігання та обробки інформації. Технічні засоби містять каталоги, інформаційні системи та системи обслуговування.

Завдання інформаційно-аналітичної діяльності складаються з моніторингу стану об'єкта управління; контролю за дотриманням рішень; аналізу зовнішніх та внутрішніх ситуацій, які впливають на їх розвиток [3].

Принципи інформаційно-аналітичної роботи включають в себе: визначення мети дослідження; розгляд понятійного апарату; розкриття фактів; забезпечення достовірності інформації.

Отже, з теоретичних положень та визначень можна зробити висновок, що інформаційно-аналітична діяльність є найважливішою складовою професійних зобов'язань персоналу підприємств та є базою для прийняття стратегічних управлінських рішень.

Використані джерела:

1. Варенко В. М. Інформаційно-аналітична діяльність. Навч. посіб. К.: Університет «Україна». 2014. 417 с.

2. Захарова І.В., Філіпова Л.Я. Основи інформаційно-аналітичної діяльності. Навч.пос. К. : "Центр учбової літератури".2013. 335 с.

3. Ященко Л.Є. Роль та місце етапу збору документів та фактів у проведенні інформаційно-аналітичного дослідження. Інформаційна освіта та професійно-комунікативні технології XX1 століття. 5-а Міжн. наук.-практ. конф.Одеса. 2012. С.26-29

Штундер В.Є. Студентка 2 курсу юридичного факультету Дніпропетровського державного університету внутрішніх справ
Науковий керівник: Тютченко С.М.
старший викладач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ

ВДОСКОНАЛЕННЯ СИСТЕМИ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ПРАВООХОРОННИХ ОРГАНІВ

Останнім часом в Україні спостерігається інтенсивне впровадження сучасних інформаційних технологій практично у всі сфери життєдіяльності держави. Особливо актуально це питання постає в діяльності Національної поліції, де широко створюються, впроваджуються та успішно використовуються у боротьбі зі злочинністю міжвідомчі банки даних та інші комп'ютеризовані системи.

Юридична діяльність - це вид соціальної діяльності, який здійснюють юристи з використанням юридичних засобів, дотримуються в установлених законом випадках юридичної форми з метою розв'язання різних юридичних проблем. Правоохоронна діяльність, на нашу думку, є самостійним видом юридичної діяльності, спрямованим на припинення порушення, захист та охорону порушених прав, свобод та інтересів громадян [1].

Основи інформаційного забезпечення правоохоронних органів України сформувалися на початку 70-х років минулого століття. У цей період стали використовувати накопичений в нашій державі досвід застосування електронно-обчислювальних машин для вирішення завдань управління.

Метою інформаційно-аналітичного забезпечення державних органів виконавчої влади є створення умов для прийняття ефективних державних управлінських рішень.

Варто відзначити, що створенню єдиної бази даних, яка б містила усю необхідну інформацію для реалізацією правоохоронними органами своїх функцій перешкоджали наступні фактори: по-перше, це слабка технічна оснащеність інформаційних центрів системи правоохоронних органів; по-друге – недостатнє застосування новітніх програмних ресурсів [1].

Мета використання інформаційно-аналітичного забезпечення правоохоронних органів зводилась до статистичного аналізу інформації, ведення кримінальних обліків, здійснення контролю за процесом розгляду повідомлень і заяв щодо злочинів.

Відсутність єдиних стандартів та класифікаторів для забезпечення функціонування інформаційних, інформаційно-телекомунікаційних систем призводить до розрізненості форматів накопичення та зберігання інформації, неможливості реалізації принципу інтероперабельності інформаційних ресурсів [2].

Визначення правового забезпечення інформаційних технологій в правоохоронній та юридичній діяльності – це системи правових дій, які складаються у визначеній послідовності, спрямовані на досягнення правового результату для формування та розвитку сукупності методів, виробничих процесів і програмно-

технічних засобів, інтегрованих з метою збирання, опрацювання, зберігання, розповсюдження, показу і використання інформації в інтересах її користувачів в сфері юридичної та правоохоронної діяльності [2].

Збільшення кількості інформаційних процесів, які виникають під час діяльності Національної поліції істотно впливають на рівень їх адаптивності до нових умов, потребує удосконалення порядку контролю за управлінськими процесами, суттєво впливає на організацію систематизації та аналізу інформації. Вирішення цих викликів полягає у застосуванні широкої автоматизації управлінських процесів у сферах відповідальності органів системи МВС, у тому числі щодо ідентифікації та верифікації особи, екстреної допомоги населенню при надзвичайних ситуаціях, реагування на адміністративні та кримінальні правопорушення [2].

До цього часу залишається неузгодженою архітектура взаємодії між інформаційними, інформаційно-телекомунікаційними системами, бракує стандартизованих інтеграційних інтерфейсів для обміну даними. Такий стан справ унеможливлює отримання оперативних даних з інших електронних реєстрів для виконання завдань, віднесених до компетенції органів Національної поліції. Подібні недосконалості створюють умови для потенційного нераціонального використання фінансових ресурсів.

Безумовно, вдосконалення системи інформаційного забезпечення правоохоронних органів позитивно відзначилося на рівні попередження, запобігання та подолання злочинності в країні. Переконливим був той факт, що інформатизація надала можливість працівникам правоохоронних органів автоматизувати однотипні та трудомісткі роботи, з їхньою допомогою розширити можливості працівників апарату управління у вирішенні конкретних завдань. Завдяки інформатизації правоохоронці мають змогу повніше виявляти тенденції та закономірності у сфері охорони громадського порядку та боротьби зі злочинністю, робити точніші прогнози, застосовувати прогресивні методи аналізу оперативної обстановки, оперативніше приймати рішення [1].

Отже, юридична та правоохоронна діяльність мають бути належним чином забезпечені відповідними інформаційними технологіями, адже їх впровадження свідчить про відповідність національної правоохоронної системи сучасним світовим критеріям ефективності функціонування [3]. Тож, проблему використання інформаційних технологій в правоохоронній діяльності вважаю актуальною. Необхідно винайти всі ресурси для її вирішення.

Використані джерела:

1. Петровський О.М. Правове забезпечення моніторингу паспортних даних в системі єдиного інформаційного простору правоохоронних органів. Електронний ресурс. URL: https://cutt.ly/zh0q3O2.

2. Цимбалюк В.І. Проблеми та перспективи удосконалення законодавства щодо інформаційного забезпечення правоохоронних органів. URL: http://www.sworld.com.ua/simpoz9/30.pdf.

3. Кишкань М.А. Гребенюк А.М. Роль інформаційних технологій в правоохоронній та юридичній діяльності. Електронний ресурс. URL: http://85.198.129.42/bitstream/123456789/4980/1/15.pdf.

Гавриш Б.О. курсант 2 курсу ФПФОДР
Науковий керівник: Мирошниченко В.О.
професор кафедри економічної та інформаційної безпеки, к.т.н., доцент
Дніпрропетровський державний університет внутрішніх справ

ПЕРЕВАГИ ТА ПРОБЛЕМИ ДИСТАНЦІЙНОГО НАВЧАННЯ

На сьогоднішній день у зв'язку з розповсюдженням глобальної пандемії коронавірусної інфекції COVID-19 більшість вищих і загальноосвітніх навчальних закладів, у тому числі і закладів зі специфічними умовами навчання були вимушені перевести навчання з очного режиму до дистанційної форми.

У зв'язку з цим майже всі здобувачі освіти зіткнулися з новою для себе формою навчання – системи дистанційного навчання або з платформами для проведення онлайн занять. І ось, вже пройшло пів року з того моменту, як студенти і учні перестали відвідувати свої навчальні заклади, за цей період багатьом з них довелося зіткнутися з перевагами, а інколи і з недоліками дистанційного навчання.

Перш за все, хотілось би почати з недоліків, так як саме вони змушують відчувати дискомфорт здобувачів освіти під час освітнього процесу.

● Майже весь навчальний матеріал ти повинен засвоїти самостійно.

Але це, в свою чергу, вимагає великої сили волі, свідомості, самоконтролю і відповідальності. Тому у тебе повинна бути величезна мотивація задля того, аби прочитати наприклад лекцію, яка містить в собі 25 сторінок різноманітної інформації.

● Така форма навчання недостатньо впливає на розвиток комунікабельності та навичок роботи в команді.

Всі ми знаємо, що спілкування через інтернет ніколи не замінить живе спілкування. А тим паче в віці від 12 років дітям та підліткам обов'язково потрібне спілкування з однолітками саме при безпосередньому їх контакті.

● Недостатній контроль за засвоєнням знань отриманих під час навчання.

Тому, як кажуть, все на твоїй совісті. Так, авжеж є сумлінні учні, які будуть виконувати всі необхідні завдання у повній мірі і в зазначений час, але і завжди існували і будуть існувати такі не зовсім сумлінні здобувачі освіти, які байдуже ставляться до своєї освіти та до зауважень інших.

● Можливість хакерського вторгнення в електронну базу даних.

Більшість закладів освіти мають спеціально відведених фахівців для контролю за інформаційною безпекою, але це не забезпечує сто відсоткову гарантію безпеки баз даних, або навіть приватної інформації користувачів цих баз.

Але по при всі ці недоліки у дистанційної форми навчання наявні і переваги перед традиційним навчанням.

● Можливість батьківського контролю над знаннями учнів.

Якщо під час звичайного навчання у батьків немає можливості для достатнього контролю якості освіти своїх дітей, то дистанційна форма навчання дає

можливість може і не цілком, але хоча б частково контролювати час освітнього процесу і кількість опрацьованого матеріалу.

● Унеможливлювання цькування учнів, булінгу та різного роду насильства.

Нажаль, ця проблема існує, і від цієї проблеми не знайдено достатньо ефективного рішення. Форма навчання через інтернет зводить до мінімуму фізичні контакти учнів, і це дозволяє учням або студентам, які під час навчання в аудиторіях та класах піддавалися булінгу, або навість насильству, в будь-якому його виді почувати себе комфортніше і безпечніше.

● Навчання дистанційно дозволяє заощаджувати час на те, щоб зібратися і дійти до навчального закладу.

В вищих навчальних закладах ця проблема не така суттєва, адже при багатьох університетах є гуртожитки, в яких можуть жити іногородні студенти, але, наприклад в спеціалізованих загальноосвітніх закладах, таких як гімназії або профільні ліцеї, ця проблема є досить актуальною, і навіть тут альтернативна форма навчання дозволяє почувати себе в комфорті.

● Дозволяє проводити навчання забезпечуючи безпеку здобувачів освіти.

Дивлячись на ситуацію в Україні, та у світі взагалі, не знаходиться альтернатив для більш безпечного проводження навчальних занять, і навіть ні достатня дистанція, ні захисні маски не гарантують тобі сто відсоткову захищеність, і саме з цією задачею дистанційне навчання цілком справляється, і перекриває цим більшість недоліків.

Підсумовуючи все вище сказане, можна з впевненістю сказати, що дистанційна форма навчання не є панацеєю, але в даній ситуації, що склалася в зв’язку з поширенням вірусу COVID-19 вона являється єдиною цілком ефективною альтернативою.

Використані джерела:

1. Державна служба зайнятості [Електронний ресурс]. – Режим доступу: https://www.facebook.com/zaniatist/posts/1455608477886316/

2. Переваги та недоліки: що варто знати про дистанційне навчання у Житомирі [Електронний ресурс]. – Режим доступу: https://zt.20minut.ua/Osvita/perevagi-ta-nedoliki-scho-varto-znati-pro-distantsiyne-navchannya-u-zh-11163782.html

Кочетова В.С. студент 3 курсу 1 групи факультету №1 ННІПКБ Одеського державного університету внутрішніх справ
Науковий керівник: Мельнікова О.О.
кандидат юридичних наук, доцент
викладач кафедри кібербезпеки та інформаційного забезпечення факультету підготовки фахівців для підрозділів кримінальної поліції Одеського державного університету внутрішніх справ

КІБЕРБУЛІНГ- РОЗВАГА ЧИ ЗЛОЧИН?

У наш час, Інтернет надає безмежних можливостей у житті суспільства. Без нього суспільство не може провести і близько години. Люди не можуть уявити своє життя без телефону, комп'ютера та головне постійного доступу до Інтернету.

В цьому є дві позиції: перша це те, що доступна будь-яка інформація для саморозвитку. За допомогою Інтернету можна отримати навчальні матеріали, можна спілкуватись з людьми, які знаходяться на іншому кінці світу. За допомогою нього також можна працювати, дивитися фільми, мультсеріали, слухати музику та багато чого іншого. Друга позиція протилежна першій. В цій позиції ми розглядаємо соціальні мережі, які виступають засобами зв’язку але можуть містити елементи вербування та жорстокості. Практично з маленького віку діти починають самостійне використання соціальних мереж і батьки можуть не замислюватися щодо загроз, які можуть там підстерігати. Однією з таких загроз може бути «кібербулінг».

Що таке кібербулінг? Як з ним боротися? Звідки він з'явився? І багато інших запитань, які цікавлять батьків, вчителів, дітей та інших.

«Кібербулінг» - це найжорстокіші знущання по відношенню до іншої людини, тобто приниження, залякування, цькування, які викликають страх у іншого із використанням будь-яких сучасних електронних (цифрових) технологій (телефонів, електронної пошти, комп'ютерів тощо).

У соціальних мережах є можливість говорити і робити найжорстокіші речі анонімно для себе, але не для тих кому це надсилається. Це може бути:

- поширення неправдивої інформації, або розміщення фотографій які ставлять в незручне становище будь-кого в соціальних мережах;
- відправка образливих повідомлень або погроз;
- видача себе за когось іншого і відправка неприємних повідомлень особам від його імені.

Кожне слово яке відправляється онлайн назавжди залишається в Інтернеті, а головне в пам'яті людини, а особливо дитини, яку принизили. Нажаль, зараз дуже жорстокі погляди. Може пройти дуже багато часу з того моменту коли дитину образили, але тим не менше це може нанести їй психологічну шкоду.

Зараз дуже актуально виставляти свої фотографії в соціальні мережі. Це можуть робити люди будь-якого віку. Можна навести приклад, коли одинадцятирічна дівчинка виклала своє фото і однолітки вирішили над нею

пошуткувати з приводу її зовнішності. Начебто здається що дрібниця, але дрібниця яку вона запам'ятає на все життя та може вважати себе з певними вадами.

Інший приклад, коли один негативний коментар з приводу ваги може змусити людей страждати від харчових розладів. Всього один негативний коментар з приводу нікчемності або непотрібності людини може привести його до самогубства.

Велика помилка людей, насамперед, дітей, які піддалися кібербулінгу це те, що вони замикаються в собі і нікому, нічого не розповідають. Вони вважають, що самі в цьому винні, що проблема в них, але це не так. Вони закриваються в собі, не хочуть ні з ким говорити. Самою великою підтримкою в такий час може бути тільки сім'я, тільки близькі люди. Так вони можуть витримати такий тиск.

На сьогоднішній день тисячі дітей піддаються кібербулінгу. Існує дуже багато випадків кібребулінгу. Найчастіше діти стикаються з такими його проявами:

- Флеймінг (flaming) – обмін короткими гнівними й запальними репліками між двома чи більше учасниками, використовуючи комунікаційні технології. Найчастіше розгортається в «публічних» місцях Інтернету, на чатах, форумах, дискусійних групах.

- Харасмент (harassment) – залучення повторюваних образливих повідомлень, спрямованих на жертву (наприклад, сотні смс-повідомлень на мобільний телефон, постійні дзвінки) з перевантаженням персональних каналів комунікації.

- Обмовлення (denigration) – розповсюдження принизливої неправдивої інформації із використанням комп’ютерних технологій. Це можуть бути і текстові повідомлення, і фото, і пісні, які змальовують жертву в шкідливій, інколи сексуальній манері. Жертвами можуть ставати не тільки окремі підлітки, а й групи.

Самозванство (impersonation) – переслідувач позиціонує себе як жертву, використовуючи її пароль доступу до її акаунту в соціальних мережах, блогу, пошти, системи миттєвих повідомлень тощо, а потім здійснює негативну комунікацію. Організація «хвилі зворотних зв’язків» відбувається, коли з адреси жертви без її відома відправляються ганебні провокаційні листи її друзям і близьким за адресною книгою, а потім розгублена жертва неочікувано отримує гнівні відповіді.

- Ошуканство (outing & trickery) – отримання персональної інформації в міжособовій комунікації й передання її (текстів, фото, відео) в публічну зону Інтернету або поштою тим, кому вона не призначалася.

- Відчуження (ostracism) – онлайн-відчуження, виключення з груп (чати однокласників, групи в соціальних мережах), відсутність швидкої відповіді на миттєві повідомлення чи електронні листи. Виключення у віртуальному середовищі наражає на серйозні емоційні негаразди, аж до повного емоційного руйнування дитини.

Кіберпереслідування – це дії з прихованого вистежування переслідуваних і тих, хто пересувається без діла поруч, зазвичай зроблені нишком, анонімно, для організації злочинних дій на кшталт спроб зґвалтування, фізичного насильства, побиття. Відстежуючи через Інтернет необережних користувачів, злочинець отримує інформацію про час, місце й усі необхідні умови здійснення майбутнього нападу.

- Хепіслепінг (happy slapping) – відносно новий вид кібербулінгу, який

починався в англійському метро, де підлітки, прогулюючись пероном, раптом ляскали один одного, тоді як інший учасник знімав цю дію на мобільну камеру. У подальшому за будь-якими відеороликами, у яких записано реальні напади, закріпилась назва хепіслепінг. Ці відеоролики розміщують в Інтернеті, де його можуть продивлятись тисячі людей, зазвичай без жодної згоди жертви.

Ще один вид кібербулінгу, що потребує окремої уваги, - новий вид сексуального насильства проти дітей в інтернеті – кібергрумінг.

Кібергрумінг – це налогодження злодіями, які гарно знають психологію дітей, довірливих стосунків з дитиною (через соціальні мережі та фейкові акаунти) з метою отримання від неї інтимних фото чи відео з подальшім шантажуванням дитини для отримання більш відвертих матеріалів, грошей чи зустрічей в офлайні.

По-друге, не рекомендується давати незнайомцю номер телефону, будь-які паролі тощо. Краще не відповідати або заблокувати образника.

У разі якщо по відношенні до дитини спричинили кібребулінг потрібно не залишатися на одинці з цим відчуттям. Потрібно шукати підтримку в родині, друзях, там де дитина упевнена, що її не образять як ні в онлайн-просторі, та к і ні в реальному житті.

Спілкування з незнайомцями в Інтернеті може нести небезпеку, тому краще спілкуватися зі знайомими у реальному житті людьми; доцільно також закрити від незнайомців свою сторінку в соціальних мережах та список друзів; не варто писати назву навчального закладу, де навчається дитина; не слід надсилати незнайомцям з Інтернету і в приватні повідомлення свою адресу та номер телефону.

Якщо ситуація вийшла з під контролю, то обов’язково необхідно зберегти докази (скриншоти листування, аудіо/відео конференцій) для демонстрації їх родичам, вчителям або навіть поліції.

Чим менше інформації про себе викладається в соціальних мережам, тим меншою є загроза бути жертвою кібербулінгу.

