Одеський державний університет внутрішніх справ
Кафедра кібербезпеки та інформаційного забезпечення
Науково-дослідна лабораторія
з проблемних питань кримінального аналізу

КІБЕРБЕЗПЕКА В УКРАЇНІ: ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ ПИТАННЯ

Матеріали
Міжнародної науково-практичної конференції
22 листопада 2019 року

Одеса
ОДУВС
2019

УДК 343.9:004.7(477)
ББК 67.51+67.408.135(4Ук)
К 38

Рекомендовано до друку рішенням кафедри кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішніх справ
(протокол № 5 від 12 грудня 2019 року)

Всі матеріали надані в авторській редакції та виражають
персональну позицію учасника конференції

Кібербезпека в Україні: правові та організаційні питання: матеріали міжн. наук.
К38 практ. конф., м. Одеса, 22 листопада 2019 р. Одеса : ОДУВС, 2019. 108 с.
ISBN 678-717-7020

У збірнику представлено стислий виклад доповідей і повідомлень, поданих на міжнародну науково-практичну конференцію «Кібербезпека в Україні: правові та організаційні питання», яка відбулася на базі кафедри кібербезпеки та інформаційного забезпечення Одеського державного університету внутрішніх справ 22 листопада 2019 року.

У матеріалах конференції приділено увагу актуальним теоретичним та практичним проблемам забезпечення інформаційної безпеки в Україні. Висвітлюється широкий спектр питань, пов'язаних з удосконаленням правового регулювання та адміністративно-правового забезпечення кібербезпеки в Україні. Розглянуто використання інформаційних систем, технологій та інформаційно-аналітична діяльність правоохоронних підрозділів у боротьбі з злочинністю та надано обґрунтовані рекомендації щодо вдосконалення підготовки персоналу для боротьби з кіберзлочинністю в Україні.

Матеріали всеукраїнської науково-практичної конференції адресовано вченим, працівникам правоохоронних органів, аспірантам (ад'юнктам), слухачам магістратури, студентам та курсантам вищих навчальних закладів.

УДК 343.9:004.7(477)
ББК 67.51+67.408.135(4Ук)

ISBN 678-717-7020

Вступне слово
ректора Одеського державного університету внутрішніх справ
кандидата юридичних наук
Аброськіна В'ячеслава Васильовича
під час відкриття всеукраїнської науково-практичної конференції
«Кібербезпека в Україні: правові та організаційні питання»
22 листопада 2019 року, м. Одеса

Шановні учасники конференції!

Мені дуже приємно бачити Вас у стінах нашого навчального закладу. Сьогодні ми зібралися з метою обговорення важливої теми: «Кібербезпека в Україні: правові та організаційні питання». Значна частина питань щодо цієї проблеми може бути вирішена організаційними заходами. Проте, із розвитком інформаційних технологій, спостерігається тенденція до зростання потреби поглибленої правової регламентації кібербезпеки.

Ефективність захисту від посягань у кіберпросторі залежить від досконалості нормативно-правової бази, національної доктрини держави в області кібербезпеки, сформованої інфраструктури, ефективності підготовки та підвищення кваліфікації фахівців, а також технічного та матеріального забезпечення їх діяльності.

Під час підготовки до цієї конференції було прикладено чимало зусиль, адже вирішення цієї проблеми має неабиякий пріоритет. Ми разом з науково-педагогічним складом університету відповідально готувалися до цього наукового заходу, запросили досвідчених науковців із навчальних закладів та наукових установ, з різних куточків України, представників різних наукових шкіл та дослідницьких установ, а також науковців різних наукових поглядів з метою всебічного дослідження даної проблеми та вирішення правових та організаційних питань кібербезпеки в Україні.

З метою здійснення ефективної боротьби поліцейськими підрозділами з високотехнологічною злочинністю в окремих підрозділах створені аналітичні центри, роботу яких потрібно вдосконалювати та здійснити реструктуризацію аналітичних служб, з метою впровадження в діяльність працівників навичок ефективного використання систем і комплексного користування даними про злочинні об'єднання, які здійснюють контроль за найпоширенішими та найнебезпечнішими суспільно-небезпечними діяннями. В системі органів Національної поліції вже у процесі створення спеціальних аналітичних підрозділів, формування професійного аналітично-розвідувального апарату та впровадження організаційно-штатних змін в вітчизняній системі правоохоронних органів.

В Україні створено основні елементи системи захисту кіберпростору: напрацьовано відповідну нормативно-правову базу; визначено основні функції й повноваження суб'єктів системи кібербезпеки, реформовано ті, що діяли, та створено нові підрозділи, які проводять діяльність у цій сфері; тривають роботи зі створення нових зразків спеціальних технічних пристроїв для кіберзахисту. Проводяться численні наукові дослідження з метою вдосконалення діяльності органів державної влади в зазначеній галузі. Через високу досвідченість суспільства з'являється новий вид високотехнологічної злочинності, яка виступає складною і відносно новою сферою діяльності правоохоронних органів, що пов'язано, передусім, з появою більш складних, динамічних та інтелектуально-розвинених кримінальних організацій.

Ці та інші проблеми виступають, як основні питання дискусії нашого наукового заходу.

Я сподіваюся, що за результатами роботи конференції нами, спільно, будуть визначені основні переваги та недоліки формування системи аналітичних підрозділів та сформовані слушні пропозиції щодо подальшого розвитку підрозділів, спрямованих на своєчасне виявлення, розслідування та запобігання злочинам у сфері високих технологій.

Обговорювані на сьогоднішньому засіданні ідеї, пропозиції та рекомендації будуть узагальнені та узгоджені, з метою подальшого їх розвитку для ефективної діяльності органів Національної поліції.