Використані джерела:

1. Про основні засади забезпечення кібербезпеки України : закон України від 05.10.2017 № 2163-VIII. Режим доступу: http://search.ligazakon.ua/l_doc2.nsf/link1/T172163.html.

2. Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві: Закон України від 23 грудня 1993 року № 3782-XII. Режим доступу: http://zakon3.rada.gov.ua/laws/show/3782-12

3. Найдьонова Л.А. Гуманізація стосунків через подолання цькування в шкільній спільноті / Наук. студії із соц. та політ. психології: Зб. ст. / АПН України, Ін-т соц. та політ. психології. К.: Міленіум, 2007. Вип. 17(20). С. 157−166.

4. Посібник для батьків «Кібербулінг та дорослий контент: як вберегти дитину". Режим доступу: http://bezpeka.kyivstar. ua/materials/articles/article7

5. Посібник про булінг «Булінг у школі: що потрібно знати"/Bullying in Schools: What You Need to Know /Пола Лангана (Paul Langan) . Режим доступу: http: //kazkarka. com/books/posibnyk-pro-bulinh

Батура Д.В. курсант ІІ курсу факультету
підготовки фахівців для органів
досудового розслідування
Науковий керівник: Прокопов С.О.
старший викладач кафедри економічної та інформаційної безпеки
Дніпропетровський державний
університет внутрішніх справ

ФІНАНСОВЕ ШАХРАЙСТВО В СОЦІАЛЬНИХ МЕРЕЖАХ

Наш сучасний світ складно уявити без соціальних мереж, таких, як:Instagram, Twitter, Facebook і тому подібні. Майже кожна людина, а особливо молодь, активно користуються соціальними мережами. Наразі складно уявити наше життя без широкого використання інтернету, соціальних мереж та месенджерів. Всі ці мережі та месенджери нам помітно спрощують життя у спілкуванні з нашими близькими та друзями, в пошуку потрібної інформації та навіть, заробляти кошти, сидячі вдома за комп'ютером.

Заробіток вдома ,а точніше в соціальних мережах, став особливо популярним саме зараз, в період карантину. Кожен намагається щось вигадати чи спростувати, як би швидше і легше заробити кошти, але не все так просто як здається. В погоні за швидкими грішми, дуже часто, ми стаємо жертвами шахрайських схем.

В соціальних мережах, гортаючи сторінки чи публікації ми натикаємось на безліч реклам з вигідними пропозиціями, де пропонують швидкий спосіб заробітку, не дивлячись на те школяр ти, студент чи доросла людина. Однією з них є схема під виглядом так званого «франчайзингу». Франчайзинг — форма співпраці між юридично та фінансово незалежними сторонами (компаніями та/або фізичними особами), в рамках якої одна сторона (франчайзер), що володіє успішним бізнесом, відомою торговою маркою, ноу-хау, комерційними таємницями, репутацією та іншими нематеріальними активами, дозволяє іншій стороні (франчайзі) користуватися цією системою на певних умовах. Тобі пропонують купити, за невелику суму, стартовий пакет для просування чи відкриття твого бізнесу в соціальних мережах або ж перепродажу цієї ж SMM франшизи іншим. Звичайно ж за таку невелику суму ніхто не надасть тобі цього пакету послуг і зазвичай після відправки коштів твій аккаунт блокують або ж продавець просто зникає і ігнорує.

Не менш привабливими є також інтернет-магазини: багатий вибір продукції, приваблива ціна, яка, зазвичай, менша ніж в звичайних магазинах та доставка, майже до оселі. Купуючи певну продукцію в Інтернеті, ми часто стаємо неуважними, довіряючи інтернет-магазинам, чим і користуються шахраї .

Зазвичай все відбувається так: створюється сайт або ж сторінка в соціальній мережі, де викладаються товари однієї номенклатурної ознаки. Наприклад, жіночий одяг певної торгової марки. На такому сайті, зазвичай, не має відгуків, привабливого дизайну, небагато інформації і працює цей інтернет-магазин, найчастіше, по 100% передплаті. Покупець обирає товар, оплачує його і чекає на відправку, але,

звичайно, замовлення ніхто нікуди відправляти не буде. Зателефонувавши за номером продавця покупець виявить, що такий номер не обслуговується.

Ще одним із найпоширеніших видів шахрайства в інтернеті є букмекерські контори. Зараз багато хто робить ставки на спорт, функціонують багато букмекерських контор і тоталізаторів, в яких можна спробувати заробити на своєму знанні спорту або інтуїції. Але якщо гравець початківець або не дуже впевнений в собі, то він може проконсультуватися з тим, хто знає, яка ставка буде прибутковою. Такою людиною є так званий «каппер». Каппер – це фахівець, який відмінно розбирається в спорті і в усьому, що з ним пов'язано, він давно займається ставками на спорт і має від них стабільний дохід, тобто його ставки успішні. Тож, як працює така шахрайська схема: вам пише людина і пропонує безкоштовно спробувати договірний матч, говорить вам про те, що у нього супер інсайдерська інформація, вам втрачати нічого і ви погоджуєтесь. Отримали перший безкоштовний прогноз на матч – виграли, отримали другий і теж виграли. Тепер ви на 100% впевнені, що у шахрає є точна інформація і він вже пропонує оплатити вам, в середньому, 5-10 тисяч за наступний прогноз матчу. Ви купуєте і програєте.

Існують й інші варіанти обману. Шахрай може зателефонувати вам від імені співробітника банку та повідомити, що ваша картка заблокована або повідомляє, що у неї заборгованість по кредиту і почали нараховуватися відсотки. Для того, щоб розблокувати або ж уникнути кредиту потрібно повідомити конфіденційні реквізити [1].

І тоді, перелякана помилковим боргом людина, не замислюючись, повідомляє все, що у неї просять. Після чого з її рахунку зникають всі гроші.

Тому, щоб не бути обдуреним в Інтернеті, як на нашу думку, необхідно слідувати наступним правилам:

1.Не розголошувати особисті данні в інтернет-мережі чи по телефону без реальної потреби. Особливо у випадках, коли вам телефонують з банку. І варто пам'ятати, що справжній співробітник банку ніколи не запитає конфіденційні дані картки, тому що це – порушення закону. Для того, щоб заблокувати чи розблокувати картку, банку не потрібно дзвонити вам і дізнаватися конфіденційні дані.

2.Не робити великих передоплат при покупці в інтернет-магазині. Краще використовувати спосіб покупки – накладений платіж. Тоді можна отримати товар, оглянути його і після цього оплатити.

3. Не користуватися підозрілими сервісами або пропозиціями інших людей. Люди або сервіси, що пропонують швидкий заробіток або допомогу в рішенні кредитних труднощів часто виявляються шахраями

4. Не приймати будь-яку інформацію за правду. Перш ніж якось відреагувати чи відповісти, задумайтесь чи схожа вона на правдиву. Навіть якщо це повідомлення від друзів в соціальних мережах. Їх аккаунт могли зламати.

5.Не реагувати на дзвінки та повідомлення від незнайомих номерів, що пропонують заробити мільйони , віддавши пару тисяч гривень.

6.Найголовніше – це бути уважним, тому що існує безліч способів, як можуть обманувати в інтернеті і навряд чи їх всі можна перерахувати. Тому, тільки уважність і недовіра до тих, хто просить, переконує і пропонує, може по

справжньому вберегти від шахраїв.

Якщо ви стали жертвою шахраїв в інтернеті, перше, що потрібно зробити – звернутися в поліцію. Зателефонуйте за номером 102 або звернутися до спеціального відділу у структурі МВС України, який займається злочинами в Інтернет просторі [2].

Використа ні джерела:

1. Дисертація з права –Теоретичні засади розслідування шахрайства в сучасних умовах, 2007 р. – розділ 1- [Електронний ресурс] - Режим доступу: http://mego.info/

2. Офіційний сайт кіберполіції України. – [Електронний ресурс] Режим доступу: https://cyberpolice.gov.ua.

Байрак К.С. курсант ІІ курсу факультету підготовки фахівців для органів досудового розслідування

Науковий керівник: Прокопов С.О.

старший викладач кафедри економічної та інформаційної безпеки

Дніпропетровський державний університет внутрішніх справ

ПРОБЛЕМИ КІБЕРБЕЗПЕКИ В УКРАЇНІ

Окремі дослідження вказують, що вдалими маніпуляціями можливо впливати на суспільну думку, а також викрадати приватну інформацію важливих осіб. Аналіз першопричин проблеми забезпечення кібербезпеки призводить до цілої низки системних проблем у галузі, ігнорувати які з кожним наступним інцидентом стає дедалі важче. Одна з головних – неефективна нормативна база та система управління. Інша і не менш важлива проблема – неготовність реагувати на кіберінциденти. Більшість компаній все ще не готові організаційно до нових хвиль кібератак та не мають підготовлених в достатній мірі фахівців у своєму штаті. Загалом управління кібербезпекою в Україні на державному рівні важко назвати ефективним. Національна система кібербезпеки обмежується переважно участю в ній силових органів (Нацполіція, СБУ, Держспецзв'язок тощо). Приватний бізнес та кіберспільнота до вирішення важливих питань майже не долучається [1].

Метою доповіді є визначення проблем та методів їх усунення в галузі кібербезпеки України. Питання кібербезпеки в Україні, на мою думку, є дуже важливим оскільки на даний момент український інтернет сервіс не є достатньо захищеним.

Давайте згадаємо 2017-й рік коли були заблоковані інтернет сервіси Росії і це не просто так, адже науковцями доведено, що завдяки вдалим маніпуляціям можливо впливати на суспільну думку, а завдяки гарному технічному забезпеченню можливо дізнатися важливу інформації про окремих осіб.

В наш час соцмережі заполонили наше життя. Навіть військовослужбовці, поліцейські та інші особи, яким заборонено або не рекомендовано вести активне Інтернет-життя, діляться різними фотографіями, розповідають чимало конфіденційної та особистої інформації, яка може бути використана, в тому числі, для підриву економіки та інших сфер держави.

Чималу проблему створює те, що професійні знавці кібербезпеки їдуть закордон оскільки на території України вони не знаходять собі місця роботи за спеціальністю або їх робота є низькооплачуваною. Ще одним чинником, який впливає на негативну оцінку кібербезпеки в Україні - це те, що Інтернет-мережу захищають тільки спецслужби України (наприклад СБУ), тоді як в США цим займаються фірми з кібербезпеки (наприклад McAfee, Palo Alto, Cisco) [2].

В якості висновків, вважаю за доцільне, запропонувати такі шляхи вирішення питання кабербезпеки України: по-перше, створити власні соцмережі, які будуть гарно розвиненими; на даний момент вже є українські платформи (наприклад Сусіди, #НаМайдані, druzi), але вони не є достатньо цікавим для користувачів [3]. По-друге створити компанії, які будуть забезпечувати кібербезпеку в Україні. По-третє, встановити високооплачувану заробітну плату для спеціалістів у галузі інформаційної безпеки, оскільки їх професія дуже важлива в сучасному високорозвиненому в технічному плані житті суспільства.

Отже, створити безпечний інтернет для українців можливо, але потрібно прикласти деякі зусилля, щоб кібербезпека України розвивалася та відповідала сучасним викликам.

Використані джерела:

1. Олексій Янковський, Олексій Барановський, Єгор Аушев, Артем Карпинський, Володимир Стиран. Українська правда: Україні потрібна нова кіберстратегія. 14.09.2019. URL: https://www.pravda.com.ua/columns/2019/09/14/7226291/

2. Шеллінг Томас К. Мікромотиви та макро поведінка. Нью-Йорк: W.W. Нортон та Ко .; 1978 рік. ISBN 978-0-12-407814-7.

3. Шакарян Пауло; Шакарян Яна; Руф Ендрю (2013). 9. Втрата довіри до своїх друзів: експлуатація соціальних мереж. Вступ до кібервійни: мультидисциплінарний підхід. Амстердам; Бостон: Сингрес ISBN 978-0-12-407814-7.

Андрусяк Л.В. курсант 4 курсу факультету підготовки фахівців для підрозділів стратегічних розслідувань
Науковий керівник: Прокопов С.О.
старший викладач кафедри економічної та інформаційної безпеки
Дніпропетровський державний університет внутрішніх справ

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ВИЯВЛЕННЯ ЗЛОЧИНІВ, ЩО ВЧИНЯЮТЬСЯ ПІД ЧАС ПУБЛІЧНИХ ЗАКУПІВЕЛЬ

Для вжиття ефективних заходів з виявлення злочинів, що вчиняються під час здійснення публічних закупівель у сфері охорони здоров'я, оперативні підрозділи повинні мати змогу здійснювати систематичне збирання та аналіз інформації з усіх відповідних джерел, щоб використовувати оперативні дані і у стратегічних, і тактичних цілях. Отримання оперативних даних передбачає оброблення й аналіз значного обсягу інформації про осіб, які підозрюються у причетності до вчинення злочину. Методи, що застосовуються для отримання і використання такої інформації, регламентуються законодавством і відомчими нормативними актами. Основною метою системи інформаційного з виявлення злочинів, що вчиняються під час здійснення публічних закупівель у сфері охорони здоров'я є всебічна інформаційна підтримка практичної діяльності оперативних підрозділів на основі комплексу організаційних, нормативно-правових, технічних, програмних та інших заходів. Інформаційне забезпечення – система пошуку й отримання відомостей про злочинів, що вчиняються під час здійснення публічних закупівель у сфері охорони здоров'я, є процес нагромадження, опрацювання, аналіз даних отриманих при здійснені обслуговуванням установ та об'єктів галузі охорони здоров'я.

Процес збирання інформації оперативними підрозділами під час оперативного пошуку залежить від особливостей оперативної обстановки, що формується на об'єктах охорони здоров'я, її оцінка та аналіз неможливі без вивчення особливостей функціонування їх господарювання. Вони складаються зі значної кількості відомостей, що мають важливе значення для діяльності оперативних підрозділів і ефективного виконання покладених на ці підрозділи завдань. Проте ці відомості перебувають у різних інформаційних системах у хаотичному стані. Щоб вони перетворились на інформацію, котра здатна забезпечити потреби оперативних підрозділів, їх потрібно систематизувати, впорядкувати, тобто створити з них інформаційний потік, що спеціально призначений для оперативних служб [1].

Із застосуванням спеціальних технічних засобів і комп'ютерних технологій для отримання, обробки й аналізу оперативно-розшукової інформації, як зазначає А.С. Овчинський, формуються нові напрями, що спираються на можливості аналітичної та комп'ютерних баз даних, використання мультимедійних систем. Розробка і впровадження в оперативну практику автоматизованих інформаційно-пошукових систем органічно збіглися і стимулювали розвиток теоретичних уявлень

про те, що оперативно-розшукова діяльність складається з двох фактично пов’язаних між собою частин: пізнавальної (пошук, збирання, аналіз та оцінка інформації, що становить оперативний інтерес) і діяльної (активної) (практична реалізація отриманої інформації) [2, с. 97].

Зростання ролі інформаційного аналізу безпосередньо пов’язано із упровадженням підходу «правоохоронної діяльності на ґрунті аналітичної інформації» (intelligence-led policing)

Такий підхід дозволяє ефективно планувати правоохоронну діяльність і відстежувати хід подій, координувати збір інформації відповідно до конкретних справ, формувати реалістичну картину діяльності об’єктів, виявляти зв’язки між подіями, робити обґрунтовані прогнози, формувати профіль злочинної поведінки, виявляти осіб, що займають ключові позиції у кримінальних мережах, і визначати їхню роль, відстежувати прибутки, отримані злочинним шляхом, ефективно спрямовувати обмежені ресурси правоохоронних органів, удосконалювати співробітництво з партнерськими структурами на національному та міжнародному рівнях[3, с. 22].

З метою комплексного інформаційного забезпечення виявлення злочинів, що вчиняються під час здійснення публічних закупівель у сфері охорони здоров’я необхідно використовувати інформаційні масиви Державної казначейської служби України про: установлення бюджетних асигнувань розпорядникам бюджетних коштів на основі та в межах затвердженого розпису бюджету; затвердження кошторисів, паспортів бюджетних програм (у разі застосування програмно-цільового методу в бюджетному процесі), а також порядку використання бюджетних коштів; взяття бюджетних зобов'язань; отримання товарів, робіт і послуг; використання товарів, робіт і послуг тощо.

Використані джерела:

1. Лебеденко В.І. Джерела, фіксація та аналітична обробка агентурної інформації / В.І. Лебеденко // Вісник Львівського ін-ту внутр. справ. – Львів: ЛІВС. – № 2 (16). – С. 240–244.

2. Овчинский А.С. Информация и оперативно-розыскная деятельность: монография / А.С. Овчинский. – М.: ИНФРА-М, 2002. – 390 с.

3. Лукашов В.А. Организация и методика аналитической работы в сфере оперативно-розыскной деятельности органов внутренних дел / В.А. Лукашов. – Омск: Омская высшая школа МВД СССР, 1983. – 32 с.

Федченко Т.К. курсант ІІ курсу факультету підготовки фахівців для органів досудового розслідування
Науковий керівник: Прокопов С.О.
старший викладач кафедри економічної та інформаційної безпеки
Дніпропетровський державний університет внутрішніх справ

ПОСЯГАННЯ НА КІБЕРБЕЗПЕКУ ЯК АКТУАЛЬНА ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ УКРАЇНИ

Розглядаючи даний аспект, хотілось би наголосити на тому, що обрана нами проблематика є досить актуальною. Адже саме від рівня захищеності державних інформаційних ресурсів залежить не лише надійне забезпечення безпеки національних інтересів, а й формування відкритого інформаційного суспільства. Вважаємо за необхідне відмітити, що загальне становище України у сфері інформатизації у порівнянні з зарубіжними країнами не може бути визнане навіть як задовільне, що у свою чергу обумовлює актуальність посягання на інформаційну безпеку держави. Тому виникає нагальна потреба створення системи забезпечення кібербезпеки України задля припинення протиправних посягань на інформаційний простір держави в умовах сьогодення.

Сьогодні дедалі більшого поширення набувають злочини в інформаційному просторі, які спрямовані як на порушення роботи, так і на розкрадання, руйнування державних інформаційних ресурсів. У свою чергу, необхідно звернути увагу на тому, що сучасні дослідники, які розглядали даний аспект сходяться на думці, що до основних джерел кібернетичних загроз слід відносити: міжнародні злочинні та терористичні угрупування хакерів, транснаціональні корпорації, іноземні державні органи, адміністративно-управлінські органи, тощо.

Традиційно загрози, що виникають в кібернетичному просторі класифікують за характером спрямованості: на внутрішні, джерелом походження яких є вітчизняний інформаційний простір, або національний сегмент глобальної інформаційно - телекомунікаційної мережі, та зовнішні, поширення яких, пов‘язане з характером глобальності мережі Інтернет.

Поряд з тим, екстериторіальність Інтернету, значно ускладнює визначення конкретного джерела загрози, так як може ідентифікуватися за доменом в одній країні, а поширювати інформацію в іншій, не розкриваючи його, за допомогою використання пошукової системи, посилання тощо.[1, с. 171]

Вважаємо, що окремої уваги заслуговують такі кіберзагрози як кібертероризм та кібершпигунство. Адже кібертерористи мають на меті не лише отримати доступ до особистих даних користувачів інформаційної мережі, а й заволодіти інформацією з обмеженим доступом задля завдання шкоди у соціальній та економічній сферах держави.

Загалом характеризують такі тенденції у сфері загроз інформаційній безпеці:

неконтрольовані ризики, пов’язані з так званим «інтернетом речей» і поширенням мережевих з’єднань; стрімке зростання «кіберзлочинів як сервісу» – надання цифрових послуг кримінальними синдикатами; зростання правових ризиків у сфері регулювання мережевих комунікацій; хакерські атаки, спрямовані на підрив репутації брендів і політичних сил [2]

Зауважимо, що наразі Україна робить доволі значні кроки щодо припинення протиправних посягань на інформаційні ресурси та забезпечення безпеки у кіберпросторі держави. Наприклад, нещодавно директор асоціації «Інформаційні технології України» К. Васюк та начальник Департаменту кіберполіції О. Гринчак підписали меморандум про співпрацю. Обидві сторони наголошують, що саме така співпраця дозволить не лише запобігти витоку в Інтернеті інформації з обмеженим доступом та персональних даних користувачів мережі, а й ефективніше забезпечувати захист прав і свобод громадян та інтересів держави від злочинних посягань у кіберпросторі.

Отже, аналізуючи зміст вищенаведених суджень доходимо висновку, що проблема захисту інформаційних ресурсів держави від протиправних посягань з боку кібертерористів та іноземних держав є доволі актуальною для України.

Тому вважаємо за необхідне приділяти якомога більше уваги аспекту кібербезпеки з метою формування відкритого інформаційного суспільства та надійного забезпечення безпеки національних інтересів у інформаційному просторі.

Використані джерела:

1. Веселова Л. Ю. Кібернетичні загрози у контексті сучасного сприйняття їх в Україні // Вісник Харківського національного університету імені В. Н. Каразіна. Серія «Право», (29), 2020., 169-175. [Електронний ресурс] Режим доступу: https://doi.org/10.26565/2075-1834-2020-29-22.

2. Thor Olavsrud. 4 information security threats that will dominate 2017. CIO (December 29, 2016) [Online tool]. – Available at: https:// cio.com/article/ 3153706/security/4-information-security-threats-thatwill-dominate-2017.htm.

Сергійчук К. М., курсант ІІ курсу факультету
підготовки фахівців для органів
досудового розслідування
Науковий керівник: Прокопов С. О.
старший викладач кафедри економічної та
інформаційної безпеки
Дніпропетровський державний
університет внутрішніх справ

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Нинішнє суспільство, як і окрема людина в ньому, просто не може себе мислити без різноманітних інформаційно-телекомунікаційних технологій. Розвиток комп'ютерної техніки, мобільного зв'язку, різних цифрових інновацій підштовхує, а іноді і змушує людину ними користуватися. Впровадження сучасних цифрових технологій в діяльність поліції України дозволить більш ефективно і якісно вирішувати завдання по забезпеченню охорони громадського порядку та боротьбі зі злочинністю. Стає все більш актуальним питання оснащення поліцейських перспективними електронними засобами, що забезпечують їх діяльність в єдиному цифровому інформаційному просторі Національно поліції. Проблематику використання сучасних інформаційних технологій в діяльності Національної поліції України досліджували такі науковці: І. Арістова, О. Бандурка, В. Цимбалюк, В. Гавловський, В. Мацюк, О. Сирова, Д. Узлов та інші. Під інформаційними та комунікаційними технологіями розуміється сукупність методів, пристроїв і виробничих процесів, використовуваних суспільством для збору, зберігання, обробки і поширення інформації.

Розвиток мереж мобільного зв'язку третього (3G) і четвертого (3,5G, 4G або LTE) поколінь, поширення точок доступу Wi-Fi надають можливість виходу в мережу Інтернет, де люди обмінюються різноманітною інформацією, споживають мультимедійний контент, отримують інформацію із засобів масової інформації, здійснюють грошові операції (оплата, переклади, поповнення). Співробітники поліції також можуть використовувати вищезгадані технології та пристрої для виконання своїх безпосередніх службових завдань.

Інтернет - міжнародна мережа з'єднаних між собою комп'ютерів, унікальний засіб всесвітньої комунікації . Сьогодні Інтернет об'єднав безліч різних мереж, мільйони комп'ютерів і більше двох з половиною мільярдів користувачів з усіх континентів планети. Проводячи аналіз тих можливостей, які дозволяють отримувати різного роду інформацію за допомогою Всесвітньої павутини, приходимо до висновків, що, наприклад, слідчий або оперативний співробітник в процесі відповідно розслідування кримінальної справи або роботи за матеріалом попередньої перевірки мають можливість оперативно отримувати будь-яку довідкову інформацію. Також можна використовувати ресурси різних підрозділів правоохоронних органів, що мають місце в Інтернеті, для знаходження

розшукуваного особи або майна. З метою організації безпосереднього зв'язку поліцейського з іншим особами, які цікавлять в реальному часі, з візуалізацією людини або без неї можна використовувати ведення розмови або відеозв'язку за допомогою IP-телефонії, використання спеціалізованих програм (за допомогою VoIP-технології (від англ. Voice over IP) - технологія передачі голосу через IP, тобто набір комунікаційних протоколів, технологій і методів, що забезпечують традиційні для телефонії набір номера, дозвон і двостороннє голосове спілкування, а також відеоспілкування через мережу Інтернет або будь-яким іншим IP-мереж [1].

Ключовим органом, на який покладено функції з формування інформаційних ресурсів Національної поліції,є Департамент інформатизації МВС України (згідно з наказом МВС України від 31 січня 2018 р. № 70 «Про затвердження Положення про Департамент інформатизації Міністерства внутрішніх справ України»). Основними завданнями Департаменту є [2]:

- вдосконалення інформаційних і телекомунікаційних технологій;
- вдосконалення автоматизованих інформаційних систем;
- розвиток сучасних цифрових систем зв'язку;
- протидія технічним розвідкам;
- технічний захист інформації;
- формування і ведення інформаційних ресурсів;
- міжвідомча інформаційна взаємодія;
- реалізація державних і відомчих програм у рамках інформатизації та інші завдання.

Одним з головних напрямків діяльності Департаменту є активна участь, поряд з іншими державними органами виконавчої влади, в процесі переходу до надання державних послуг в електронному вигляді.

Необхідно відзначити, що впровадження електронних регламентів не обмежується лише наявністю можливості у громадян звертатися за отриманням послуг через Інтернет, це також внутрішня робота органів влади між собою.

За підтримки Консультативної місії Європейського Союзу в Україні в Національній поліції започатковано впровадження моделі поліцейської діяльності, керованої аналітикою (Intelligence-Led Policing/ILP), згідно з якою оперативноаналітична інформація/intelligence слугує підставою для проведення операцій/розслідувань, а не навпаки [3].

Використання передових досягнень науки і техніки, сучасних інформаційно-телекомунікаційних мереж загального користування та обмеженого доступу, доступу до різноманітних баз даних відіграє важливу роль в інтенсифікації процесу передачі, обміну та отримання інформації в ході попередження, припинення і розкриття злочинів в діяльності Національної поліції

Використані джерела:

1. Узлов Д.Ю., Струков В.М. Про новий підхід до взаємодії поліції з населенням на основі сучасних інформаційних технологій // «Сучасні проблеми правового, економічного та соціального розвитку держави» : тези доп. V Міжнародної науково-практичної конференції (м. Харків, 18 листопада 2016 року) /

МВС України, Харківський національний університет внутрішніх справ. – Харків, 2016. – 472 с.
2. Наказ МВС України «Про затвердження Положення про Департамент інформатизації Міністерства внутрішніх справ України» від 31 січня 2018 р. № 70. [Електронний ресурс]. - Режим доступу: http://search.ligazakon.ua/l_doc2.nsf/link1/MVS819.html
3. Carter J. G., Phillips S. W., Gayadeen S. M. Implementing Intelligence-Led Policing: An Application of Loose-Coupling Theory / Journal of Criminal Justice. – 2014. - № 42. - p. 433-442.

Попова Т. В. курсант І курсу факультету
підготовки фахівців для органів
досудового розслідування
Науковий керівник: Прокопов С. О.
старший викладач кафедри економічної та
інформаційної безпеки
Дніпропетровський державний
університет внутрішніх справ

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

Глобальна всесвітня мережа, що об'єднує мільйони комп'ютерів у транснаціональну єдину систему Інтернет відкриває широкі можливості спілкування та обміну інформацією. Постійне вдосконалення мережі Інтернет відбувається в процесі кардинальної трансформації сфер праці, дозвілля та політики. Щодня велика верства користувачів мережі свідомо і несвідомо стають правопорушниками. На сьогодні комп'ютерні злочини - це одна з найдинамічніших груп суспільно небезпечних посягань, шахрайство в інтернет або, як в народі говорять інтернет-шахраї. Швидко збільшуються показники поширення цих злочинів, а також постійно зростає їх суспільна небезпечність. Кіберзлочинці стають дедалі стійкішими, підвищують рівень професіоналізму. Анонімність, безконтрольність та вседозволеність дає змогу шахраям господарювати в Інтернеті та відчувати свою безкарність [1].

Подальше дослідження та розроблення соціально-психологічного портрета злочинця, який вчиняє шахрайства в мережі Інтернет, є актуальним і становить не лише теоретичне, а й практичне значення. Можливість визначення соціально-психологічних даних про особу інтернет-шахрая є одним із головних факторів як у

розслідуванні злочину, так і в організації заходів протидії та профілактиці таких злочинів. Поінформованість про властивості особистості суб'єктів злочинної діяльності у сфері вчинення інтернет-шахрайств дає змогу оперативним працівникам, слідчим своєчасно виявляти, розслідувати такі злочини, визначати тактику проведення допиту, криміналістичних операцій [2, с.71-73].

Характеристику особи злочинця становлять ті дані, за якими можна визначати ефективні шляхи розшуку та викриття злочинця [2, с.72-73]. Одним із перших елементів шахрайства є особа злочинця. Під час дослідження особи злочинця важливу роль відіграють як сліди, залишені ним у процесі вчинення злочину, так й інформація про соціально-психологічні риси особи, що дає змогу звузити коло пошуку, виокремити категорії, групи людей і навіть конкретних осіб, які мають унікальні особливості, що є досить складним упродовж розслідування віртуального злочину.

Наявні також певні особливості, що обумовлюють вибір конкретної злочинної діяльності, яку шахрай планує вчиняти або вже його скоїв. Тому за видом інтернет-шахрайства, учиненого злочинцем, можна визначити відмінні особливості виражені в наявній сукупності психологічних властивостей та запропонувати її психологічний портрет. Таким чином, під час розслідування конкретних злочинів коло можливих суб'єктів можна істотно звузити.

Психологічна характеристика особи-шахрая базується на концепції, яка запропонована юридичною психологією, згідно з якою в основі складання психологічного портрета відмітними рисами для інтернет-шахрая слід вважати:

Такі особи мають широкий кругозір, високий інтелектуальний рівень, добре орієнтуються на прогнозуванні поведінки та застосувань способів маніпуляції, щодо знаходження слабких сторін жертви, рішучість, уважність, схильність до постійного ризику є фізіологічно необхідним для шахрая. Більшість злочинців мають схильний дар уяви, вони використовують вплив і вміння переконувати людей, вміння викликати довіру. Спостережливі, з швидкою реакцією на обстановку та самоконтроль у різних ситуаціях. Ще до особистих якостей належить уміння привернути до себе навколишніх, відчути і зрозуміти їх психічні стани.

Щоб спіймати шахрая, слід мислити як він, знати його психологічні особливості поведінки. Це надає можливість зрозуміти методологію формування шахрайства, ураховуючи основні його елементи – мотив, можливість, раціональність.

Психологічний аналіз, профілювання інтернет-шахраїв під час розслідування потребує об'єднання інформації з різних джерел, зокрема дослідження та інтерпретація всіх речових доказів, дослідження жертви, надання характеристики особистості злочинця та його поведінки, даних про спосіб злочинних дій, мотив злочинця та можливості вчинити злочин [3, с. 61-63].

Шахрайство являє собою своєрідну "інтелектуальну" злочинну діяльність. Здійснення такої діяльності передбачає, що шахрай у своїй свідомості розробляє різні схеми проведення шахрайської операції. Маючи соціально-психологічну характеристику особи інтернет-шахрая, можна скласти соціально-психологічний портрет, прийоми розробки психологічного портрета злочинця дозволяють

аргументовано висунути версію про ознаки особистості, яка вчинила злочин. Метою його складання є створення загального уявлення про тип особистості злочинця, вироблення стратегії, пропонування варіантів того, як знайти особу, що вчинила злочин. Особливості портрета інтернет-шахрая є підґрунтям для слідчих органів для розслідування злочину, організації заходів протидії та профілактики шахрайств, розроблення тактик ведення допиту, проведення обшуку, затримання тощо[4].

Отже, соціально-психологічна характеристика поведінки особи, яка вчиняє шахрайства в мережі Інтернет, сприятиме вдосконаленню методів розслідування таких шахрайств і вчасному їх виявленню.

Використані джерела:

1. Часопис Київського університету права. – 2010. - № 4. – С. 346-349

2. Антонова Н. О. Психологічна зрілість як основа готовності до професійної діяльності психолога/ Н.О. Антонова, Л.І. Рибачук [Електронний ресурс]. – Режим доступу : http://journals.uran.ua/index.php/2227-6246/article/view/162200.

3. Теоретичні засади розслідування шахрайства в сучасних умовах : монографія / О. Л. Мусієнко ; за ред. проф. В. Ю. Шепітька. — Х.: Право, 2009. — 168 с.

4. Брисковська О. М. Соціально-психологічна характеристика особи, яка вчиняє шахрайство в мережі Інтернет / О. М. Брисковська [Електронний ресурс]. – Режим доступу: https://doi.org/10.33270/01201141.70

Луц Н.А. курсант ІІ курсу факультету підготовки фахівців для органів досудового розслідування
Науковий керівник: Прокопов С.О.
старший викладач кафедри економічної та інформаційної безпеки
Дніпропетровський державний університет внутрішніх справ

ІНФОРМАЦІЙНЕ СУСПІЛЬСТВО ЯК ОКРЕМИЙ ШЛЯХ РОЗВИТКУ УКРАЇНИ

Сучасна фінансово-економічна криза спричинила кризу традиційних ринкових відносин. Криза з усією силою показала, що нинішнє індустріальне суспільство втрачає енергію розвитку і перевантажено величезною кількістю невирішених проблем і невизначеностей. Для пошуку подальшого шляху розвитку слід враховувати, що індустріальний період закінчився в кінці минулого століття. Ілюзія

сьогоднішньої модернізації суспільства на основі проведення індустріальних реформ поглинає все більшу частку ресурсів, не даючи ніяких нових шляхів розвитку. В результаті, боротьба з кризою перетворюється просто в нарощування обмеженості розвитку. Разом з тим історичний досвід свідчить, що при виникненні соціально-економічних проблем завжди створюються шляхи та методи їх вирішення. В сьогоднішніх умовах ми спостерігаємо два шляхи розвитку з індустріального укладу. Перший шлях - це рух суспільства назад - до "неофеодалізму", другий - це нескінченне "реформаторство" індустріалізму, на практиці виливається у перманентний простой. Є ще третій шлях, про який говорять, але в силу інерції на який мало звертають уваги - це експансія в інформаційний простір та інформаційну економіку з наступною побудовою інформаційного суспільства.

Перший і другий шлях припускають відмову від досягнень демократії і чреваті новими формами авторитаризму, третій характеризується розширенням демократичних засад і заміну індустріальних смислових спектрів на інноваційні. Причому третій шлях найбільш суспільно прийнятний і соціально очікуваний, хоча супроводжується опором старого адміністративного апарату. Визначальною рисою третього шляху розвитку є те, що він породжує новий чинник виробництва - інформацію, знання і їх контекст. Тут треба зазначити, що категорія "фактора виробництва" є головною для визначення суспільного способу виробництва і суспільства в цілому. Коли поряд із землею і працею з'явився новий фактор виробництва - капітал, який визначив новий спосіб виробництва, суспільства отримали назву капіталістичних. При цьому, у порівнянні з попередньою людською історією, недовге панування нового фактора виробництва дозволило здійснити такі зрушення в економіці і житті людей, які набагато переважають все досягнуте за тисячоліття. Цей історичний досвід переконливо доводить, що поява нового фактора виробництва відкриває величезні можливості зростання економіки і добробуту, а його аналіз свідчить про нові переваги в порівнянні з вже відомими. Традиційні засоби виробництва в процесі праці зношуються фізично і морально.

Відмінна риса інформації і знань полягає в тому, що в процесі споживання вони не зменшуються, а навпаки, примножуються. При цьому слід зауважити, що використання інформації і знань має бути етичним, тому що етика інформації і знання є первинною по відношенню до їх суті і є визначальною для переходу до інформаційного суспільства. Друга перевага полягає в тому, що традиційні фактори виробництва - земля і капітал - примножують головним чином фізичні сили людини, а інформація і знання реалізують і примножують розумові його потенції, що зумовлюють інтелектуалізацію виробництва і праці, що породжує нові поняття - інтелектуальна власність, інтелектуальний капітал, інтелектуальний продукт. Не можна ефективно господарювати без використання цих нових процесів і понять [1].

Візьмемо, наприклад, інтелектуальний капітал. Його роль в економіці швидко зростає. Досить сказати, що його частка у вартості підприємств в країнах Західної Європи досягає 50-68%, а у нас в балансі підприємств він дорівнює 1%. За традицією ми вважаємо вартість підприємств за обсягом матеріальних цінностей,

матеріальних активів в той час, коли все зростаючу роль відіграють нематеріальні активи. Це знижує ціну наших підприємств.

Завдяки своїм якостям інформація і знання відіграють визначальну роль в інноваційному розвитку, обумовлюючи інтелектуалізацію економіки, дія інтелектуального капіталу, зростання інтелектуальної власності та інтелектуальної продукції. Ставка держав на модернізацію економіки та інновації - це ставка, в кінцевому рахунку, на інформацію і знання як якісно новий фактор виробництва. Уряди тільки намагаються створювати нові системи управління (про що йшла мова на недавньому Всесвітньому економічному саміті в Давосі), розуміючи, що сьогоднішня економіка і індустріальні методи господарювання не відповідають інноваційним вимогам товариств. Сьогоднішній розвиток інформаційного простору, завдяки Інтернету, який сформував інформаційну техносферу, технологічно визначено. Але невирішеним є конструювання на цій базі інститутів нового суспільства. Таке конструювання відбувається в США в вигляді "стратегії хмарних обчислень", в Євросоюзі ця стратегія виписана як "Цифровий порядок денний для Європи до 2020 року" [2].

У СНД такі конструкції реалізуються на базі мережі інформаційно-маркетингових центрів (ІМЦ), яка визначена міжурядовою "Угодою про співробітництво держав - учасниць СНД у створенні, використанні та розвитку міждержавної мережі інформаційно-маркетингових центрів для просування товарів і послуг на національні ринки", яке сьогодні ратифіковано в Білорусії, Таджикістані і Україні і вступило в юридичну силу.