Шановні учасники конференції, бажаю всім творчого натхнення, жвавих та цікавих дискусій, плідної роботи.

СЕКЦІЯ 1
ПРАВОВЕ РЕГУЛЮВАННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

Сутність інформаційної безпеки в умовах розвитку сучасного суспільства

Гончаров М.В.
аспірант кафедри теорії, історії права
і держави конституційного права
Університету державної фіскальної служби України

Сучасний стан суспільного розвитку характеризується як етап формування інформаційного суспільства. Впровадження новітніх інформаційних технологій значно прискорює процес отримання, обробки, аналізу інформації. Широкий і оперативний доступ до інформації підвищує ефективність її використання, що стає невід'ємним елементом управління всіма інститутами і процесами.

Інформаційні технології стали постійним супутником сучасної людини не лише на робочому місці, вони увійшли майже в усі сфери людського життя. Розповсюдження нових інформаційних технологій, в основі яких лежить широке використання комп'ютерної техніки та засобів комунікацій, оптимізації та автоматизації процесів в усіх без виключення сферах життєдіяльності, призвело до пошуку нових шляхів використанням інформаційно-комунікаційних систем в різних сферах діяльності суспільства.

Необхідною умовою розвитку сучасного суспільства є високий рівень інформаційної безпеки. Саме тому ефективне здійснення правового регулювання інформаційними ресурсами є важливою умовою забезпечення інформаційної безпеки та реалізації виваженої державної політики.

Сучасна Україна повною мірою включена в процеси інформатизації суспільства і формування єдиного світового інформаційного ринку. Інформаційний фактор відіграє значну роль у державотворчому процесі, у поданні та відстоюванні інтересів держави. Особливе місце у цьому спектрі суспільних відносин займають проблеми правового забезпечення інформаційної безпеки [1, с. 17].

Наукових визначень інформаційної безпеки існує сьогодні дуже багато, однак досі немає єдиної думки щодо її сутності.

За визначенням В. Гурковського, інформаційна безпека України – це суспільні відносини, пов'язані із захистом життєво важливих інтересів людини і громадянина, суспільства та держави від реальних та потенційних загроз в інформаційному просторі, що є необхідною умовою збереження та примноження духовних і матеріальних цінностей державоутворювальної нації, її існування, самозбереження і прогресивного розвитку України як суверенної держави, що залежить від цілеспрямованої інформаційної політики гарантій, охорони, оборони, захисту її національних інтересів [2, с. 74].

Використовує категорію національних інтересів і О. Баранов, визначаючи інформаційну безпеку як стан захищеності національних інтересів України в інформаційному середовищі, за якого не допускається (або зводиться до мінімуму) завдання шкоди особі, суспільству, державі через неповноту, несвоєчасність, недостовірність інформації й несанкціоноване її поширення та використання, а також через негативний інформаційний вплив і негативні наслідки функціонування інформаційних технологій [3, с. 60-62].

Інформаційну безпеку як стан захищеності національних інтересів України в інформаційній сфері від загроз особі, суспільству, державі через неповноту, несвоєчасність інформації, несанкціоноване поширення та використання інформації, негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій визначають також В. Шатун та О. Гладун [4, с. 175].

Якщо звернутися до нормативного визначення інформаційної безпеки, то слід зазначити, що чинне законодавство України не містить відповідного розгорнутого тлумачення цього поняття, проте нормативні акти, які торкаються питань інформаційної безпеки, закономірно розглядають її в контексті більш загального поняття національної безпеки [5, с. 67].

Відтак, інформаційна безпека є не лише самостійною складовою національної безпеки, а й невід'ємною частиною політичної, економічної, оборонної та інших складових національної безпеки.

Таким чином, забезпечення належного рівня інформаційної безпеки є необхідною умовою розвитку сучасного суспільства. Тому, створення ефективної системи інформаційної безпеки є однією з

найнагальніших завдань демократичної та правової держави. А забезпечення інформаційної безпеки України є визначальним напрямом державної політики, від якого залежатиме існування держави, її національна безпека, соціально-економічний розвиток та відповідне місце у світовому співтоваристві.

Література:

1. Ніщименко О. А. Інформаційна безпека Екраїни на сучасному етапі розвитку держави і суспільства. Наше право. 2016. № 1. С. 17–23.
2. Гурковський В.І. Безпека як об'єкт правовідносин в умовах глобального інформаційного суспільства. Правова інформатика. 2010. № 2(26). С. 72–77.
3. Баранов О.П. Передумови створення Державної спеціальної служби транспорту та її завдання в системі національної безпеки України. Вісник Національної академії державного управління при Президентові України. 2014. № 3. С. 60–65.
4. Шатун В. Т. Інформаційна безпека – невід'ємна складова національної безпеки України. Наукові праці Чорноморського державного університету імені Петра Могили комплексу «Києво-Могилянська академія». 2016. Т. 267. Вип. 255. С. 174–180.
5. Ткачук Т.Ю. Правове забезпечення інформаційної безпеки в умовах інтеграції України : Дис. ... док. юрид. наук : 12.00.07. Ужгород, 2019. 487 с.

Проблеми кваліфікації та криміналізації фішингу

Даніч М.А.
магістр 1-го курсу факультету підготовки фахівців
для органів досудового розслідування
Одеського державного університету внутрішніх справ

На сьогоднішній день людство не може уявити себе без коп'ютерної технології та різних видів доступу до віртуального простору. Проте, як відомо, медаль має дві сторони. З одного боку ми бачимо, що наш світ не зупиняється на одному місці та прогресує, але незважаючи на це разом з прогресом у світі науки просувається прогрес і в світі злочинності. Кіберзлочинність є об'єктивним наслідком глобалізації інформаційних процесів і появи глобальних комп'ютерних мереж. З ростом використання інформаційних технологій в різних сферах діяльності людини зростає і використання їх в цілях здійснення злочинів. Кіберзлочинність по своїй суті набагато ширше комп'ютерної злочинності і включає в себе цілий спектр протиправних діянь.

Злочини в сфері кібербезпеки на зараз одні з найнебезпечніших та найчисельніших, через те що, це порівняно з іншими видами злочинів є новим. Тому потрібно, аби поліція розвивалась в ногу з технікою, але це дуже важко у зв'язку з необізнаністю населення в механізмі його здійснення. Ще у 2012 році Україною називали «раєм для хакерів», так як наша законодавча база не так добре розвинена у сфері кібербезпеки, як у інших країн. Є деякі злочини, які не потребують особливих розумінь у техніці та вмінню користуватися комп'ютерною мережою. Одним із таких видів є фішинг. Його вважають одним із найпопулярніших та найнебезпечніших видів кібершахрайства.

Фішинг – це один із різновидів інтернет-шахрайства**,** який дозволяє обманним шляхом отримувати різну цінну інформацію, маскуючи комунікації так, ніби вони надійшли з надійного джерела. Надалі інформація може бути використана для доступу до пристроїв або мереж. Цільовий фішинг є цілеспрямованою фішинговою атакою, яка спирається на використання особистої інформації жертви, що робить атаку більш надійною. Взагалі є доволі багато видів «фішингу»:

Створення обманних веб-посилань. Інтернаціональні доменні імена (IDN) можуть використовуватися для створення заплутано схожих доменних імен, дозволяючи використовувати не-ASCII символи.

Візуальні подібності між символами в різних сценаріях, які називаються гомогліфами, застосовують для створення доменних імен, що візуально неможливо диференціювати. Це спонукає користувачів приймати один домен за інший.

Голосовий та текстовий фішинг. Для отримання інформації про обліковий запис зловмисники використовують телефонні дзвінки та текстові повідомлення. Спочатку вони надсилають клієнтам банків повідомлення, де стверджують, що їхній обліковий запис заблоковано. Це спонукає користувачів

подзвонити на вказаний номер телефону або зайти на веб-сайт, що контролюється шахраями, і залишити конфіденційну інформацію.

Клонування веб-сайтів, підробка та перенаправлення. Веб-сайти, вразливі до атак типу межсайтовий скриптинг (XSS), використовуються зловмисниками для запису власного контенту на інший веб-сайт. XSS-атака може застосуватися для перехоплення даних, введених на скомпрометованому сайті (включно з ім'ям користувача та паролем), які зловмисники використають пізніше [1].

Вчені виділяють інші види «фішингу», такі як кейлоггери та скрінлоггери. Це також атака зловмисного програмного забезпечення, коли зловмисник відслідковує вхідні дані з клавіатури, на якій людина надсилатиме відповідну інформацію через інтернет до хакера. Або викрадення сесії – це тип нападу зловмисного програмного забезпечення, коли зловмисник відслідковує систему користувача, і будь-що контролюється, тому, коли користувач увійде до банківських реквізитів чи іншої інформації, корисної для правопорушника, він буде захоплений шкідливим програмним забезпеченням та використовувати інформацію при передачі коштів без знань користувача.

Проте, існує несумнівна потреба в тому аби кваліфікувати даний злочин. Існує 16 розділ в Кримінальному Кодексі України «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». Однак не завжди можна кваліфікувати даний вид злочину саме під цей розділ. Тому що для того, щоб злочин відбувся, необхідно встановити всі обставини, які вчинилися, особливо мету. Фішинг – це мистецтво обману. За допомогою соціальної інженерії зловмисники користуються людською цікавістю, страхом і довірливістю, аби маніпулювати своїми жертвами.

Якщо злочинець отримав інформацію шляхом підглядання, то це крадіжка. Якщо він використав технічні засоби для того, щоб зняти цю інформацію, то це вже кіберзлочин. І кваліфікація відбувається кожен раз окремо, індивідуально, в залежності від обставин, коли можна виявити, що громадянин втратив дані своєї банківської картки або рахунку.

Якщо звернути увагу на ч. 3 ст.190 КК України (шахрайство), то, можна виділити ту обставину, що норма не цілком конкретизована в частині скоєння шахрайства шляхом незаконних операцій з використанням електронно-обчислювальної техніки. Оскільки в даному випадку саме завдяки такому розширеному тлумаченні та відсутності в українському законодавстві ефективних методів боротьби зі злочинами, які вчиняються з використанням електронно-обчислювальної техніки, значна кількість злочинців залишається непокараною.

Ще однією з головних проблем, чому злочини в сфері ІТ-технологій мають низький рівень розкриття, є те, що людям не вистачає спеціальних знань у боротьбі з кіберзлочинністю. У зв'язку з тим, що бурхливий розвиток комп'ютерної техніки та телекомунікаційних мереж методики судово-експертного дослідження даних об'єктів вимагають постійного оновлення та доопрацювання. Кожного року змінюються формати даних, операційні системи, протоколи і середовище перенесення даних, технічні засоби, що забезпечують процес передання інформації тощо. Сліди кіберзлочинів досліджуються за допомогою комп'ютерно-технічної експертизи та експертизи відео- та звукозапису. А щодо наукової експертизи, то він повністю залежить від рівня професійної підготовки експертних кадрів, а серед них близько 3% мають наукові ступені [2; с. 1].