Методологічно мережу ІМЦ спирається на фундаментальні розробки Львівсько-Варшавської школи логіки (1890-1939 рр.), Австрійської економічної школи, на практичну реалізацію завдань програми ЗДАС (Загальнодержавної автоматизованої системи обробки та обліку інформації) Інституту кібернетики ім. В.М. Глушкова. Мережа ІМЦ являє собою сукупність інформації, зануреної в законодавчо оформлену інформаційно-технологічне середовище, яка дозволяє моделювати і реалізовувати будь-які господарські, адміністративні, управлінські та бізнес-процеси. На практиці мережу ІМЦ реалізує перехід до нової економічної моделі. Головне - не потрібно значних витрат бюджету, а економічний ефект виходить миттєво, що створює умови для подолання кризових явищ [3].

В якості висновку можна визначити що мережа інформаційно-маркетингових центрів дозволяє подолати фазовий бар'єр переходу від індустріальної фази розвитку до нової формації. Крім вище згаданого, мережа ІМЦ має ще цілий ряд пріоритетних якостей. Важливим економічним показником сьогодні вважається рейтинг кібер-могутності, тобто "Здатності держави розгортати критичну цифрову інфраструктуру, необхідну для продуктивної і безпечної економіки" до складу якої входять: нормативно-правове регулювання кібер-простору, електронний економічний і соціальний контекст, технологічна інфраструктура та її використання. Мережа інформаційно-маркетингових центрів на практиці дозволить Україні вирішити проблему відставання від розвинених країн в питаннях розвитку.

Використані джерела:

1. О.О. Чуприна, К.С. Чуприн Методологічні підходи до оцінювання інтелектуального капіталу// Вісник Національного університету «Юридична академія України імені Ярослава Мудрого» № 3 (14) 2013. [Електронний ресурс] Режим доступу: http://econtlaw.nlu.edu.ua/wp-content/uploads/2016/01/3-22-34.pdf
2. Давос-2019: главные месседжи Всемирного экономического форума. Экономическая правда [Електронний ресурс] Режим доступу: www.epravda.com.ua/rus/publications/2019/01/27/644694/
3. Перспективи розвитку ринку хмарних обчислень в Україні: переваги та ризики. Аналітична записка. Національний інститут стратегічних досліджень. [Електронний ресурс] Режим доступу: http://old2.niss.gov.ua/articles/1191/

Гупал Д. курсант факультету підготовки фахівців для органів досудового розслідування Дніпропетровського державного університету внутрішніх справ
Науковий керівник: Рижков Е.В.
к.ю.н. , доцент, завідувач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ

ТЕХНІЧНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ ТЕХНІЧНИМИ КАНАЛАМИ З ОБ'ЄКТІВ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

З метою протидії злочинності, ефективного попередження, припинення та розкриття злочинів органи та підрозділи Національної поліції України здійснюють необхідні: слідчі (розшукові) дії; негласні слідчі (розшукові) дії; оперативнорозшукові дії. Під час підготовки та проведення зазначених дій працівники поліції використовують інформацію з обмеженим доступом в акустичному та електронному вигляді [1, с. 20].

Така інформація може циркулювати в акустичному вигляді під час проведення нарад щодо планування певних негласних заходів. В електронному вигляді інформація циркулює, наприклад, під час підготовки необхідних документів, таких як плани, звіти, клопотання до суду.

Дана інформація може бути цікавою для представників організованих злочинних груп, та, навіть, представників іноземних розвідок. Вони можуть отримати доступ до цієї інформації шляхом фізичного доступу на об'єкт де циркулює ця інформація (в службовому кабінеті працівника поліції).

Також за допомогою сучасних приладів зловмисники можуть аналізувати

бездротові мережі (Wi-Fi) та вилучати незаконним методом данні жертви. Сучасні засоби технічної розвідки дозволяються підключатися дистанційно до обчислювальних машин, створювати перешкоди у телекомунікаційних каналах між пристроями і супутниковою системою, бездротових мережах [2].

В разі отримання несанкціонованого доступу сторонніх осіб до інформації з обмеженим доступом, це може призвести до більш ефективної протидії злочинців щодо документування їх діяльності з боку працівників правоохоронних органів або неможливості затримання злочинців.

З метою не допущення витоку інформації з об'єктів інформаційної діяльності поліції необхідно вживати заходів з технічного захисту інформації, таких як періодичний пошук засобів негласного зйому інформації («закладних пристроїв») та використання технічних засобів захисту акустичної інформації та електронно-обчислювальних машин.

На сьогоднішній день на ринку представлено багато різних за призначенням та технічними можливостями технічних засобів пошуку та захисту інформації, як українського так і закордонного виробництва. При цьому періодично на ринку з'являються нові розробки та нові технічні засоби.

Під час вибору технічних засобів, що будуть використовуватися для забезпечення захисту інформації, слід звернути увагу на такі технічні засоби як:

1. Тепловізори – використовуються для виявлення пристроїв, що виділяють температурне поле. Зазвичай ці прилади приховуються зловмисником у стінах.

2. Багатофункціональні пошуковий прилади – зазвичай вони поєднують в собі широкосмуговий детектор електромагнітного поля, приймач інфрачервоного діапазону, різні додаткові зонди для перевірки провідних ліній і оцінки віброакустичного захисту приміщення [3, с. 102].

3. Частотоміри – дозволяють виміряти частоту сигналу безконтактно, за допомогою антени. Така властивість дозволяє застосовувати їх як для замірів «відомих» сигналів, так і для пошуку «прихованих» сигналів від підслуховуючих пристроїв (жучків).

Таким чином, можна зробити висновок, що для забезпечення захисту інформації з обмеженим доступом від витоку з об'єктів інформаційної діяльності Національної поліції можуть використовуватися різноманітні технічні засоби, як пошукові та засоби захисту інформації.

Використані джерела:

1. Красіков Д.О. Правове забезпечення інформаційної безпеки в діяльності органів внутрішніх справ України: автореф. дис. ... канд. юрид. наук: 12.00.19 К., 2019. - 20 с.

2. Іванець Т.М. Інформаційев безпека держави як умова для збереження національного суверенітету. [Електронний ресурс] Режим доступу: http://intkonf.org/ivanets-tm-informatsiyna-bezpeka-derzhavi-yak-umova-dlya-zberezhennyanatsionalnogo-suverenitetu/ (дата звернення: 12.11.2020).

3.Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 рр.: Закон України № 537V від 9 січня 2007 р. Відомості Верховної Ради України. 2007. № 12. Ст. 102.

Жила Т.В. студентка юридичного факультету Дніпровського державного університету внутрішніх справ
Науковий керівник: Тютченко С.М.
старший викладач кафедри економічної та інформаційної безпеки Дніпровського державного університету внутрішніх справ

ПРИНЦИПИ ФУНКЦІОНУВАННЯ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Інформаційна безпека-це стан захищеності систем обробки і зберігання даних, при якому забезпечено конфіденційність, доступність та цілісність інформації. Властивістю інформації є її використання та розвиток в інтересах громадян. Багато науковців розглядають інформаційну безпеку як комплекс заходів, спрямованих на забезпечення захищеності інформації особи, суспільства і держави від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки запису чи знищення (у цьому значенні частіше використовують термін «захист інформації») [1]. Інформаційна безпека країни характеризується захистом стабільності у таких основних сферах життя, як економіка, технології та управління громадською діяльністю, які пов'язані з небезпечною дестабілізацією деструктивних, суперечних інтересам країни інформаційним впливам.

Головними принципами забезпечення інформаційної безпеки є: законність, баланс інтересів особи, суспільства і держави; комплексність; системність; інтеграція з міжнародними системами безпеки; економічна ефективність.

Поняття інформаційної безпеки не обмежується безпекою технічних інформаційних систем або захистом інформації в цифровій або електронній формі. Об'єктивно кажучи, поява "інформаційної безпеки" зумовлена появою методів обміну інформацією між людьми та усвідомленням того, що їх інтереси та інтереси їхніх спільнот можуть бути знешкодженими. Інформаційне спілкування, його існування та розвиток забезпечують і встановлюють обмін інформацією між усіма верствами суспільства.

Функції забезпечення інформаційної безпеки підприємств [2]:

- розробка методів аналізу загроз, оцінки рівня інформаційної безпеки підприємства і систем її забезпечення;
- організація і здійснення діяльності із захисту інформації;
- експлуатація технічних засобів захисту інформації;
- аудит і контроль функціонування системи інформаційної безпеки підприємства.

З розвитком нових ІТ-технологій концепція інформаційної безпеки була значно розширена. Деякі експерти зазначають, що доцільніше повністю замінити поняття інформаційної безпеки поняттям мережевої безпеки. Це пов’язано з тим, що захист процесів, інформації та діяльності в сучасному кіберпросторі залежить не

лише від втрати інформації. Безпека мережі - це захист від вірусів, хакерських атак та підробки даних. Наприклад, вони можуть не тільки видаляти або красти дані, але й впливати на роботу та продуктивність роботи персоналу або, навіть, зупиняти виробництво. Інформація також може використовуватися для нападу на людей або будівлі. Тож, інформаційна безпека стала частиною мережевої безпеки.

Сучасна кібербезпека охоплює три фактори: системи, процеси та люди. В результаті широкої цифрової інтеграції у життєдіяльність людей та технології , проблеми інформаційної безпеки іноді стають проблемами безпеки життя. Тому потрібна нова концепція концепція інформаційної безпеки, яка б могла вирішити широкий спектр проблем у кіберпросторі сучасності.

Неможливо створити систему, захист якої не можна буде зламати. Основним принципом може бути створення такого механізму захисту, вартість зламу якого буде дорожчою за інформацію, яку можна отримати. Тому необхідним є впровадження програмних засобів безпеки, які вмонтовані до складу програмного забезпечення системи і є потрібними для виконання функцій захисту. За словами експерта з кібербезпеки Дмитра Ганжело: "Усунення наслідків кібератак часто обходиться в кілька разів дорожче, аніж профілактика боротьби з ними."

В сучасних умовах, не гарантуючи належний захист інформації, неможливо забезпечити стабільний економічний розвиток як окремого підприємства так і держави. В Україні забезпечення інформаційна безпека здійснюється шляхом захисту інформації — у випадку, коли необхідність захисту інформації визначена законодавством в галузі захисту інформації. Для реалізації захисту інформації на підприємствах створюється Комплексна система захисту інформації (КСЗІ) [3].

Використані джерела:

1. Інформаційна безпека. Електронний ресурс. URL:https://cutt.ly/Fh0wSMc

2. Основні поняття безпеки інформаційних технологій. Електронний ресурс. URL: https://infopedia.su/1x2f0c.html

3. Безпека особистої інформації. Електронний ресурс. URL: https://sites.google.com/site/bezpekaosobistoieinformaciie

Зосімов А. курсант факультету підготовки фахівців для органів досудового розслідування Дніпропетровського державного університету внутрішніх справ
Науковий керівник: Гребенюк А.М.
доцент кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ

ВІРТУАЛЬНЕ ПРАВО ЯК ІННОВАЦІЙНИЙ НАПРЯМ В ЮРИДИЧНІЙ НАУЦІ

Освоєння Інтернету – це вивчення й звикання до нього як до нового інформаційного середовища з різноманітними способами активності в ній. На сьогоднішній день ми стоїмо на порозі остаточного утвердження інформаційного суспільства – новій ланці розвитку людства. Ми навіть не можемо собі уявити сучасне у якому відсутня глобальна інформаційна мережа.

У зв'язку з активним користуванням Інтернетом в повсякденному житті, в усіх куточках світу проводиться багато досліджень, тематикою яких є взаємодія Інтернету та суспільства, їх впливу один на одного. Однак, думки й позиції авторів мають серйозні розбіжності, тобто ми не можемо сказати, що існують однозначні визначення і поняття стосовно цієї теми, це свідчить про те, що для того, щоб дійсно прогресувати в цій сфері, треба проводити серйозні, масштабні та, насамперед, комплексні дослідження. Доволі сумним є той факт, що всі види наукових робіт, присвячені цій тематиці, дійсно можна перелічити на пальцях. У цей же час, в юридичній літературі проблематика загального дослідження інтернет-права (яке є не лише окремим суб'єктом, а ще й пов'язане і поширюється на кримінальне, цивільне та інші галузі права) розповсюджується занадто повільно [1].

В останні роки відбулися деякі позитивні зміни у галузі правового регулювання ІТ-технологій, але, на жаль, ми не можемо приділяти особливої уваги цьому невеличкому прогресу, оскільки ми все ще не маємо однозначної правової термінології. Слід зауважити, що навіть найпоширеніші поняття, без яких регулювання правових відносин просто неможливе, не мають однозначного трактування [3].

Процедура глобалізації, абсолютно нові й невідомі нікому раніше економічні та соціальні явища нового тисячоліття зовсім не вимагають від нас «відкидання» усіх старих норм і понять, вони також не змушують нас відбудовувати в усіх галузях права все по-новому, орієнтуючись тільки мінімальним досвідом або взагалі, намагатися бездумно відтворити моделі заходу. Навпаки! Побудова нової, сучасної концепції інтернет-права відбувається на основі тих самих визначень, категорій, які вже створено раніше. Це навіть допомогло б у розширенні та доповненні загального понятійного апарату зі сторони теорії держави та права, а також й багатьох інших галузей юридичної науки [2],[4].

На сьогоднішній день інтернет-право досліджується безпосередньо як явище

тісно пов’язане з інформаційним правом, цей факт обґрунтовується певними причинами, які стосуються спільності об’єктів дослідження цих сфер знань [1].

Проаналізувавши усе вищезазначене, можемо сказати, що наразі інтернет право – це сучасне, абсолютно автономне відділення юридичної науки, і понад усе - інформаційного права.

Тож, на нашу думку, інтернет-законодавство - це сукупність законів та певних актів, що регулюють відносини у відповідному просторі. В якості таких відносин можуть виступати безпосередньо пов’язані з соціально-правовим керуванням віртуального простору відносини, на встановлених правових, моральних, етичних основах.

Використані джерела:

1. Інформаційне право [Електронний ресурс]. - Режим доступу: http://telecomlaw.ru/studyguides/infolaw/kopylov_2002.pdf

2. Бачило И.Л. Информационное право: учебник / И.Л. Бачило, В.Н. Лопатин, М.А. Федотов; под ред. акад. РАН Б.Н. Топорнина. – СПб.: Издательство “Юридический центр Пресс”, 2001. – 789 с

3. Бачило И. Л. Информационное право: учеб. для магистров / И. Л. Бачило. – 3-е изд., перераб. и доп. – М. : Юрайт, 2013. – 564 с.

4. Венгеров А.Б. Теорія держави і права. Учебник. - 2-е изд. - М.: Омега-Л, 2005. - 595 с.

Кусайко І. Ю., курсант 3 курсу факультету підготовки фахівців для органів досудового розслідування Дніпропетровського державного університету внутрішніх справ
Науковий керівник: Рижков Е.В.
кандидат юридичних наук, доцент,
завідувач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ

ІНФОРМАЦІЙНА ДІЯЛЬНІСТЬ ПРАВООХОРОННИХ ОРГАНІВ В ДІЯЛЬНОСТІ УКРАЇНСЬКОЇ ПОЛІЦІЇ ТА ПОЛІЦІЇ ЗАРУБУЖНИХ КРАЇН

На сьогоднішній день суспільство не стоїть на місці та переживає науково-технічну революцію. В результаті активного впливу людини на ту чи іншу сферу виробництва виникають інформаційні технології. Використання інформаційних технологій та систем відіграє чималу роль в діяльності поліції. За останні роки активно впроваджується використання комп’ютерної техніки у роботі правоохоронних органів. Це впливає насамперед на розслідування кримінальних

правопорушень, а здійснення автоматизованого пошуку сприяє систематизації та аналізу доказової інформації.

Актуальність інформаційного забезпечення діяльності поліції характерна не тільки для України, а й для більшості іноземних держав, де багато уваги приділяється використанню інформаційних технологій та систем в діяльності правоохоронних органів. Зокрема, правоохоронці за кордоном намагаються використовувати нові технології для розкриття, виявлення та навіть профілактики злочинів. Вони широко використовують соціальні мережі, насамперед, для зв'язку з населення, та в подальшому для отримання важливої інформації. Наприклад, Росія для відстеження активності в соціальних мережах використовує спеціальні термінали «Призма». Система може відстежувати окремо стоять блог-майданчики і соцмережі. Всього, за словами розробників, під око Кремля потрапляють 60 млн «джерел». При цьому система аналізує тональність висловлювань кожного з цих джерел з похибкою 2-3% практично в реальному часі. В моніторинг потрапляють практично всі майданчики, за винятком Facebook, стверджують розробники. У тому числі блоги на LiveJournal, Twitter, YouTube.[1]До речі, таку ж систему розробляли і в Україні, але через відсутність фінансування розробка була призупинена. Україна в деякому плані «відстає» в плані моніторингу та аналізу соціальних мереж через ряд причин, а саме через недостатню кількість спеціалістів,що працюють у цьому напрямку та відсутність нормативно закріплених повноважень у правоохоронців щодо здійснення заходів для протидії злочинності у сфері кіберпростору.

Британські правоохоронці також наголошують,що соціальні мережі відіграють важливу роль у розкритті та виявленні злочинів,вони навіть включили відповідний курс для підготовки молодих співробітників. Велика Британія є прикладом того як поліція повинна співпрацювати с громадськістю. Наприклад,для поінформованості британців про криміналістичну ситуацію в країні був створений електронний сервіс «Карта злочинності». Зокрема, сервіс допомагає дізнатися рівень злочинності у будь-якій частині Великої Британії, а також виявити які злочини найбільш поширені у певному районі та дізнатися інформацію про правоохоронця,який обслуговує даний район.[2]

Важливу роль в інформаційному забезпеченні поліції США відіграє система Compstat. Перший принцип програми CompStat - впевненість в дієздатності поліції. Другий полягає в тому, що в основі ефективного скорочення злочинності і вирішення проблеми поліпшення якості життя лежать чотири напрямки, а саме: своєчасний і точний збір інформації, ефективна тактика, швидке розгортання сил і засобів, продовження роботи і оцінка гарантії стратегічного вирішення проблеми. Крім того, база даних містить щоденну статистику по інцидентах із стрілянино ю і жертвам перестрілок, а також викликам поліції. Цифри, включені в звіт CompStat - не остаточні, призначені лише для того, щоб якомога швидше надати керівникам поліції найбільш наближені до фактичних даних значення. Тобто система, можна сказати, є засобом раннього оповіщення, що забезпечує готовність до реагування на швидко змінливі умови і дозволяє своєчасно розгортати і перерозподіляти ресурси.

В Україні робота з базами даних поліції здійснюється відповідно до Положення про Інтегровану інформаційно-пошукову систему органів внутрішніх

справ України від 12.10.2009 р. №436, затвердженого наказом Міністерства внутрішніх справ України.

Таким чином, як показує досвід інших країн організація роботи правоохоронних органів з використанням інформаційного забезпечення та постійного зв'язку з громадськістю впливає на підвищення ефективності роботи поліції та є дієвим засобом для розкриття, виявлення та попередження злочинів.