Особливу увагу під час проведення розслідування кіберзлочинів приділяють збиранню доказів. Сторона обвинувачення здійснює збирання доказів шляхом: проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій; витребування та отримання від органів державної влади, органів місцевого самоврядування, підприємств, установ та організацій, службових та фізичних осіб речей, документів, відомостей, висновків експертів, висновків ревізій та актів перевірок; здійснення міжнародного співробітництва під час кримінального провадження; проведення інших дій, передбачених КПК України. Особи повинні дотримуватись обережності при зборі, упаковці або зберіганні цифрових пристроїв, щоб уникнути зміни, пошкодження або знищення цифрових доказів. Уникайте використання будь-яких інструментів або матеріалів, які можуть виробляти або випускають статичну електрику або магнітне поле, оскільки вони можуть пошкодити або знищити докази [3; с. 135-136].

При зборі електронних доказів, треба мати необхідні знання про сучасні види програмного та апаратного забезпечення систем і пристроїв, які можуть містити електронні докази, починаючи від стаціонарних комп'ютерів, їх компонентів, ноутбуків і комп'ютерних мереж, і завершуючи окремими мобільними телефонами, смартфонами та іншими гаджетами. Треба розуміти, які саме потенційні електронні докази та як саме можуть зберігатися в них, та яким чином, при яких умовах та ким вони можуть бути знищені. Необхідно мати теоретичні знання та практичні навички захисту місця

електронного злочину та електронних доказів від знищення. Відповідно, необхідно впевнено орієнтуватись в умовах виробничого, офісного та домашнього кібернетичного середовища. Необхідно вміти ідентифікувати та зупиняти спроби та процеси знищення комп'ютерних даних, які можуть містити електроні докази злочинів. Але не кожна особа обізнана в данному питанні, тому це дуже важка робота, іноді через невміння збирати такого роду докази стає неможливим покарання злочинців.

Отже, дуже важливим аспектом у тому, аби кваліфікувати фішинг за статтею Кримінального Кодексу України, немає конкретизації в ч. 3 ст. 190, а саме про вчинення шахрайства шляхом незаконних операцій з використанням електронно-обчислювальної техніки. Другим важливим недоліком є те, що при збиранні електронних та цифрових пристроїв, через недостатність знання можна пошкодити докази, що унеможливлює покарання для злочинців.

Література:

1. Пилипенко О. Фішинг та цільовий фішинг: поради по захисту. [Електронний ресурс]. Режим доступу: https://www.imena.ua/blog/phishing-and-target-phishing/
2. Комасюк І.С. Кіберзлочинність і сьогодення . *Українське право*. 2017. № 2. С. 1.
3. Г.В. Муляр, О.С. Ховпун Особливості доказування кіберзлочинів. *Право. Людина. Довкілля*. 2019. № 3. С. 135-136.

Кібербезпека та інтелектуальна власність: питання правового забезпечення

Коротун О.М.
докторант
науково-дослідний інститут публічного права (Київ)
к. ю. н.

Питання кібербезпеки в епоху інформаційних технологій все більше турбує світову спільноту, адже з технологій стрімко зростає кількість порушень та злочинних діянь, внаслідок чого цілі держави, їх установи та численна кількість приватних корпорацій та інших установ і організацій несуть значні збитки.

За даними ООН щороку кіберзлочинність завдає державам та приватним особам дуже великої шкоди, щорічні збитки від кіберзлочинності у світі в розмірі 1,5 трлн доларів. На жаль, прогнози експертів з кібербезпеки невтішні. В майбутньому кількість злочинів та збитків від кібератак лише зростатиме, адже зазвичай правопорушники йдуть щонайменше на крок попереду механізмів, які мають державні органи та приватні особи щодо запобігання і розкриття таких злочинів. Наша країна також є мішенню кібератак. Лише за останні кілька років державні установи неодноразово були атаковані з кіберпростору. Згідно зі звітом, який міститься на веб-сайті Департаменту кіберполіції України у 2018 році працівники цього Департаменту були залучені до розслідування більше ніж 11 тисяч кримінальних проваджень, вчинених у сфері високих інформаційних технологій.

Використовуючи сучасні технології, це можуть бути різноманітні злочини. Так, у цьому році кіберполіцією України був затриманий **х**акер, який за допомогою спам-розсилки інфікував вірусами техніку користувачів мережі та викрадав їх конфіденційну інформацію. Викрадені бази даних, які він зберігав на своєму комп'ютері, налічували інформацію щодо мільйонів потерпілих, викрав 6 мільйонів доларів із рахунків американських фінансових установ [1].

Проблемним питанням, яке нерозривно пов'язано з інформаційними технологіями, кібербезпекою є охорона суб'єктивних прав правовласників та інших учасників правовідносин у сфері інтелектуальної власності.

На сьогодні, кожний продукт або послуга, які ми вживаємо або отримуємо у повсякденному житті, – це результат інтелектуальної, творчої діяльності людини. Сьогодні все більше зростає розуміння того, що трансформація науково-технічних розробок в інноваційний продукт, придатний для виробництва і ринку, чи не найважчий етап у ланцюзі, який пов'язує розробника зі споживачем, а тому належна охорона суб'єктивних прав суб'єктів права інтелектуальної власності на належні ним об'єкти права інтелектуальної власності визнається в усьому світі невід'ємним елементом ринкових відносин [2, с. 6].

Особливо це стосується авторського права, його використання в мережі Інтернет, що у свою чергу потребує ліцензованого використання програмного забезпечення, використання антивірусних програм з метою захисту персональних даних тощо. На жаль дуже часто співробітники як державних,

так і приватних установ використовують неліцензійне програмне забезпечення, що дозволяє порушникам через таке комп'ютерне забезпечення безперешкодно вчиняти різноманітні порушення. Так, у 2014 році компанія «Лабораторія Касперського» спільно з Європолом та Інтерполом розкрила групу Carbanak, яка успішно на протязі багатьох років виводила кошти з банків через банкомати або онлайн-банкінг. Діяла група досить просто, через електронну пошту заражалися комп'ютери рядових співробітників і збиралися з них дані про те, яким чином влаштована робота в цьому банку і хто за що відповідає, а у подальшому це допомагало сформувати шляхи крадіжки коштів [3].