Використані джерела:

1. В федеральних органах власти внедряют специальные терминалы «Призма» для отслеживание активности в блогах и социальных сетях [Електронний ресурс]. - Режим доступу: http://bda-expert.com/2012/08/v-federalnyh-organah-vlasti-vnedryayut-specialnye-terminaly-prizma-dlya-otslezhivaniya-aktivnosti-v-blogah-i-socialnyh-setyah/

2. Колодяжний М. Г. Досвід Великої Британії у використанні громадськості щодо запобігання злочинності // Форум права., 2013., № 3. - С. 317–323.

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

ОСОБЛИВОСТІ КІБЕРПРОСТОРУ ЯК ОБ'ЄКТА КРИМІНАЛІСТИЧНОГО ДОСЛІДЖЕННЯ

Стрімкий розвиток комп'ютерних технологій зумовлює появу нових форм взаємодії між членами суспільства. Суспільство отримало доступ до безмежних інформаційних потоків, що призвело до розширення можливостей сучасної злочинності. Використання кіберпростору для вчинення злочинів привертає до нього увагу в криміналістичних дослідженнях.

Указ Президента України від 15 березня 2016 року «Про рішення Ради національної безпеки і оборони України» від 27 січня 2016 р. «Про стратегію кібербезпеки України» передбачає створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Законодавець вбачає в кіберпросторі певне середовище, в якому можуть бути вчинені кримінальні правопорушення та сформулював загальні завдання, пов'язані з забезпеченням безпеки функціонування і використання кіберпростору. Це зобов'язує суб'єктів сектору безпеки та оборони створити умови для забезпечення ефективної боротьби із кіберзлочинністю [1].

Кіберпростір є складовою частиною інформаційного простору і утворюється як за допомогою мережі Інтернет та безпосередньо у ній функціонує, а може бути автономною системою, не пов'язаною із глобальною мережею. Автор праці « Декларація незалежності кіберпростору» зазначив: «Електронний інформаційний простір має два рівні – обмін інформацією у формі програмних кодів, які створюють кіберпростір та віртуальне життя, створене внаслідок обміну інформацією між користувачами мережі [2]. Кіберпростір – це результат взаємодії між людьми шляхом обміну інформацією в електронній цифровій формі. Можна стверджувати, що кіберпростір як об'єкт криміналістичного дослідження має подвійну природу, а саме: технічну і соціальну.

Інтернет є основним, але не єдиним засобом створення кіберпростору. З урахуванням комп'ютерної складової електронного обліку інформацією, кіберпростір утворюють усі телекомунікаційні мережі, комп'ютерні системи й пристрої, що забезпечують передачу вихідної інформації іншим користувачам. Інформація в електронній цифровій формі, що має криміналістичне значення, за своєю фізичною природою є доступною безпосередньому сприйняттю через використання програмно-технічних засобів. Внаслідок знищення, копіювання, блокування, модифікації та іншого впливу на комп'ютерну інформацію шляхом доступу до неї утворюються певні відомості, які в криміналістиці називають інформаційними слідами. Носіями таких слідів є відповідні технічні засоби, а не матеріальні об'єкти чи свідомість людини, тому ці сліди ще називають віртуальними.

Віртуальні сліди є досить складним об'єктом для пізнавальної діяльності слідчого в рамках певного кримінального провадження. Такі сліди можуть зберігатися Інтернет - провайдерами або користувачами на певному матеріальному носії. З метою ефективного виявлення, фіксації та аналізу інформаційних слідів, які мають криміналістичне або доказове значення необхідно використовувати нові підходи у провадженні слідчих (розшукових) дій та належних слідчих дій, оскільки віртуальність кіберпростору забезпечує відносну конфіденційність інформації про особу злочинця та можливість впливати на свідомість певної категорії осіб. Це приваблює злочинців для використання кіберпростору в механізмі вчинення злочину [3].

Для дослідження кіберпростору слідчий може проводити огляд у ході якого описати технічне, програмне забезпечення, канали зв'язку із обов'язковим залученням спеціаліста. Матеріали фотозйомки, звукозапису, відеофіксації досліджуються як документі відповідно до ст. 99 Кримінального процесуального кодексу України (далі – КПК), у відповідній формі фіксуються і долучаються до матеріалів справи [4].

Кіберпростір як складову частину обстановки кримінального правопорушення можна дослідити за допомогою допити його учасників, наприклад, адміністратор групи у соціальній мережі може надати відомості щодо інформації, яка надсилалась користувачами групи, часу їх спілкування, моменту появи та реакції користувачів на відповідне повідомлення.

Доцільно також проводити негласні слідчі дії у формі зняття інформації з транспортних комунікаційних мереж та зняття інформації з електронних інформаційних систем, оскільки великий обсяг інформації у кіберпросторі передається за допомогою телекомунікаційних мереж та електронних систем.

Для дослідження кіберпростору слідчий призначає такі експертизи як: авторознавча, яка допомагає визначити автора і виконавця текстів та повідомлень у соціальних мережах; семантико – текстуальна експертиза писемного мовлення, яка досліджує зміст словосполучень, речень, текстів і виявляє висловлювання у формі публічних закликів до певних дій, наприклад, до участі у межових заворушеннях, терористичних актах; лінгвістична експертиза, яка досліджує мовленнєву діяльність в усній формі і зафіксовану у фоно або відеограмі; фототехнічна експертиза, яка допомагає ідентифікувати предмети, приміщення і ділянки місцевості на знімках; портретна експертиза для ідентифікації особи або трупа за фотознімком або відеозаписом.

Із комплексу інженерно-технічних експертиз може бути призначено експертизу комп'ютерної техніки і програмних продуктів та експертизу телекомунікаційних систем. Основними завданнями цих експертиз є характеристика параметрів інформаційних систем; робочий стан технічних засобів; встановлення фактів та способів передачі інформації [5].

Для оперативного виявлення злочинів, вчинених з використанням можливостей кіберпростору слід враховувати особливості вчинення злочину для його кримінально-правової кваліфікації; можливості, які створює кіберпростір для вчинення злочинів; вплив кіберпростору на методику розслідування окремих видів злочинів. У механізмі злочинної діяльності кіберпростір як обстановка злочину є передумовою швидкого досягнення злочинного результату в порівнянні з традиційною обстановкою.

Значні труднощі для розкриття та розслідування злочинів з використанням можливостей кіберпростору становить неможливість контролювати весь обсяг інформації в Інтернеті та соціальних мережах.

Визнання на державному рівні суверенного права регулювати комунікаційні можливості (наприклад, у Китаї, Ірані та деяких інших країнах) призводить до технічних помилок електронного зв'язку через надмірну завантаженість провайдерів. З одного боку, це зумовлює певні обмеження права на свободу слова, а з іншого – забезпечення державою належної правової охорони відносин у кіберпросторі,оскільки неузгодженість законів приваблюють злочинців. Адже правоохоронні органи стикаються з великою кількістю перешкод, коли під час розслідування встановлюють факт перебування під юрисдикцією іншої держави телекомунікаційної мережі, використаної для вчинення злочину, або власника інформаційного ресурсу, якого треба захищати від протиправного посягання [6].

За словами Крацберга М.: «Сама по собі технологія є ні гарною, ні поганою, але й нейтральною її не назвеш» [7]. Результати використання технологій залежать від мети суб'єкта їх застосування. Соціальні мережі створили безмежні можливості для об'єднання віддалених одна від одної осіб з метою діяльності організованих злочинних угрупувань. Організована злочинність активно використовує обстановку

кіберпростору для скоєння терористичних актів, незаконного обігу наркотичних засобів, піратства та інших кримінальних злочинів. Соціальні мережі стали масивом відомостей про реальне життя конкретної людини і ця база може бути використана для вчинення злочину.

Отже можна зробити висновок, що кіберпростір – це інформаційний простір взаємодії між людьми за допомогою електронних інформаційних технологій, обмін інформацією за допомогою яких здійснюється на основі системи стандартів, що пояснює технічну і соціальну природу кіберпростору.

Для досягнення злочинного результату використовуються такі особливості кіберпростору як дистанційність, що забезпечує транскордонну складову такої злочинної діяльності і викликає необхідність вирішення питань територіальної юрисдикції; оперативність дій щодо обробки інформації, що сприяє прискоренню або якісному приховуванню злочину; віртуальність, що ускладнює процес виявлення злочинця та дослідження інформаційних слідів; комунікативність, яка сприяє діяльності організованої злочинності як на національному, так і міжнародному рівнях; недосконаліть та наявність прогалин у законодавчій базі щодо забезпечення інформаційної безпеки та правової охорони відносин у кіберпросторі, що дав змогу уникати кримінальної відповідальності [8].

Тому враховуючи ці особливості потрібно застосовувати оновлені методи, прийоми та засоби з метою вирішення практичних завдань розслідування злочинної діяльності.

Використані джерела:

1. Рішення Ради національної безпеки і оборони України від 27 січня 2016 р. «Про стратегію кібербезпеки України. Указ Президента України». [Електронний ресурс].- Режим доступу: www.rada.gov.ua
2. Шевченко Е.С., Михайлюченко Н.Н. Кіберпростір як елемент обстановки скоєння злочину /Е.С. Шевченко, Н.Н. Михайлюченко// Академічний юридичний журнал. – 2015.- №1.-С.53-54
3. Динту В.А. Місце кіберпростору в системі обстановки злочину/ В.А. Динту// Науковий вісник Херсонського Державного Університету. - 2016.- вип.2-Ф.3. – С.72-75
4. Кримінальний процесуальний кодекс України від 13.04.2012 р. станом на 18.10.2018 р. [Електронний ресурс].- Режим доступу: www.rada.gov.ua
5. Самойленко О.А. Природа кіберпростору як об’єкта криміналістичного дослідження / О.А. Самойленко// Криміналістика і судова експертиза.- 2018.- вип. 1.- С. 176-180
6. Бєлєнський В.П. Відповідальність за кіберзлочини за кримінальним правом США, Великої Британії та України (порівняльне – правове дослідження)/ В.П.Бєлєнський// Юридичні науки. – 2016.- вип.1- Г. 2.-С. 83-86
7. Волинець В.О. Віртуальна реальність: поняття та сутність /В.О.Волинець// Часопис Київського університету права. – 2014. –вип.30.-С. 35-37
8. Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва /Д.В.Дубов//Вісник книжкової палати. - 2014.- вип. 2- С. 328-329

Збарацька Ю.О.
магістр групи М-ПД-921
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник: **Рибальченко Л.В.**
кандидат економічних наук, доцент
Дніпропетровського державного
університету внутрішніх справ

ШЛЯХИ ВПРОВАДЖЕННЯ В УКРАЇНІ ПРОГРЕСИВНОГО ЗАРУБІЖНОГО ДОСВІДУ ГРОМАДСЬКОГО ВПЛИВУ НА ЗЛОЧИННІСТЬ

В усьому світі боротьба із злочинністю ведеться на законодавчому рівні, проводяться заходи щодо виявлення, попередження та розкриттю злочинної діяльності груп та окремих громадян, які причасні та задіяні у злочинній діяльності. Реалізація та ефективна стратегія боротьби із злочинністю є запорукою зменшення рівня злочинності та зростання безпеки в державі.

Боротьба із злочинністю є соціально-управлінською та політичною категорією, вплив на причини, умови та розвиток, її попередження, виявлення наслідків та розкриття сутності є складним питанням, вирішення якого покладено на правоохоронні органи. Латентна частка злочинності [3] проявляється у різних сукупностях, які були скоєні, але які не стали відомими правоохоронним органам чи суду. До основних технологій, які використовуються в організаціях для протидії економічним злочинам та шахрайству, належать: регуляторна політика, моніторинг комунікацій, постійний моніторинг, тестування транзакцій (операцій), моніторинг електронної пошти, обробка великих масивів даних, залучення спеціалістів з аналізу даних тощо. До найбільш популярних технологій захисту даних в світі належать: моніторинг електронної пошти, постійний моніторинг, регуляторна політика та тестування транзакцій (операцій), частка яких становить більше 30% [1].

Дослідження зарубіжного досвіду до участі громадськості щодо запобігання злочинності дає підстави для запровадження стратегій та пропозицій, які стосуються удосконалення правоохоронної діяльності в існуючій проблемі. Різні напрями удосконалення державної внутрішньої політики у сфері запобігання злочинності із використанням громадськості можна класифікувати за їх характером на кілька видів, що охоплюють заходи політичної, нормативно-правової, організаційно-управлінської, соціально-психологічної й технічної спрямованості [2].

Відповідно до розуміння у західних країнах світу поняття «громадськість» у широкому значенні, необхідно відповідним чином формувати державну політику у сфері залучення різних соціальних інститутів до діяльності із запобігання злочинності в Україні. Звідси громадськістю охоплюватимуться не лише громадські формування правоохоронної спрямованості та окремі громадяни, а й заклади освіти і охорони здоров’я, органи самоорганізації населення, церква, релігійні організації, ЗМІ, волонтери, близькі родичі злочинців та правопорушників.

Заходи політичного характеру полягають у наявності в Україні політичної волі

на використання сучасних альтернативних підходів у модернізації правоохоронної діяльності, оптимізації роботи органів кримінальної юстиції у першу чергу за рахунок розширення участі недержавних суб'єктів у сфері запобігання і протидії злочинності.

Досліджуючи рівень безпеки в світі у 2020 році, необхідно зазначити, що самою безпечною країною є Катар, рівень безпеки в якій дорівнює 88,14, далі йде Тайвань, (84,35), ОАЕ (84,3). Україна із 129 країн світу знаходиться на 84 місці за рівнем безпеки (51,15) та на 46 місці за рівнем злочинності (48,85) [3].

Європейський досвід боротьби із злочинності приділяє увагу участі громадськості у запобіганні злочинності. В Німеччині фінансування такого проекту здійснюється за рахунок видатків державного утримання органів, які є його учасниками.

В Італії укладаються меморандуми про безпеку між МВС Італії та місцевими державними органами з метою приведення вимог безпеки громадян до належного забезпечення їх прав. Для зменшення злочинів в Італії використовують засоби відеоспостереження у громадських місцях та повідомлення до поліції, також проводять інформаційно-агітаційну кампанію щодо запобігання сімейному насильству через запровадження телефонної анонімної лінії.

У Франції щодо запобіжної діяльності проти злочинності на національному рівні відіграє Міжвідомчий комітет, до якого входять різні міністри французького уряду, але провідна роль відводиться міністрам внутрішніх справ, юстиції та освіти. Вони започаткували премію щодо запобігання злочинності, яка запроваджена Форумом з питань безпеки Франції (FFSU).

Провідні країни світу досягли успіхів у правоохоронній діяльності через ефективне використання коштів, які виділено на боротьбу із злочинністю та використанню допомоги громадськості та окремих громадян.

Сучасне розуміння громадськості для запобігання злочинності у провідних західних країнах світу відрізняється від вітчизняного. Тому дослідження сучасного зарубіжного досвіду громадського впливу на злочинність дозволяє дійти таких висновків, що українську правову систему необхідно реформувати шляхом підвищення рівня довіри громадян до діяльності правоохоронних органів поліції.

Використані джерела:

1. Рибальченко Л.В., Косиченко О.О. Латентність економічних злочинів як загроза безпеці підприємництва в Україні / Л.В. Рибальченко, О.О. Косиченко // Регіональна економіка та управління. - №3 (25) серпень 2019 р. – С.68-73

2. Колодяжний М. Г. Закон України «Про Національну поліцію» – крок до народу чи повернення у минуле / М. Г. Колодяжний // Юрид. вісн. України. – 2015. – №51–52 (26 груд. 2015 р. – 3 січ. 2016 р.). – С. 16, 17.

3. Рівень злочинності у світі. [Електронний ресурс]. – Режим доступу: - https://visasam.ru/emigration/vybor/prestupnost-v-mire.html

Калашник В.О. магістр групи М-ПД-922
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник: Рибальченко Л.В.
кандидат економічних наук, доцент
Дніпропетровського державного
університету внутрішніх справ

СТРАТЕГІЇ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМНИЦТВА

Останнім часом сучасні підприємства здійснюють свою діяльність в умовах високої невизначеності процесів, що відбуваються у світовій та вітчизняній економіці. При таких умовах успішна діяльність їх систем економічної безпеки залежить від рівня стратегічного управління, в основі якого лежить стратегія економічної безпеки підприємства. Як необхідність першої черги, економічна безпека підприємства має бути обґрунтована з точки зору стратегічного управління, тобто для ефективного управління підприємством. Важливим питанням є забезпечення економічної безпеки підприємства та розробка стратегій, як головного орієнтиру в цьому напрямку.

Метою дослідження є розвиток методичних підходів щодо формування стратегій економічної безпеки підприємства.

Важливою складовою частиною стратегічного управління економічної безпеки підприємства є стратегічне планування. Як зазначено в роботі [1], під стратегією економічної безпеки підприємства розуміють сукупність найбільш значущих рішень та заходів, спрямованих на забезпечення прийнятного рівня безпеки функціонування підприємства. Визначають три типи стратегії фінансово-економічної безпеки підприємства:

- раптового реагування на загрози;
- прогнозування небезпек та загроз;
- відшкодування завданих збитків.

У даному підході крок за кроком викладено типи стратегій, але він не передбачає усю повноту поняття «економічна безпека підприємства». Сенс запропонованих стратегій у даному підході полягає тільки в роботі з загрозами – усунення, запобігання, компенсація, але економічна безпека дещо ширша за загрози.

Стратегії економічної безпеки підприємства, в залежності від репутації підприємства, запропоновані в роботі [3] у вигляді матриці «Економічна безпека підприємства - репутація підприємства». Такий підхід можна вважати є незвичайним та цікавим, але вузько направленим, тобто таким, що не розкриває усього змісту дослідження, що спростовує його результати.

В роботі [1] наведено такі типи стратегій корпоративної економічної безпеки підприємства:

- орієнтовані на усунення існуючих або запобігання виникнення можливих загроз економічній безпеці;

- націлені на запобігання збитку від впливу існуючих або можливих загроз економічній безпеці;
- спрямовані на компенсацію збитку в результаті дії загроз економічній безпеці.

Головними рисами цього підходу є також обмеженість типів стратегії за змістом та невизначеність критеріїв їх відокремлення. В роботі [2] пропонуються такі стратегії фінансово-економічної безпеки:

- забезпечення росту прибутковості його власного капіталу; формування фінансово-економічних ресурсів;
- фінансово-економічної стабільності;
- безпеки інвестиційної діяльності;
- нейтралізації фінансово-економічних ризиків;
- безпеки інноваційної діяльності;
- захисту його конкурентної позиції;
- антикризова стратегія.

Такий перелік є повним та об'ємним за змістом в комплексі, але громіздким та складним за використанням. Запропоновані стратегії окремо одна від іншої є фрагментарними, що не дає змоги розробити комплексної, дієвої та універсальної стратегії.

Запропоновані типи стратегій економічної безпеки підприємства логічно, послідовно та в повній мірі відповідають концептуальним положенням [2], працюють на досягнення її цілей. При виборі того чи іншого типу стратегії економічної безпеки підприємства необхідно враховувати зазначені концептуальні аспекти питомої категорії, що систематизує елементи системи економічної безпеки підприємства та робить механізм її забезпечення дієвим.