Будь-які інформаційні технології нерозривно пов'язані з інтелектуальною власністю, тому вказані процеси супроводжуються не тільки розвитком різноманітних інформаційних технологій, але й розвитком законодавства, що проявляється у перманентному процесі появи нових нормативно-правових актів.

Розуміючи важливість захисту персональних даних у Європейському Союзі прийнято нормативний акт – Директива Європейського парламенту і Ради (ЄС) №2016/1148, під назвою «Безпека мереж та інформації» (Network and Information Security), що набрав чинності 09.05. 2018 р., який встановлює правила роботи з персональними даними (GDPR) і ставить досить жорсткі вимоги до технічної складової захисту персональних даних [4].

Правову основу забезпечення кібербезпеки України становлять Конституція України, закони України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, цей та інші закони України, Конвенція про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, укази Президента України, акти Кабінету Міністрів України, а також інші нормативно-правові акти, що приймаються на виконання законів України.

Відзначаючи проблемність безпеки держави, що проявляються у різноманітних негативних проявах, Указ Президента України № 92/2016 Про рішення Ради національної безпеки і оборони

України від 04.03.2016 року «Про Концепцію розвитку сектору безпеки і оборони України» [5]. Головними завданнями сектора безпеки і оборони визначено захист конституційного ладу, економічного, науково-технічного й оборонного потенціалу України, законних інтересів держави та прав громадян від розвідувально-підривної діяльності іноземних спеціальних служб, посягань з боку окремих організацій, груп та осіб, а також забезпечення громадської безпеки та охорони державної таємниці, іншої інформації з обмеженим доступом, забезпечення інформаційної та кібербезпеки.

Отже, на сьогодні в Україні діють закони та підзаконні нормативні акти, які регулюють відносини в цій сфері. Серед значної кількості нормативних актів, важливу роль у захисті інтелектуальної власності відіграє «Конвенції про кіберзлочинність» від 23.11.2001 р. [6], яка є частиною українського законодавства.

Відповідно до Конвенції про кіберзлочинність, кіберзлочини умовно поділяються на чотири види. До першого виду належать правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем. До цього виду кіберзлочинів можна віднести всі злочини, спрямовані проти комп'ютерних систем і даних (наприклад, навмисний доступ до комп'ютерної системи або її частини; навмисне пошкодження, знищення, погіршення, зміна або приховування комп'ютерної інформації; навмисне вчинення, не маючи на це права, виготовлення, продажу, придбання для використання, розповсюдження або надання для використання іншим чином пристроїв, включаючи комп'ютерні програми).

До другого виду кіберзлочинів належать правопорушення, пов'язані з комп'ютерами. Такі злочини характеризуються умисним діянням, що призводить до втрати майна іншої особи шляхом будь-якого введення, зміни, знищення чи приховування комп'ютерних даних або будь-якого втручання у функціонування комп'ютерної системи, з шахрайською або нечесною метою набуття, не маючи на це права, економічних переваг для себе чи іншої особи.

Третій вид кіберзлочинів охоплює 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.

Четвертим видом є умисні дії, пов'язані з порушенням авторських та суміжних прав, відповідно до вимог Бернської Конвенції про захист літературних і художніх творів, Угоди про торговельні аспекти прав інтелектуальної власності та Угоди ВОІВ про авторське право, а також національного законодавства України [7].

Водночас, якщо аналізувати чинні вітчизняні нормативно-правові акти у сфері кіберзлочинності, які мають безпосереднє відношення до інтелектуальної власності, варто зазначити, що на сьогодні, законодавець не спроможний встигати за тими видами правопорушень, що

виявляються у правозастосовній діяльності. Тому беручи до уваги існуючі проблемні питання законодавчого забезпечення, законодавцю необхідно більш діємо співпрацювати з науковцями, практичними працівниками з метою забезпечити належний захист інтелектуальної власності, в тому числі й у сфері кібербезпеки.

Література:

1. Веб-сайт Департаменту кіберполіції України. URL: https://cyberpolice.gov.ua/
2. Світличний О. П. Право інтелектуальної власності: Підручник. Вид. 2, змін. і доп. К.: НУБіП України, 2017. 355 с.
3. Раєцький А. Кібербезпека бізнесу це не лише технічні заходи. URL: https://legalitgroup.com/kiberbezpeka-biznesu-tse-ne-lishe-tehnichni-zahodi/
4. Директива Європейського парламенту і Ради (ЄС) №2016/1148. https://zakon.rada.gov.ua/laws/show/984_013-16/sp:max100?sp=:max100&lang=uk
5. Про Концепцію розвитку сектору безпеки і оборони України: Указ Президента України № 92/2016 від 04.03. 2016 р. https://zakon.rada.gov.ua/laws/show/n0002525-16
6. Про ратифікацію Конвенції про кіберзлочинність: Закон України від 23.11.2001 р. Відомості Верховної Ради України. 2006. № 5-6. Ст. 71.
7. Нікулеско Д. Ера нових видів злочинів.

Кримінальна відповідальність за злочини вчиненні у сфері кібепростору

Щирська В.С.
доцент кафедри
кримінального права та кримінології
факультету підготовки фахівців
для органів досудового розслідування
Одеського державного університету внутрішніх справ
к.ю.н.
Слободянюк А.В.
курсант 308 взводу факультету підготовки фахівців
для органів досудового розслідування
Одеського державного університету внутрішніх справ

Відповідно до частини першої статті 361-1 Кримінального кодексу України створення з метою використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, - караються штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років. [1, с-154].