На економічну безпеку підприємництва впливає ціла низка чинників, до яких належать економічні злочини. Особливості латентності економічних злочинів, які представляють загрозу безпеці підприємництва в Україні, засоби боротьби із злочинність та міжнародний досвід забезпечення безпеки держави та підприємництва, представлено в роботах [4, 5].

Таким чином, економічна безпека підприємства займає важливе місце в процесі ефективного управління ним, тому є невід'ємною ланкою його стратегічного управління, в залежності від цілей господарювання, засобів і можливостей їх досягнення, умов господарювання та конкурентного середовища, та ін. В роботі ми визначили, що стратегічне планування є важливою складовою частиною стратегічного управління економічної безпеки підприємства. Економічна безпека підприємства, як фактор ефективного управління ним, є об’єктом стратегічного управління. Задля якісного забезпечення економічної безпеки підприємства запропоновано концептуальний підхід до формування стратегії економічної безпеки підприємства, в рамках якого сформульовані такі послідовні типи стратегій: виживання, існування, обмеженого зростання та зростання.

Використані джерела:

1. Линник О.І. Стратегія економічної безпеки підприємства як фактор

зменшення впливу зовнішніх та внутрішніх загроз / О.І. Линник, Н.В. Артеменко // Вісник НТУ „ХПІ”. Серія: Технічний прогрес і ефективність виробництва. – Х.: НТУ „ХПІ”. - 2013. - № 67 (1040) - С. 159-169

2. Стратегічне управління фінансово-економічною безпекою підприємства [Електронний ресурс]/ О.В. Черевко // Ефективна економіка. – 2014. - №2 . - Режим доступу: http://www.economy.nayka.com. ua/?op=1&z=3302

3. Дмитрук Є.В. Визначення стратегії фірми в залежності від сили та напряму впливу репутації підприємства на рівень його економічної безпеки / Є.В. Дмитрук // Вісник східноукраїнського національного університету імені Володимира Даля. – 2010. - №8(150). – С. 358-364

4. Рибальченко Л.В., Косиченко О.О. Латентність економічних злочинів як загроза безпеці підприємництва в Україні / Л.В. Рибальченко, О.О. Косиченко // Регіональна економіка та управління. - № 3 (25) серпень 2019 р. – С.68-73

5. Рибальченко Л.В., Рижков Е.В., Тютченко С.М., Гавриш О.С., Варяниченко А.О. Колективна монографія «Безпека підприємництва». Монографія. ДДУВС. 2020. - 180 с.

Торопов А.О. магістр групи М-ПД-921
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник: Рибальченко Л.В.
кандидат економічних наук, доцент
Дніпропетровського державного
університету внутрішніх справ

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

Персональні дані - інформація про набір інформації, за якою можна ідентифікувати особу, загальне та особливі ознаки категорії:

Загальні категорії включають - відповідальність, ім’я, батьки, адресу, телефони, паспортні дані, освіта, сімейний стан, економічний та фінансовий статус, дані про майно, банківські дані, підпис, дані з актів цивільного стану.

До особливих категорій відносин - расового, етнічного та національного походження, політичних, членства в політичних партіях та організаціях, профспілках, релігійних організацій громадських організацій глобальної спрямованості, релігійних та світових вірувань, даних та місця народження, персональних даних про майно та немайнові відносини.

Особистості з іншими особами професійної, ділової, особливої родини, а також інформація про підрозділи та явища, що відбулися або були створені в

побудованій, іншій, товариській, державній охороні здоров'я, матеріальній станції, місці проживання та проживання в інших районах життя людини.

Про «захист персональних даних» на фізичних осіб. Закон застосовується до фізичних та юридичних осіб, які здійснюють будь-які дії або сукупність дій, таких як збір, реєстрація, накопичення, зберігання, адаптація, модифікація, поновлення, використання та розповсюдження (розповсюдження, продаж, передача), знеособлення, знищення персональні дані, в тому числі із застосуванням інформаційних (автоматизованих) систем.

Закон може не застосовуватися, якщо дані обробляються:

- особа виключно для особистих чи побутових потреб;
- виключно для журналістських та творчих цілей за умови дотримання балансу між правом на повагу до приватного життя та правом на свободу вираження поглядів;
- щодо отримання архівної інформації репресивних органів.

Особисті дані є одними з найскладніших при роботі в цій галузі. Саме у визначенні містяться межі та критерії віднесення певної інформації до цієї категорії. Аналізуючи визначення, що містяться у національних та міжнародно-правових актах, слід зазначити, що вони здебільшого збігаються. Наприклад, у Конвенції Ради Європи 1981 року про захист фізичних осіб щодо автоматичної обробки персональних даних цей термін визначається як: "будь-яка інформація, що стосується конкретної особи або особи, яку можна конкретно ідентифікувати".

На наш погляд, ми повинні погодитися з визначенням, яке міститься в Законі, де персональні дані визначаються як: "інформація або сукупність інформації про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована". Це визначення є досить стислим і чітким і відповідає існуючим міжнародним підходам до розуміння цього поняття.

У 2017 році Європейський Союз профінансував проект «Twinning Ombudsman», щоб допомогти Україні привести свою систему захисту даних у відповідність з міжнародними та, зокрема, європейських стандартів. У листопаді 2018 року ініціатива завершила свою роботу. Команда проекту підготувала більше десятка рекомендацій і методик для ефективної реалізації реформи, але проект законодавчого акту так і не був внесений в український парламент.

Всупереч вироблені рекомендацій, етап реалізації публічно не висвітлювався, тому можна тільки задатися питанням, чому проект провалився. Можливо, тоді не було політичної волі. На жаль, два роки по тому результати роботи проекту так і не використовуються.

Справедливо розглядати Україну як один з провідних аутсорсингових центрів у Східній Європі, який володіє потужними відділами досліджень і розробок і охоплює всі стадії розробки програмного забезпечення. Це також рідна країна для ряду провідних світових стартів, від Grammarly і Preply до Gitlab і People.ai.

Огляд діючої законодавчої бази

Україна є членом Ради Європи з 1995 року, тому українське національне законодавство враховує розробки і стандарти, розроблені Радою. Зокрема, в 1997 році Україна ратифікувала Європейську конвенцію про права людини. Конвенція

108 була ратифікована в 2010 році. Після ратифікації Україна прийняла Закон України «Про захист персональних даних», який багато в чому ґрунтувався на положеннях Конвенції 108 до Директиви ЄС про захист даних від 1995 року і відображає більшість їх положень.

З тих пір в закон були внесені лише незначні зміни, в основному стосуються регулюючого органу і системи обов'язкових повідомлень наглядових органів. Після реформи захисту даних ЄС в 2016 році важко стверджувати, що Україна надає відповідні гарантії конфіденційності.

Наглядовий орган: проблеми і труднощі

На сьогоднішній день нагляд і контроль за захистом даних в Україні здійснює Уповноважений Верховної Ради з прав людини. Комісар є не окремим органом із захисту даних, а парламентським омбудсменом, який здійснює нагляд за захистом прав людини в цілому. У 2019 журналістська організація «Українська правда» зробила офіційний запит про склад секретаря уповноваженого і опублікувала отриману відповідь. Відділ захисту персональних даних складався всього з 13 чоловік, а його бюджет становив не більше 150 000 євро. З населенням більше 41 мільйонів чоловік відділ з 13 чоловік не в змозі належним чином контролювати захист персональних даних. Наприклад, в 2018 році регулюючий орган Великобританії Управління комісара за інформацією - збільшив штат до 700 осіб, щоб мати можливість виконувати весь обсяг роботи.

Інше питання: основна роль комісара полягає в здійсненні парламентського контролю. Концепція парламентських омбудсменів має на увазі непряму залежність і підзвітність українському парламенту, Верховній Раді як у функціональному, так і в організаційному аспектах. У той же час орган, який регулює недоторканність приватного життя, повинен нести відповідальність за нагляд не тільки за приватним, але і за державним сектором, включаючи виконавчу, судову і законодавчу гілки влади, тому максимально можлива незалежність є ключем до діяльності органу.

Таким чином, поточного забезпечення конфіденційності в Україні як і раніше не вистачає ресурсів і незалежності. Такої ж думки дотримуються і представники Ради Європи, які проаналізували заплановану реформу захисту даних в Україні в 2018 році. А оскільки в проекті реформи пропонувалося залишити комісара в якості єдиного наглядового органу, представник Ради Європи висловив стурбованість тим, що Україна не скористалася можливістю створити незалежний і непідлегла регулюючий орган.

Використані джерела:

1. Положення про Державну службу України з питань захисту персональних даних [Електронний ресурс]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/390/2011#Text

2. Щодо згоди на обробку персональних даних [Електронний ресурс]. - Режим доступу: https://zakon.rada.gov.ua/rada/show/v-302736-12#Text

3. Рибальченко Л.В., Косиченко О.О. Проблеми безпеки персональних даних в Україні / Л.В. Рибальченко, О.О. Косиченко // Регіональна економіка та управління / Запоріжжя. 2019. – С.57-62

Волошина В.С. магістр групи М-ПД-922
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник: Рибальченко Л.В.
кандидат економічних наук, доцент
Дніпропетровського державного
університету внутрішніх справ

ОСОБЛИВОСТІ ЕКОНОМІЧНОЇ БЕЗПЕКИ ДЕРЖАВИ

На сучасному етапі розвитку та глобалізації питанням економічної безпеки приділяється чи немало уваги, але подолання та вирішення у різних країнах світу не схоже один на одного. Стан досліджень, на даний момент, статики та динаміки економіки в Україні дає можливість дійти до висновку, що наша країна перебуває у стані глибокої економічної кризи.

Хоча, станом на сьогодні винесено дуже багато питань щодо вивчення проблем пов'язаних з економікою їх прогресивне вирішення знаходиться на організаційному процесі, водночас, залишається багато невирішених проблем у теорії та практиці економічної безпеки, що є чи не найголовнішою складовою безпеки нашої держави.

Не дивлячись на вище викладене, ситуацію погіршує відсутність систематизації стосовно понятійного апарату у даному напрямку, а також конкретних пропозицій щодо використання нових методів та моделей управління економічною безпекою та економікою в цілому.

Кінцевою метою системи економічної безпеки є підтримка сталого розвитку країни та захисту економічних інтересів, як громадян, так і країни, зменшення й уникнення ризиків їх життєдіяльності в поточному результаті – встановлення найбільш можливого стану безпечного економічного середовища.

У системі державної безпеки економічна безпека здійснює чітко сформульовані функції. Її природа полягає в тому, що вона є матеріальною основою національної суверенності. Тобто, економічна безпека – це комплекс дієвих заходів офіційних державних органів, які забезпечують стійкість до зовнішніх та внутрішніх загроз, характеризують здатність національної економіки до розширеного самовідтворення та задоволення потреб громадян, суспільства і держави на певному визначеному рівні та часовому проміжку [1].

Наразі основними загрозами економічній безпеці України виступають:

- скорочення валового внутрішнього продукту;
- низька конкуренція (конкурентноспроможність продуктів);
- корупція;
- критичний стан захищеності основних засобів;
- нерівномірності розвитку територій та населення;
- витік капіталу за кордон.

Сучасний розвиток економіки держави – це рівень взаємопроникнення в економіку інших держав в умовах дотримання вимог гіперконкуренції.

Створення умов і факторів економічної безпеки повинно забезпечити належне середовище для інвестицій та інновацій, удосконалення виробництва, підвищення продуктивності та конкуренції на робочих місцях [2].

Особливою рисою економічної безпеки є те, що вона постійно відображає рівень ефективності функціонування усіх її структкрних елементів, що дозволяє своєчасно виявити загрози та уникнути їх, і запобігти небезпеці завдання збитків держави [3].

Отже, з огляду на суперечності та інтеграційні тенденції сьогодення, особливе місце належить проблемі економічної безпеки держави як основи забезпечення її суверенітету, конкурентоспроможності, обороноздатності, підтримання соціальної злагоди в суспільстві, органічного входження країни в систему світової економіки. Зазначимо, що відсутність єдиного розуміння суті економічної безпеки та визначення її складових як в науковій літературі, так і в нормативноправовій базі, породжує низку суперечностей та зумовлює актуальність подальших наукових розробок у цій сфері.

Використані джерела:

1. Про стратегію національної безпеки України : Указ Президента України від 26.05.2015 р. № 287/2015. – [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/287/2015.

2. Груб З. В. Економічна безпека України в сучасних умовах /З.В. Груб // Державне управління. 2018. - №2 – С. 97-101.

3. Rubalchenko L., Ryzhkov E. Ensuring enterprise economic security. Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs. 2019. Special ISSUE №1.- P.268-271

Мороз В.Ю. магістр групи М-ПД-922
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник: Рибальченко Л.В.
кандидат економічних наук, доцент
Дніпропетровського державного
університету внутрішніх справ

УПРАВЛІННЯ ЕКОНОМІЧНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА

Економічна безпека становить собою динамічний інститут, який, використовуючи свої економічні та політичні властивості в ринковій системі господарювання, здійснює функції різнопланового забезпечення ефективної економічної діяльності всіх підрозділів та підсистем, функції по формуванню та підтримці відповідної конкурентоспроможності та функції захисту економічних інтересів у разі неефективного функціонування економіки.

Під управлінням економічною безпекою фірми розуміється комплекс взаємопов'язаних процесів планування, організації, стимулювання і контролю, які забезпечують економічну безпеку фірми. Систему заходів із забезпечення економічної безпеки підприємства необхідно погоджуватися з цілями діяльності підприємства і ресурсами, які є на конкретній фірмі. Місія підприємства, основні цілі і комплекс заходів із забезпечення ступеня його економічної безпеки повинні мати вектори схожої направленості. Тільки на основі виявлення інтересів підприємства й їх гармонізації з суб'єктами зовнішнього оточення, що взаємодіють із останнім, можливе забезпечення економічної безпеки. Така гармонізація розглядається як форма активного захисту уважності підприємства.

Економічна свобода підприємства є уразливою до внутрішніх та зовнішніх загроз і при цьому може змінюватися в бажаному напрямі під впливом упорядкованої сукупності керівних дій менеджменту підприємства протягом певного проміжку часу, керованість економічної безпеки компанії має залежати від списку позицій. По-перше, важливою умовою керованості економічної безпеки є вибір критерію якості, який, передовсім, повинен характеризувати властивості стійкості керованої системи. Якщо керована система не буде стійкою, то достатньо виникнення одиничної загрози, щоб її безпека була істотним чином порушена. По-друге, керованість системи залежить від безлічі можливих значень вхідних параметрів. Загалом, що ширше безліч можливих значень вхідних параметрів, то при слабкіших критеріях досягатиметься керованість.

Із характерною для сучасних умов підвищеною нерівномірністю розвитку зовнішнього і внутрішнього середовищ підприємств повинна розширюватися і стрімкість збору, аналізу, ступінь важливості інформації, а також коректуватися темп прогнозування і самі методи ухвалення зовнішньоекономічних рішень. Необхідно особливо підкреслити, що в будь-якій концептуальній моделі управління підприємством часовий аспект управління доцільно виділити в особливий блок. Інакше управлінська реакція свідомо ризикує відстати від реальної політичної динаміки, через що стане неможливим не тільки випереджальне стратегічне управління, але й ефективний контроль за наслідками розвитку ризикової ситуації, особливо на етапі її переростання в кризу. Дана умова потребує більш уважного розгляду взаємозв’язку керованості економічною безпекою підприємства і рівнем його організаційної зрілості. До керованості економічної безпеки підприємства як до об’єкта управління має бути висунутий контракт, який, зумовлений природою економічної безпеки фірми. Під вимогою може розумітися дія, умова або конкретний документ.

У межах даного дослідження під вимогами до керованості економічної безпеки підприємства розуміються певні умови, яких має виконувати менеджмент підприємства при управлінні економічною безпекою підприємства, що можуть бути зафіксовані в його внутрішній справі. До головних зобов'язань належать:

•кількісна оцінка;
• прийнятність;
• гнучкість;
• адаптивність;

• динамічність;
• прогнозованість;
• прозорість;
• результативність;
• економічність;
• соціальна відповідальність.

Соціальна відповідальність як вимога до керованості економічної безпеки підприємства є обопільно гострою необхідністю, тобто спрямованість у зовнішнє, та внутрішнє середовище. Для України важливим є започаткування умов для розвитку соціальної відповідальності. Сьогодні концепцію соціальної відповідальності поширюють та намагаються інтегрувати у свою ділову активність, насамперед, усі великі вітчизняні підприємства, банки, корпорації. Водночас вона також має істотний вплив на малий та середній бізнес, сталий роз виток суспільства.

Таким чином, механізм управління економічною безпекою доцільно розділити на такий, що забезпечує попереджуванні рекомендації щодо впливу, та механізм антикризового управління. Рекомендації для управлінням економічною безпекою підприємства є проектування плану його розвитку, аналіз, передчуття, проектування необхідності основних змін і своєчасне реагування на події.

Використані джерела:

1. Ляшенко О.М. Концептуалізація управління економічною безпекою підприємства / Монографія 2-ге видання, перероблене/ Київ 2015. - [Електронний ресурс]. — Режим доступу: http://old2.niss.gov.ua/content/articles/files/lyashenko_1_druk-43fc7.pdf

2. Рибальченко Л.В., Рижков Е.В., Тютченко С.М., Гавриш О.С., Варяниченко А.О. Колективна монографія «Безпека підприємництва». Монографія. ДДУВС. 2020. - 180 с.

Дудник В.В. – студентка 1 курсу юридичного факультету
Науковий керівник: Синиціна Ю.П. доцент кафедри економічної та інформаційної безпеки, к.т.н., доцент (Дніпропетровський державний університет внутрішніх справ, м Дніпро)

АКТУАЛЬНІ ПИТАННЯ ВЗАЄМОЗВ'ЯЗКУ ІНФОРМАЦІЙНОЇ ТА НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

В умовах сучасних глобальних та регіональних інформаційних протистоянь, деструктивних комунікативних впливів, зіткнення різновекторних національних

інформаційних інтересів, поширення інформаційної експансії та агресії, захист національного інформаційного простору та гарантування інформаційної безпеки стають пріоритетними стратегічними завданнями сучасних держав у системі глобальних інформаційних відносин.

Збереження інформаційного суверенітету, формування ефективної системи безпеки в інформаційній сфері є актуальною проблемою і для України, яка часто є об'єктом зовнішньої інформаційної експансії, маніпулятивних пропагандистських технологій та руйнівного інформаційного вторгнення.