Зростання злочинів із застосування інформаційно-телекомунікаційних систем є глобальною проблемою і тому знаходження шляхів їх вирішення є актуальним. Успішність запобігання таким злочинам, їх викриття та притягнення винних осіб до відповідальності наразі є достатньо рідкісним явищем, якщо порівнювати з кількістю таких правопорушень.

Дана тема стала об’єктом численних досліджень вітчизняних науковців, таких як: П. Біленчук, Б. Кормич, Т. Костецька, Є. Кравець, Н. Лебедєва, В. Монахов, В. Наумов, Р. Шагієва.

У наш час злочини у сфері кіберпростору є досить розповсюдженими. відчувати себе захищеним від таких злочинів практично неможливо. Межі кіберпростору є безмежними, хакери мають досить розвиненні навички , щоб залишитися в ньому інкогніто і тому це створює проблеми при розслідуванні таких злочинів. Тисячі злочинів кожного дня пов’язані із викраденням персональних даних, коштів із рахунків, блокуванням діяльності. Під колом можливих жертв не тільки люди, а й компанії і навіть держави. Під поняттям кібербезпеки розуміється захищеність життєво-важливих інтересів суспільства та держави у процесі використання кіберпростору, яка забезпечує сталий розвиток інформаційного суспільства і цифрового комунікативного середовища.

До правової основи кібернетичної безпеки України входять такі нормативно-правові акти: Конституція України, Кримінальний кодекс України, закони України «Про основні засади забезпечення кібербезпеки України», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основи національної безпеки» та інші закони, Доктрина

інформаційної безпеки України, Конвенція Ради Європи про кіберзлочинність та інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України.

Кіберзлочини умовно поділяються на чотири види. До першого виду належать правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем. До цього виду відносяться всі злочини, спрямовані проти комп'ютерних систем і даних. До другого виду кіберзлочинів належать правопорушення, пов'язані з комп'ютерами. Такі злочини характеризуються умисним діянням, що призводить до втрати майна іншої особи шляхом будь-якого введення, зміни, знищення чи приховування комп'ютерних даних або будь-якого втручання у функціонування комп'ютерної системи. Третій вид кіберзлочинів охоплює правопорушення, пов'язані зі змістом, що полягає у здійсненні умисних незаконних дій щодо вироблення, пропонування або надання доступу, розповсюдження дитячої порнографії, а також володіння такими файлами у своїй системі. Четвертим видом є умисні дії, пов'язані з порушенням авторських та суміжних прав, відповідно до вимог Бернської Конвенції про захист літературних і художніх творів, Угоди про торговельні аспекти прав інтелектуальної власності та Угоди ВОІВ про авторське право, а також національного законодавства України. [2]

За інформацією голови Департаменту кіберполіції Сергія Васильовича Демедюка, щороку кількість кіберзлочинів в Україні збільшується в середньому на 2,5 тисячі. Згідно зі звітом, який міститься на веб-сайті цього правоохоронного органу, у 2018 р. працівники Департаменту кіберполіції були залучені до розслідування більше ніж 11 тисяч кримінальних проваджень, кіберполіції не озвучує реальних результатів таких розслідувань.[3]

Існує перелік статтей Кримінально кодексу 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, 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».

Багато судових рішень винесених за результатами розгляду кримінальних проваджень можна знайти в Єдиному державному реєстрі судових. В реєстрі містяться вироки за вказаними статтями, а також ухвали слідчих суддів щодо кримінальних проваджень, які сьогодні знаходяться у провадженні органів досудового розслідування.

Порушення статті 361 Кримінального кодексу України є досить поширеним явищем для України. Кожного року До ЄДРС вносяться відомості про нові злочини.

Великої уваги приділили до справи першого заступника голови Сум Володимира Войтенка. Йому було пред'явлено обвинувачення за ч.1 ст. 357, ч.2 ст. 361 КК України, несанкціоноване втручання в роботу автоматизованих систем, що призвело до підробки інформації, вчинене повторно; привласнення офіційного документа, вчинене в особистих інтересах. Прокуратура обвинувачує його у втручанні в роботу системи «Рада» шляхом голосування карткою тодішнього депутата Сумської міської ради Сергія Науменка за визначення компанії «А-Муссон» переможцем конкурсу на вивезення сміття в м.Суми. Суд ухвалив накласти арешт на документи вилучені 21.01.2019 на підставі ухвали слідчого судді у приміщеннях Сумської міської ради. [4]

Отже можемо зробити висновок, що притягнення злочинців до відповідальності за вчинення злочинів у межах кіберпростору є тривалим процесом, який вимагає чітких доказів. Відомості, які представлені в Єдиному державному реєстрі судових рішень свідчать про те, що у нашій країні триває боротьба з кіберзлочинність. З кожним роком кількість уих злочинів збільшується.

Література:

1. Кримінальний кодекс України: чинне законодавство із змінами та доповненнями на 12 вересня 2019 року: Офіц. текст . К.: Алерта, 2019. 208с.
2. Конвенція про кіберзлочинність. [Електронний ресурс]. http://zakon2.rada.gov.ua/laws/show/994_575/print1330337542993813

3. Юридична газета online (електронний ресурс) режим доступу http://yur-gazeta.com/publications/practice/inshe/kiberbezpeka-vrazlivi-momenti.html
4. Постанова суду №79373231, 24.01.2019 [Електронний ресурс]. https://youcontrol.com.ua/ru/catalog/court-document/79373231/

Кібершпіонаж - загроза сучасному інформаційному суспільству

Нашинець-Наумова А.Ю.
заступник декана з науково-методичної та навчальної роботи
факультету права та міжнародних відносин
Київського університету імені Бориса Грінченка
д. ю. н., доцент

Якщо говорити про правове регулювання діяльності в українському сегменті глобальної інформаційно-телекомунікаційної мережі «Інтернет», то за багато років слабкого правового режиму виникла середа з дуже низькою правовою культурою і багатьма проявами режиму безвідповідальності. З розвитком інформаційних технологій стали розроблятися інструменти для шпигунства з використанням як спеціалізованих пристроїв, так і програмного забезпечення. На відміну від класичних методів розвідки і шпигунства, нові технології внесли в них суттєві коригування. В даний час іноді неможливо встановити, хто саме розробив те чи інше програмне забезпечення для проведення розвідувальних дій у сфері високих технологій. Розробниками подібного спеціалізованого програмного забезпечення можуть бути як приватні особи, так і підприємства різної форми власності, з різними джерелами фінансування. Нерідко особи, які розробили програмне забезпечення, не є тими особами, які його використовують для здійснення кібершпіонажу. Це ускладнює, а іноді унеможливлює, ідентифікацію осіб, які здійснюють кібершпіонаж, і як результат – їх залучення до встановленої форми відповідальності. Подібна практика призводить до того, що зацікавлені особи найчастіше самостійно вишукують методи протидії проявам кібершпіонажу в кожному конкретному випадку. Останні включають в себе класичні методи підвищення інформаційної захищеності об'єктів, а також спеціалізовані методи кіберконтррозвідки [1, с. 88].

На відміну від загальної думки, що об'єктами нападу в кібершпіонажі є міжнародні, міждержавні, державні органи, організації та установи, на справді об'єктами нерідко виявляються комерційні компанії та підприємства. Однак, з якихось причин до цих обставин не приділяється належної уваги, особливо якщо це не було пов'язано з розкраданням державної таємниці. Кібершпигуни нерідко мають на меті крадіжку цілого масиву інформації, оскільки такі дії дозволяють отримувати велику кількість персональних даних та/або комерційно значущої інформації. Метою цих дій може бути зміна або видалення певної інформації, що дозволяє усунути компрометуючі відомості, створити позитивну (негативну) історію або, наприклад, створити певні умови для здійснення іншої протиправної дії. Робота щодо припинення навмисних протиправних дій бачиться неможливою без чіткого розуміння найбільш значущих політичних чинників розвитку комп'ютерної злочинності. Саме в цьому контексті слід відповісти на питання, які процеси демократичного управління та які юридичні норми повинні бути погодженні для прийняття рішення щодо застосування тих чи інших відповідних заходів.

До «найвагоміших політичних чинників, що визначають розвиток комп'ютерної злочинності в Україні, слід віднести:

1) розвиток руху хактивістів як політичної причини комп’ютерної злочинності. Хактивізм (hacktivism, від анг. hack – рубати та activism – активізм [2]) – це суспільний рух, який передбачає боротьбу за права та свободи людини та громадянина за допомогою використання комп’ютерних технологій та інформаційно-телекомунікаційних мереж, включаючи Інтернет;

2) заподіяння шкоди державним інтересам, діяльності механізму державної влади України збройними силами ворожих країн, шляхом використання шкідливих комп'ютерних програм в якості інформаційної зброї;

3) діяльність спецслужб іноземних держав щодо українських органів влади, установ, підприємств для отримання інформації геополітичного, військово-технічного, дипломатичного та іншого стратегічного характеру, тобто «кібершпіонаж» [3, с. 41].

Особливого значення зазначені проблеми набувають з урахуванням фактичної відсутності ефективно функціонуючого, закріпленого на законодавчому рівні правового механізму забезпечення інформаційної безпеки, істотного відставання України від більшості розвинених держав і ряду держав з перехідною економікою за рівнем впровадження інформаційно-комунікаційних технологій [4, с. 4].

В силу своєї природи кібертероризм і кібершпіонаж «кидають виклик сферам дослідження частково через великий масштаб дій і подій, що мають місце» [5, с. 42]. Подібна особливість кібершпіонажу, на наш погляд, робить єдино можливим і доцільним консолідацію зусиль щодо забезпечення національної інформаційної безпеки в одній державній службі. Створення подібної служби дозволить організувати єдині підходи щодо забезпечення режиму безпеки та правопорядку на національному рівні, а в разі наявності належної політичної волі і міжнародної кон'юнктури і на міжнародному рівні. В умовах складної економічної ситуації важливими є консолідація матеріальних ресурсів і кадрового складу. Це дозволить за умови створення належних організаційно-правових механізмів забезпечити необхідний режим національної інформаційної безпеки, ефективно використовувати бюджетні кошти та наявний кадровий потенціал, ефективно протидіяти актам кібершпіонажу, а також іншим загрозам національної інформаційної безпеки. На думку автора, така служба повинна бути наділена широкими повноваженнями відповідно до Кодексу України про адміністративні правопорушення та Кримінально-процесуального кодексу України. Подібний підхід дозволить створити «живу» структуру, здатну відповідати мінливим викликам сучасного інформаційного суспільства. Наділена необхідними кадровими і матеріально-технічними ресурсами для оперативної компетентної реалізації своїх вузькоспеціалізованих повноважень в рамках спеціальної підслідності, така служба позитивно вплине на стан інформаційної захищеності, рівень законності і правопорядку в національному сегменті інформаційно-телекомунікаційної мережі «Інтернет».