В умовах російсько-українського конфлікту захист національного інформаційного простору від негативних інформаційно-психологічних впливів, операцій та війн, гарантування інформаційної безпеки та інформаційного суверенітету набувають особливого значення і стають чинниками збереження національної ідентичності України та функціонування її як суверенної та незалежної держави [1, с. 25]. Існує два аспекти трактування інформаційної безпеки у контексті національної безпеки. З одного боку, інформаційну безпеку розглянуто як самостійний елемент національної безпеки будь-якої країни, а з іншого – інтегрована складова будь-якої іншої безпеки: військової, економічної, політичної тощо. Найповнішим є таке визначення: інформаційна безпека – це стан захищеності життєво важливих інтересів особистості, суспільства і держави, за якого зводиться до мінімуму завдання збитків через неповноту, невчасність і недостовірність інформації, негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації [2, с. 35]. Це визначення є оптимальним та відображає усі аспекти взаємодії суб'єктів інформаційних відносин. Увага до проблем гарантування інформаційної безпеки України зумовлена антиукраїнськими впливами, які пропагують ідеї сепаратизму, насильства, національної ворожнечі і є спробами руйнування національної ідентичності України, знищення міжнаціональної злагоди, посягання на конституційний лад України, територіальну цілісність держави. Проблема гарантування інформаційної безпеки України актуалізується в умовах війни на Сході, коли з боку Російської Федерації відбувається інформаційна експансія, упереджене та тенденційне висвітлення фактів та явищ, а технології російських інформаційно-психологічних операцій спрямовані на забезпечення домінування в українському (а також у глобальному) інформаційному просторі та на утримання медійної переваги. Через російські пропагандистські інформаційно-психологічні кампанії, акції, медіа заходи відбувається вплив не лише на суспільну свідомість громадян України, а й на світову громадськість [3, с. 4]. Основні напрями інформаційно-психологічних атак проти України наведені на рис. 1.

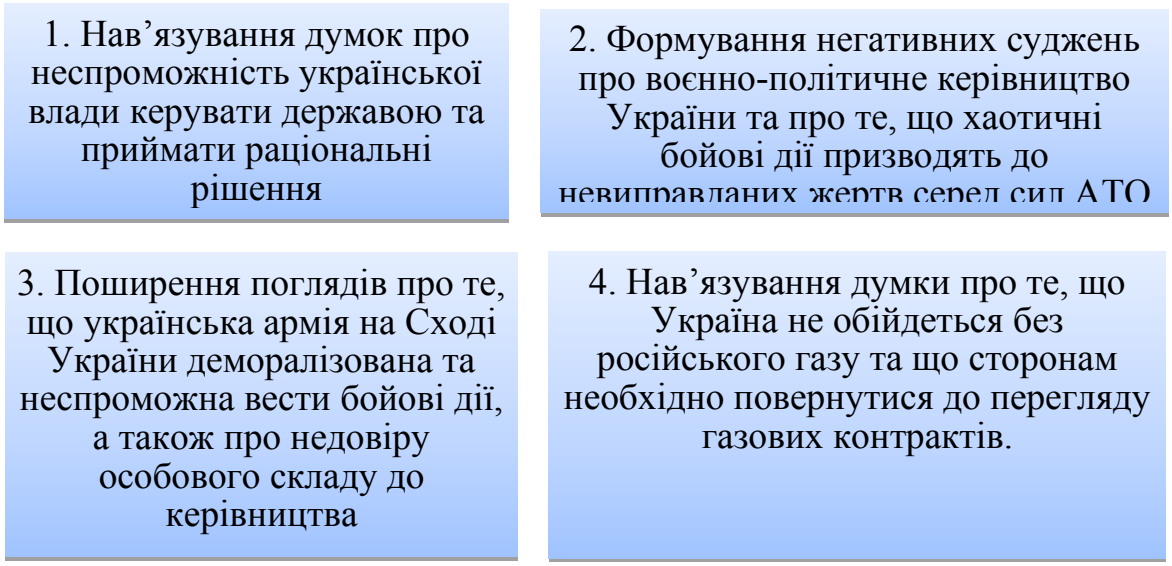


Рис. 1. Основні напрями інформаційно-психологічних атак проти України

Експерт зазначає, що цільовою аудиторією Кремля зараз є населення РФ, російськомовна діаспора за кордоном, населення України, зокрема в окупованих районах Донбасу, громадяни західних країн, а також країн БРІКС та Митного союзу, близькі Росії за політичними поглядами [3, с. 6].

Україна стала об'єктом інформаційно-психологічних впливів, операцій, війн та її інформаційна безпека опинилась під загрозою. Світова громадськість відчуває брак інформації або отримує її з інших джерел, які часом дезінформують, надають викривлену, спотворену, неповну інформацію.

Основні напрями негативних впливів на інформаційний простір України наведені на рис. 2.

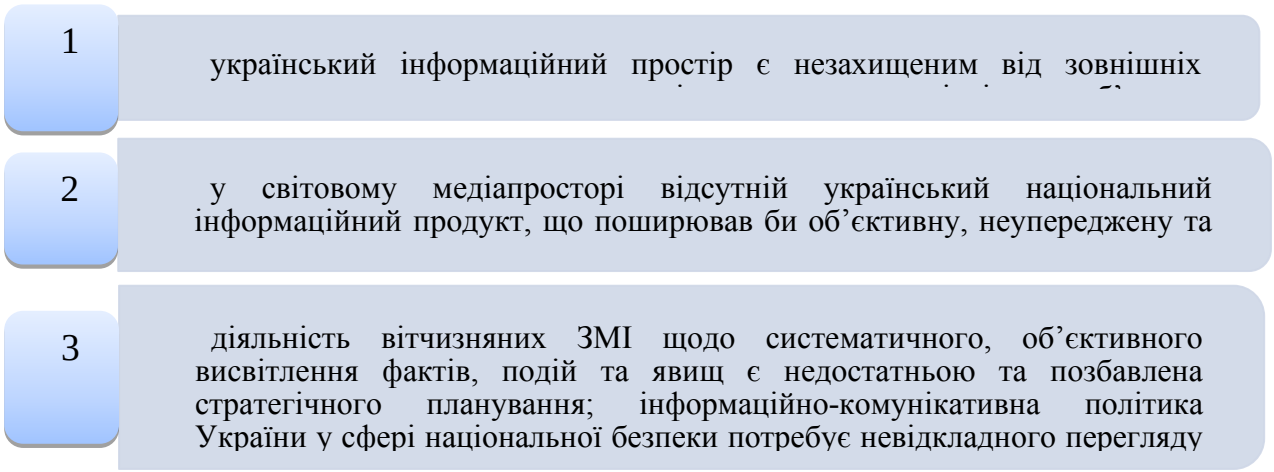


Рис. 2. Основні напрями інформаційно-психологічних атак проти України

Водночас проти України активно застосовується потужний медіаресурс, здійснюється експансія іноземних суб'єктів на ринку інформаційних послуг, активізуються негативні інформаційні впливи, які спрямовані на викривлення реальності, заниження міжнародного іміджу держави. Рівень інформаційної безпеки держави, значною мірою, зумовлений рівнем її інформаційної інфраструктури. На жаль, як зазначає В. Петрик, низький загальний рівень інформаційної

інфраструктури України сприяє експансії іноземними компаніями ринку інформаційних послуг, що створює сприятливі умови для перерозподілу ефірного часу на користь іноземних програм, окремі з яких засмічують український інформаційний простір своїм баченням подій, пропагують спосіб життя та традиції, тим самим деструктивно впливаючи на суспільство і державу, руйнуючи морально-етичні основи генофонду української нації.

Недостатній професійний, інтелектуальний і творчий рівень вітчизняного виробника інформаційного продукту та послуг, його не конкурентоспроможність не лише на світовому ринку, а й в Україні, призводить до того, що українська аудиторія, природно, віддає перевагу іноземним інформаційним програмам. Недостатній контроль з боку держави за дотриманням законів України політичними силами, ЗМІ та окремими особами, які займаються підприємницькою діяльністю в інформаційній сфері, призводить до того, що нині трапляються непоодинокі випадки надання ефірного часу теле- та радіопрограм, спрямованим на руйнування моральних цінностей, свідомості української нації.

З метою протидії негативним впливам інформаційної пропаганди та інформаційних війн, задля нейтралізації та упередження реальних та потенційних загроз в інформаційному просторі України виникає необхідність удосконалення нормативно-правового забезпечення та запобігання й нейтралізації потенційних і реальних загроз національній безпеці в інформаційній сфері.

Використані джерела:

1. Почепцов Г. Сучасні інформаційні війни / Г. Почепцов. – К.: Вид. дім «Києво-Могилянська академія», 2015. – 497 с.

2. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції [Текст] : навч. посіб. / В. А. Ліпкан, Ю. Є. Макименко, В. М. Желіховський. – К.: КНТ, 2006. – 345 с.

3. Медвідь Ф. Інформаційна безпека України: виклики та загрози Електронний ресурс. – Режим доступу. URL: http://www.nato.ru. if.ua/journal/2009-2-28.pdf.

Староконь Ю.М. – студентка 1 курсу юридичного факультету
Науковий керівник: Синиціна Ю.П. доцент кафедри економічної та інформаційної безпеки, к.т.н., доцент (Дніпропетровський державний університет внутрішніх справ, м. Дніпро)

РОЛЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ СУЧАСНОГО СУСПІЛЬСТВА

Мабуть, кожен студент замислюється над тим, навіщо він вивчає той чи інший предмет. Також і всі люди в нашому суспільстві хоч раз замислювались, навіщо нам

ті чи інші поняття, сфери діяльності тощо. Теж саме з інформаційною безпекою, не всі люди усвідомлюють її важливість в нашому житті.

Інформаційна безпека є однією із найсуттєвіших складових частин національної безпеки країни, її забезпечення, завдяки послідовній реалізації та бездоганно сформульованій інформаційній стратегії, значною мірою сприяла б забезпеченню досягнення успіхів при вирішенні проблем з політичної, військово-політичної, військової, соціальної, економічної та інших державних сфер діяльності.

Вивченням ролі держави у формуванні інформаційного суспільства займаються такі вчені, як Арістова І. [1], Почепцов Г. [2] та ін. Ряд публіцистів Супрун В. [3], Ярочкін В. [4] розробили основні принципи забезпечення інформаційної безпеки. В той же час,окремого дослідження вимагають структурно-функціональні аспекти процесу гарантування інформаційної безпеки.

Поняття інформаційна безпека можна розглядати з двох сторін. З одно боку, це захищеність інформаційного середовища суспільства, що забезпечує його формування, використання та розвиток в інтересах громадян, організацій чи держави. А з іншого боку, інформаційна безпека - це стан захищеності потреб в інформації певної особи, суспільства, держави, при якому забезпечується їх існування та розвиток, що не залежить від наявності зовнішніх та внутрішніх інформаційних загроз. Інформаційним середовищем називають сферу діяльності суб'єктів, пов'язану зі створенням, обробленням й споживанням будь-якої інформації.Стан інформованості визначає ступінь адекватності сприйняття суб'єктами дійсності, і як наслідок – обґрунтованість прийняття будь-яких рішень та дій [5]. В правових аспектах інформаційна безпека – це одна із сторін розгляду інформаційних відносин, в межах інформаційного законодавства з позиції захисту життєво необхідних інтересів певної особистості, суспільства чи держави. Акцентування уваги на можливих загрозах, цим інтересам і на механізмах усунення або запобігання цих загроз суто правовими методами. Принципи забезпечення інформаційної безпеки містять: законність, баланс інтересів особи, суспільства і держави, комплексність, системність, інтеграція з міжнародними системами безпеки, економічна ефективність (рис. 1).

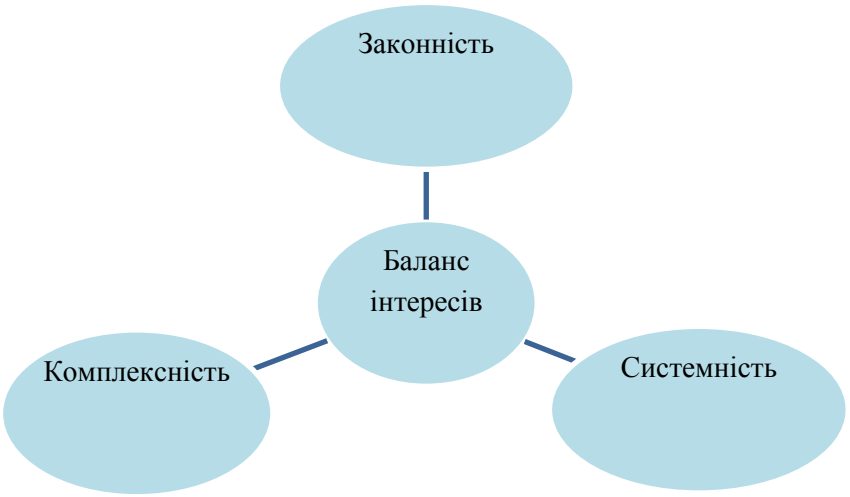


Рис. 1. Принципи забезпечення інформаційної безпеки

Об’єктами інформаційної безпеки можуть бути: свідомість та психіка людини, інформаційні системи різного масштабу та призначення. Соціальних об’єктами інформаційної безпеки є: особистість, колектив, держава, суспільства, світове товариство.

До суб’єктів інформаційної безпеки відносять: державу, що здійснює свої функції через відповідні органи; громадян; суспільні або інші організації та об’єднання, яка володіють повноваженнями стосовно забезпечення інформаційної безпеки відповідно до чинного законодавства (рис. 2).

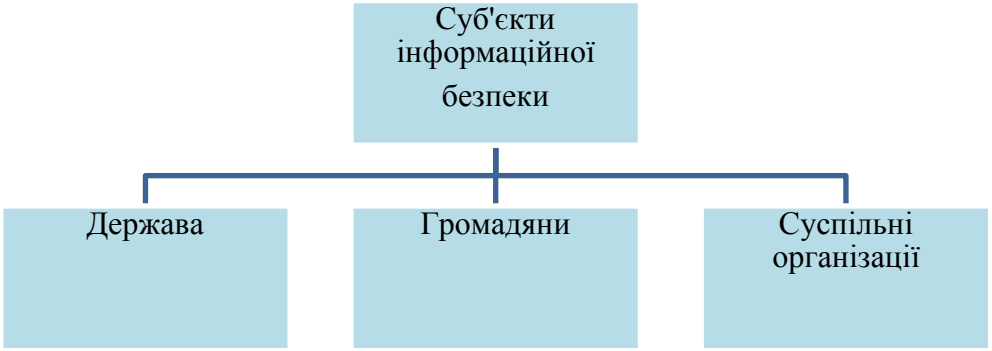


Рис. 2. Складові інформаційної безпеки

Інформаційну безпеку поділяють на інформаційну безпеку особистості та інформаційну безпеку держави.

Інформаційна безпека особистості – це захищеність психіки та свідомості людини від небезпечного інформаційного впливу - маніпулювання свідомістю: дезінформування, спонукання до образливих дій, самогубства тощо.

Інформаційна безпека держави - міра захищеності держави чи державного суспільства, стійкості основних сфер життєдіяльності (економіки, науки, технологічної сфери, сфери управління, військової справи тощо), відносно небезпечних інформаційних впливів. Інформаційна безпека держави характеризується здатністю протистояти цим впливам.Концепція інформаційної безпеки держави – це систематизована сукупність відомостей про інформаційну безпеку держави та шляхи її забезпечення. В рамках цієї концепції проводиться системна класифікація руйнівних факторів та інформаційних загроз безпеці особистості, суспільства, держави; обґрунтовують основні положення з організації забезпечення інформаційної безпеки держави; розробляються пропозиції стосовно способів і форм забезпечення інформаційної безпеки.

Загрози інформаційній безпеці – сукупність умов і факторів, що створюють небезпеку життєвонеобхідним інтересам особистості, суспільства й держави в інформаційній сфері. Загрози інформаційній безпеці поділяються на три основні групи (рис 3): загрози впливу неякісної інформації (недостовірної, фальшивої, дезінформації) на особистість, суспільство, державу; загрози несанкціонованого й неправомірного впливу сторонніх осіб на інформацію і інформаційні ресурси, їх виробництво, формування й використання; загрози інформаційним правам і свободам особистості (праву на виробництво інформації, її поширення, пошук,

одержання, передавання та використання; праву на інтелектуальну власність на інформацію, в тому числі й речову).

Дестабілізуючі фактори - це явища або процеси, які породжують інформаційні загрози. Джерелами дестабілізуючих факторів можуть бути як окремі особи, так й організації та їх об'єднання. Особливу групу джерел складають інформаційні системи та засоби, так як вони одночасно є знаряддями приведення в дію інформаційних загроз, каналом їхнього проникнення у свідомість особистості або суспільну свідомість і творцем загроз, що виникають внаслідок технічних несправностей або інших причин.

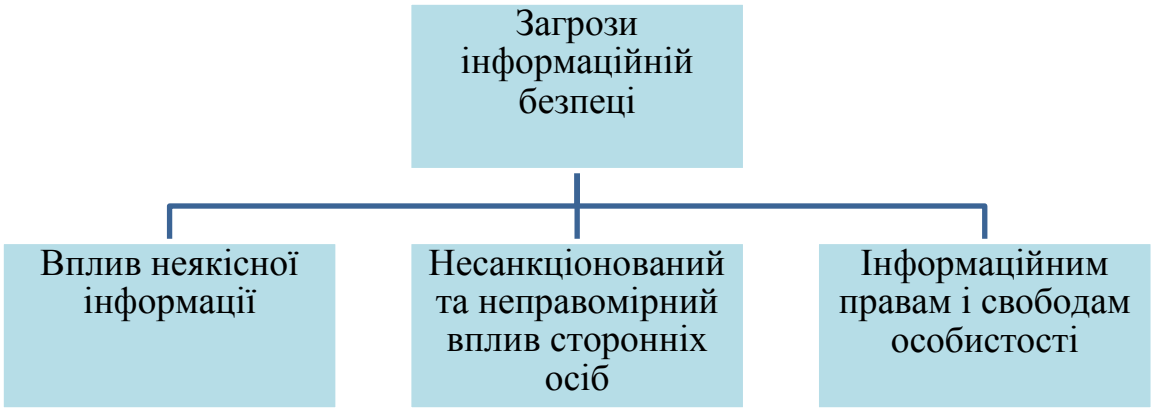


Рис. 3. Класифікація загроз інформаційної безпеки

Джерелом дестабілізуючих факторів також може бути природне середовище. Кожному джерелу властиві певні види дестабілізуючих факторів, які можна подати у вигляді міждержавних і внутрішньодержавних.До внутрішньодержавних дестабілізуючих факторів відносять: правовий вакуум у більшості питань забезпечення інформаційної безпеки, порушення законодавства з питань інформаційної безпеки, політичні конфлікти, відмови, збої, технічні помилки інформаційних засобів, природні явища, що ускладнюють передачу, прийом і зберігання інформації або руйнують інформаційні системи.Міждержавні дестабілізуючі фактори – це конфлікти різноманітних масштабів і проявів (в економіці, політиці, ідеології, дипломатії тощо).

Отже, як висновок я хочу сказати що інформаційне суспільство може існувати тільки лише за умови, що його члени оволодіють інформаційною культурою – будуть дотримуватись етичних норм поведінки в інформаційному просторі. Це сформує інформаційний захист кожної людини та суспільства у цілому. Формування інформаційного середовища не у відповідності з глобальними законами функціонування природних систем може наблизити критичну ситуацію на планеті не менш, ніж ядерна загроза. Інформація вже стала стратегічним озброєнням. Тому кожна людина мусить знати, що коли вона вносить нову інформацію в інформаційний простір, вона тим самим керує формуванням інформаційного середовища людей, тобто безпосередньо впливає на свідомість та розвиток інших людей. Кожен новий блок інформації, який надходить в інформаційне середовище людства, повинен мати правила безпечного користування. Як окрема людина, так і суспільство в цілому має можливість запобігати інформаційних небезпек, завдяки

формуванню інформаційного щита: системи цінностей, яка орієнтована на глобальні принципи безпеки життєдіяльності людства [6].

Використані джерела:

1. Арістова,І.В.Діяльність органів внутрішніх справ щодо реалізації державної інформаційної політики : монографія [Текст] / І. В. Арістова. –Х. : Нац. ун-т внутр. справ, 2006. –354 с.
2. Почепцов Г.Г., Чукут С.А. Інформаційна політика: навч. посіб. — Київ: Знання, 2006. – 665 с.
3. Suprun, V.M. Information sovereignty as part of information security: theoretical and legal aspects. Електронний ресурс. URL: http://www.nbuv.gov.ua/portal/natural/vkhnu/Pravo/2009.
4. Yarochkin, V. The security system company. Електронний ресурс. URL: http://www.nbuv.gov.ua.
5. Костецький Р. Інформаційна безпека особистості: Інформаційна безпека Електронний ресурс. URL: https://sites.google.com/site/infobezpekaosobu/informacijna-bezpeka
6. Варивода К.С. Інформаційна безпека підлітків в Інтернет мережі / К.С. Варивода // Молодий вчений. – 2016. – № 3. – С. 365-368. Електронний ресурс. URL: http://molodyvcheny.in.ua/files/journal/2017/9.1/10.pdf

Стеценко В.В., курсант
Травина Д. В., курсант
Науковий керівник: Богучарова О.І.
професор кафедри юридичної лінгвістики
та практичної психології,
доктор психологічних наук, доцент
Луганського державного університету
внутрішніх справ імені Е.О. Дідоренка

ХМАРНІ ТЕХНОЛОГІЇ У ФОРМУВАННІ МЕДІАЦІЙНОЇ КОМПЕТЕНТНОСТІ МАЙБУТНІХ ПРАВООХОРОНЦІВ

Осмислення та подальша імплементація у вітчизняну правову систему програм відновного правосуддя, особливо в частині роботи з дітьми, наприклад, відпрацювання та захист виявлених жертв жорстокого поводження, шкільного булінгу, експлуатації і торгівлі людьми (підлітки і жінки) має на меті, звісно, відновлення справедливості та збалансування потреб потерпілого, правопорушника та громади. Проте, не менш важливим у всіх таких випадках є також намагання

правоохоронців зробити основну оперативну діяльність ефективнішою, зокрема, завдяки удосконаленню інформаційної обробки факту правопорушення, чи навіть, злочину. На Заході ці сучасні інформаційні технології отримали назву «кейс-менеджменту». Інформаційне удосконалення за технологією кейс-менеджменту передбачає перехід від звичайної фіксації в ЄРДР на електронні бази даних і платформи, в яких зафіксовано дані жертв, винуватців, їх відбитки пальців щодо кожного окремого кейсу домашнього чи шкільного насилля або торгівлі людьми, з тим, щоб якісно провести етап досудового розслідування та підготувати матеріали до акцій медіації.

Звертаючись до організаційних процедур медіації, або відновного правосуддя варто зазначити, що цей тип правосуддя може існувати в таких основних формах: програми примирення (посередництво чи медіація) між потерпілою стороною, правопорушником за участі посередника (медіатор); сімейні конференції переважно до неповнолітніх, в яких беруть участь також члени сім'ї сторін, родичі; кола правосуддя, де крім сторін включено представників громади, а також представників суду та прокуратури [1, с.202; 2, с.258]. Очевидно усі організаційні процедури медіації потребують інформаційного забезпечення, нових технологій, систем бази даних.

У практиках медіації, або відновного правосуддя на Заході інформаційне забезпечення і бази даних, як правило, створюють благодійні організації, Міністерства соціальної політики та підвідомчі їм структури, міжнародні установи тощо. Притому усі ці структури можуть надавати доступ до цього інформаційного забезпечення поліції у разі необхідності, хоча в поліцейських структурах теж можливі аналогічні бази даних щодо зазначених випадків, щоправда, менші за обсягом. Наприклад, такою загальною базою даних є EURODAC, в якій зберігаються відбитки пальців прохачів притулку і нелегальних мігрантів у країнах-учасницях ЄС; система управління інформацією про захист дітей CPIMS+, яку використовують ЮНІСЕФ; внутрішня система MaGIK Casebook, яка поширюється департаментом США з надання допомоги дітям. Узагалі технології сфери кейс-менеджменту, головним чином, передбачають використання управлінського програмного забезпечення, а також хмарних технологій та баз даних.

Зважуючи на три вищевказані основні форми відновного правосуддя, можна зазначити ті переваги, що здатні надати хмарні бази даних правоохоронцям?

По-перше, централізоване хмарне збереження інформації дозволяє отримати доступ до різних типів даних по конкретному кейсу, у тому числі перевірити причетність винуватця до інших випадків; по-друге, хмарні системи забезпечують доступ до інформації в польових умовах, у дорозі через звичайне підключення до Інтернету. Крім того, процеси опрацювання отриманих даних у хмарних технологіях стають простіші завдяки розміщенню усієї інформації в центральне цифрове сховище, що підвищує ефективність управління інформацією. Також у хмарній системі можливі додаткові опції, як-от автоматичного відслідковування факту правопорушення (кейсу) і відправлення своєчасних нагадувань для фіксації та правового супроводу. І головне, як правило, системи хмарних технологій впроваджуються на рівні декількох відомств та служб, що дозволяє залучити не лише батьківську громадськість чи родичів обох сторін, а й соціальних працівників

із служби захисту дітей, спеціалістів у сфері охорони здоров'я або підтримки психічного здоров'я та реабілітації жертв злочинів, учителів, громаду міста чи центру, адвокатів, суддів, прокурорів. Звісно, хмарні технології це вартісне впровадження, яке потребує необхідних компетенцій у співробітників правоохоронних органів, опанування компетенціями з хмарних технологій курсантами ще в стінах ЗВО з специфічними умовами навчання, також й адаптації стандартних робочих процедур до нової хмарної системи збереження інформації.

Застосування альтернативних методів вирішення складних життєвих ситуацій із захисту дітей, підлітків, жінок у різних програмах за загальновизнаних міжнародних стандартів, особливо в сфері кримінального судочинства, вимагає поступово змінювати «парадигму покарання» на «відновну парадигму». Оскільки суть останньої полягає в тому, що завданням кримінальної юстиції повинно бути не покарання винного, а відновлення права особи, що постраждала від злочину, тому медіація має стати дієвою нормою. І нарешті, щоб розрізнити випадки, які дійсно перспективні з точки зору створення умов для примирення потерпілих і правопорушників та усунення наслідків, спричинених злочином, необхідні ефективні системи сучасних інформаційних технологій, які дозволяють зберігати і отримувати інформацію, що гарантує актуальність і доступність даних по кожному випадку правопорушення. Отже, у підсумку відновне правосуддя, збагачене хмарними технологіями і компетенція ми правоохоронців створюють умови для соціальної реінтеграції правопорушника, психологічного і легалізованого шляху відновлення прав потерпілого, зменшення рецидиву та позбавлення громади від завеликої кількості кримінальних покарань та тюрем.

Використані джерела:

1. Зер Г. Зміна об'єктива: новий погляд на злочин та правосуддя / Г. Зер ; пер. з англ. М. Яковлєва. – К. : Унів. вид-во «Пульсари», 2004. – 224 с.

2. Райт М. Восстановительное правосудие – путь к справедливости / М. Райт ; пер. с англ. – К. : Издатель Захаренко В. А., 2007. – 304 с.

3. Медіація в судовій, правоохоронній та правозахисній системах. Мат-ли міжн. наук-практ. конф. (Одеса, 30-31 травня 2019 р.). – Одеса: ОДУВС, 2019. – 289 с.

Кліменко А.О. студентка 2 курсу юридичного факультету
Науковий керівник: Синиціна Ю.П. доцент кафедри економічної та інформаційної безпеки, к.т.н., доцент (Дніпропетровський державний університет внутрішніх справ, м. Дніпро)

АКТУАЛЬНІ ПИТАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

В сучасних умовах для оперативного та ефективного забезпечення діяльності поліції України, спрямованої на запобігання вчиненню правопорушень; виявленню причини та умов, що сприяють вчиненню правопорушень, а також протидії злочинності є комплексне застосування інформаційно-пошукових та інформаційно-телекомунікаційних систем, засобів та технологій, що потребує запровадження надійної системи інформаційної безпеки.

Вагомий внесок у розвиток фундаментальних теоретичних та методологічних засад інформаційного забезпечення в правоохоронній діяльності здійснили наступні науковці такі, як: Арістова І.В., Бандурко О.М., Бєляков К.І. та інш. Незважаючи на велику кількість наукових досліджень у даній сфері, питання використання сучасних інформаційних технологій в діяльності національної поліції України ще й досі є актуальним.

Інформаційна безпека - це стан захищеності систем обробки і зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації, або комплекс заходів, спрямованих на забезпечення захищеності інформації від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки, запису чи знищення [1].

На думку вченого Д.О. Красікова, забезпечення інформаційної безпеки правоохоронних органів України здійснюють за двома формами:

– організаційною (організація роботи правоохоронних органів, роботи, пов’язаної з обігом, збиранням, обробкою, зберіганням та використанням інформації, взаємодія працівників правоохоронних органів щодо забезпечення інформаційної безпеки);

– правовою (видання наказів та розпоряджень, розроблення положень, інструкцій, складання планів тощо) [2, с. 11–15].

Отже, узагальнено можна сказати, що інформаційна безпека - це статус безпеки систем обробки та зберігання даних, який може забезпечити конфіденційність, доступність та цілісність інформації, використання. По-друге, інформаційна безпека - це стан захисту інформаційних потреб людей, суспільства та країни, незалежно від існування внутрішніх та зовнішніх інформаційних загроз, інформаційна безпека може забезпечити їх існування та поступовий розвиток. Стан свідомості визначає достатність сприйняття навколишнього дійсності предметом, а отже, визначає ефективність прийнятих рішень і дій.

В інформаційному законодавстві, з точки зору захисту особистих інтересів, інформаційна безпека є одним із аспектів, що розглядають інформаційні відносини в рамках інформаційного законодавства. Об'єктами інформаційної безпеки можуть бути: свідомість, психологія людини; інформаційні системи різного масштабу та різного призначення. До соціальних об'єктів інформаційної безпеки належать особи, команди, країни, суспільство та міжнародне співтовариство. До тем інформаційної безпеки належать: держава, яка виконує свої функції через відповідні установи; громадяни, громадські чи інші організації та об'єднання, які мають право забезпечувати інформаційну безпеку відповідно до закону. Безпека персональної інформації полягає у захисті людської психології та свідомості від небезпечної інформації: маніпуляції свідомістю, дезінформація, підбурювання до образ, самогубство тощо.

Загрози інформаційній безпеці - низка умов та факторів, які загрожують життєво важливим інтересам окремих людей, суспільства та країни в інформаційному полі. Основні загрози інформаційній безпеці поділяються на три категорії:

- загрози впливу неякісної інформації (недостовірної, неправдивої, дезінформаційної) на окремих людей, суспільство та країну;
- загроза несанкціонованого та незаконного впливу третіх осіб на інформацію та інформаційні ресурси (системи їх виробництва, формування та використання);
- загрози інформаційним правам та особистій свободі (права на отримання інформації, розповсюдження інформації, пошук, отримання, передачу та використання; право знати, включаючи права інтелектуальної власності на власність)

Фактори загрози, розділені за видами, поділяються на політику, економіку, організацію та технологію

Явища, що породжують інформаційні загрози та процеси природного та штучного походження, називаються дестабілізуючими факторами. Джерелом руйнівних факторів також може бути природне середовище. Кожне джерело має певні типи нестабільності, яка може мати місце у міждержавній та побутовій формах.

До внутрішніх факторів дестабілізації належать: правовий вакуум у більшості питань інформаційної безпеки; порушення правил інформаційної безпеки; порушення законів та норм про інформаційну безпеку; політичні конфлікти; збої, відмови інформаційних систем, технічні помилки (засоби); природні явища, які ускладнюють передачу, прийом та зберігання інформації або руйнують інформаційні системи.

Інформаційна безпека розглядається як глобальне питання захисту інформації, інформаційного простору та інформаційного суверенітету, а також питання інформаційної підтримки урядових рішень. Фактично вирішувати питання інформаційної безпеки та переслідувати кожну державу за порушення або загрозу інформаційній безпеці відповідно до міждународного права,відповідних міжнародних договорів та національного законодавства. Інформаційна безпека регулюється певними міжнародним законами та нормативними актами, які

містяться в документах ООН та ЮНЕСКО, документах європейських організацій та нормативних актах різних країн.

Отже можна зробити висновок, що інформаційна безпека діяльності поліції України є однією із ключових в системі функціонування правоохоронних органів. Ефективна організація інформаційної безпеки в забезпеченні інформаційно-правової діяльності органів поліції України може бути здійснена завдяки виявлення загроз, внутрішніх та зовнішній факторів дестабілізації інформаційній безпеці, а також інтеграції інформаційних систем правоохоронних органів та систем безпеки всіх рівнів до єдиного інформаційного середовища на державному та міжнародному рівнях.

Використані джерела:

1. Піпа Н. Основні поняття інформаційної безпеки: Інформаційна безпека Електронний ресурс. URL: https://sites.google.com/site/osnovuib/

2. Красіков Д.О. Правове забезпечення інформаційної безпеки в діяльності органів внутрішніх справ України: автореф. дис. канд. юрид. наук: 12.00.07 / Д. О.Красіков. – К., 2012. – 20 с.

Антропов Б.О., курсант факультету підготовки фахівців для органів досудового розслідування Дніпропетровського державного університету внутрішніх справ
Науковий керівник: Рижков Е.В., завідувач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ, к.ю.н., доцент

ВИКОРИСТАННЯ МУЛЬТИМЕДІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ВДОСКОНАЛЕННЯ РІВНЯ ОСВІТНЬОГО ПРОЦЕСУ

У реаліях нашого часу спостерігається постійний розвиток новітніх технології, автоматизованих систем, програмних продуктів, які с кожним роком все більше і більше вдосконалюються і розповсюджуються як у світовому значенні так і у побутовому.

Крім того, багато держав світу у своїх навчальних закладах різних рівнів активно використовує новітні технології. Як показує світова практика застосування

технічних засобів з виходом до мереж Інтернет - поєднання навчання і технології збільшує цікавість здобувачів до навчання, підвищує його ефективність, а також спрощує засвоєння навчального матеріалу. Особливо це набуло своєї актуальності під час світової проблеми, коли освітні заклади закриваються на карантин і заняття проходять дистанційно.

Щодо використання мультимедійних технологій у процесі навчання, у світовому розумінні - це не новина. Проте, ми хочемо сконцентрувати свою увагу щодо використання сенсорних технологій touch IR, а саме - інтерактивної дошки [1]. Вказану технологію активно використовують у навчальних закладах оскільки це дуже сучасно і зручно, адже одним дотиком руки до поверхні, можна відкрити будь-який комп'ютерний додаток або сторінку в Інтернеті, продемонструвати потрібну інформацію або просто малювати. Також, важливою особливістю є те, що під час роботи з інтерактивною дошкою в навчальних закладах здобувач освіти засвоює інформацію не тільки через аудіальний та візуальний канали сприйняття, але й через естетичний канал, який майже не використовується в сучасній педагогіці. Тому здубувачі, які недоотримали інформацію через цей канал, є потенційними "трієчниками". Цю ситуацію можуть виправити саме інтерактивні технології SMART, коли кожен інтуїтивно обирає найбільш зручний для себе спосіб сприйняття інформації під час роботи з інтерактивною дошкою. Дослідження показали, що в навчальних закладах з інтерактивною дошкою люди хочуть вчитися більше [2].

Повертаючись до нашої теми, а саме вдосконалення рівня освітнього процесу, то впровадження інтерактивних дошок у закладах МВС буде позитивно впливати на процес навчання, що у свою чергу обов’язково підвищить рівень навчання. У Дніпропетровському державному університеті внутрішніх справ є такий досвід при викладанні навчальних дисциплін інформаційного та математичного спрямування. Проте, на наш погляд, інтерактивні дошки настільки універсальні, що були б незамінні при викладанні і інших навчальних дисциплін, таких як кримінологія та криміналістика, кримінальне право та кримінальний процес, інш. Реально можливо збільшити ефективність навчання, підвищити інтерес майбутніх офіцерів поліції до навчання та своєї майбутньої професії. Також, варто пам’ятати, що система нових технологічних рішень, які включають в себе сучасні технології, допомагають реалізувати один з основних принципів "учись вчитися". Незалежно від етапу навчання, застосування інтерактивної дошки на заняттях виводить процес навчання на якісно новий рівень [3].

Важливо відмітити емоційний стан підчас навчання, адже інтерактивна дошка дозволяє розрядити високу емоційну напруженість і оживити навчальний процес. Також, використанням інформаційних технологій через інтерактивну дошку не тільки пожвавлює навчальний процес (що особливо важливо, якщо враховувати психологічні особливості, зокрема тривале переважання наочно-образного мислення над абстрактно-логічним), а й підвищує мотивацію до навчання. Навчальні заняття, які проведені із використанням інтерактивної дошки в силу своєї наочності, барвистості і простоти, приносять найбільший ефект, який досягається підвищеним психоемоційним фоном здобувачів вищої освіти при сприйнятті навчального

матеріалу.

Отже, інтерактивна дошка дозволяє представити навчальний матеріал більш наочно, доступно і зрозуміло. Також, вона сприятиме реалізації розвиваючого навчання, проблемно-діалогічного підходу, дозволить організувати на навчальному занятті дослідницьку діяльність, що є дуже корисним для майбутніх працівників поліції. Її використання дозволить здійснити диференційований підхід в навчанні. Крім того, застосування комп'ютерних тестів, перевірочних ігрових робіт, дозволить викладачеві за короткий час отримувати об'єктивну картину рівня знань здобувача та його підготовленість до заняття.

Використані джерела:

1. Какие сенсорные технологии используются на больших экранах? URL: https://habr.com/ru/post/181876/
2. Інтерактивні технології - стандарт сучасного навчального закладу URL: https://leater.com/ua/services/interaktivn-tekhnolog-dlya-navchannya.html
3. Лавщук В. І., Лавщук Л. А. Загальні прийоми використання інтерактивних дошок URL: http://journal.osnova.com.ua/article/46300

Наукове видання

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Матеріали Всеукраїнського науково-практичного семінару

(м. Дніпро, 26 листопада 2020 р.)

Українською мовою

Редактор, оригінал макет – *А.В. Самотуга*

Підп. До друку 18.12.2020. Формат 60х84/16. Друк – трафаретний. Папір офісний.
Гарнітура – Times. Ум. -друк. арк. 7,45 . Обл.-вид. арк. 7 .Тираж 100 прим.
Зам. № 03/18-зб

Надруковано у Дніпропетровському державному університеті внутрішніх справ
49005, м. Дніпро, просп. Гагаріна, 26, тел. (056) 370-96-59
Свідоцтво суб'єкта видавничої справи ДК №6054 від 28.02.2018