Проблема боротьби з кібершпіонажем в значній мірі ускладнюється через глобальний масштаб інформаційних мереж. В даному випадку ефективності вжитих зусиль заважають ті ж проблеми, які притаманні будь-якому комерційному проекту міжнародного рівня. Крім того, виникають і додаткові складнощі, пов'язані з участю структур приватного сектора. Якщо якийсь вебсайт з шкідливим контентом має розширення, наприклад, .ch (Швейцарія), але належить Росії і розміщений при цьому в Нідерландах, то хто в такому випадку несе за нього відповідальність, і які правові норми повинні при цьому застосовуватися? Але навіть відповідь на це головне питання, тобто хто конкретно стоїть за тією чи іншою IP-адресою, вимагає участі суб'єктів приватного сектора, багато з яких або взагалі не зберігають подібну інформацію, або не хочуть нею ділитися. Ця проблема ускладнюється ще й тим, що в багатьох країнах законодавство з цього питання або зовсім відсутнє, або має дуже обмежений характер [6, с. 17]. У багатьох випадках, навіть якщо керівництво країни рішуче налаштовано на боротьбу з кіберзлочинністю, у держави немає необхідних технічних можливостей для розробки потрібного законодавства або механізмів його реалізації в разі, якщо таке законодавство вже існує. В умовах відсутності необхідної нормативно-правової бази та технічних можливостей для її реалізації, злочинці можуть увійти в Інтернет анонімно, користуючись мережею на території слабо розвиненої держави (наприклад, за допомогою незареєстрованої SIM-карти) і безкарно здійснювати свої злочини із-за кордону. За словами голови консультативної ради Міжнародного багатостороннього партнерства проти кіберзагроз (міжнародна організація, що діє під егідою ООН) Датук Мухаммеда Нур Аміна, такі країни ризикують перетворитися в «недієздатні держави кіберпростору» (cyber failed states). З огляду на витратність заходів щодо забезпечення безпеки інформаційних мереж (за різними оцінками, від 3 до 10% від загальних витрат на утримання мереж), незрозуміло, як скоро такі держави зможуть оволодіти необхідними ресурсами [6, с. 23].

Тому необхідно створити загальну стратегію і загальні правові норми, які б регулювали правила боротьби з кібершпіонажем на міжнародному рівні. Однак зусилля з розвитку міжнародного співробітництва в цій сфері неминуче вимагатимуть вирішення такої серйозної проблеми, як дотримання оптимального балансу між вимогами про збереження анонімності, конфіденційності та відкритості, з одного боку, і вимогам кібербезпеки, з іншого боку, зокрема, що стосується інформаційних обмінів і вдосконалення можливостей щодо пошуку кіберзлочинців. У контексті боротьби з кіберзагрозами існує і цілий ряд інших проблем демократичного врядування.

З наведеного аналізу можна зробити такі висновки. Для організації ефективної боротьби з кібершпіонажем держава повинна вийти за рамки чисто урядового підходу і прийняти новий підхід, на центральне місце якого має бути поставлено дієве державно-приватне партнерство. Так, наприклад, правоохоронні органи не можуть ефективно боротися з кіберзлочинністю в умовах, коли аналогічні функції і обов'язки не зосереджені у них в руках, а розподілені серед цілого ряду міністерств і відомств, а створення офіційних мереж державно-приватного партнерства в цій сфері ускладнюється, або ці мережі функціонують неефективно. Остання обставина має особливе значення, враховуючи, що обидві сторони цього партнерства не схильні ділитися важливою інформацією, особливо у випадках, коли справа стосується міжнародних і зарубіжних компаній. У такому партнерстві повинні бути задіяні не тільки приватні суб'єкти, які беруть участь в так званих «критичних» сферах діяльності, але і фірми, що спеціалізуються в сфері інформаційної безпеки, а також розробники програмного забезпечення,

виробники обладнання, оператори сервісів електронних платежів і електронної пошти, хостінг-провайдери, учасники банківського і фінансового секторів, торговельні Інтернет-фірми і фізичні особи.

Література:

1. Галушкин А.А. Кибершпионаж – угроза современному обществу. *Вестник МГОУ*. Серия: Юриспруденция. 2015. № 2. С. 87–91.
2. Хактивизм [Електронний ресурс]. Режим доступу: http://www.tadviser.ru /index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A5%.
3. Евдокимов К.Н. Политические факторы компьютерной преступности в России. *Информационное право*. 2015. № 1. С. 41–47.
4. Тедеев А.А. Ценностные ориентиры государственной инновационной политики в сфере обеспечения устойчивого развития электронного бизнеса в России *Финансы и кредит*. 2012. № 14. С. 2–6.
5. Luppicini R. Illuminating the Dark Side of the Internet with Actor-Network Theory: An Integrative Review of Current Cybercrime Research // Global Media J. (Canadian Edition). 2014. Vol. 7 (№ 1). P. 35–50.
6. Бенджамин С. Бакленд Демократическое управление и вызовы кибербезопасности. Женева: Женевский центр демократического контроля над вооруженными силами. 2013. 47 с.

Кібербезпека як (трудо)правоутворюючий чинник

Панасюк О.Т.
доцент кафедри трудового права
та права соціального забезпечення
Київського університету імені Тараса Шевченка,
к. ю. н., доцент

На правове регулювання трудових відносин вливають чинники, які утворюються у різних сферах суспільного життя (економічній, політичній, соціальній сфері, сфері світогляду та ціннісних орієнтацій).

В сучасних умовах на зміст правового регулювання впливає такий складний інтегрований фактор як кібербезпека. Це явище включає як позитивний так і негативний аспекти.

Явище, яке позначається терміном «кібербезпека», має своїм походженням два методологічних джерела. Перше, це технологічний розвиток, які виступає основою не тільки сфери промислового виробництва, але на усіх сфер суспільного життя.

Друга, це існування ризиків та загроз одночасно із перевагами технологічного розвитку, вплив яких подекуди є настільки значним, що дозволяє порівнювати його з театром бойових дій [1, с. 72 - 72].

Обидві вказані тенденції змінюють суспільну організацію праці, що призводить до появи норм та конструкцій трудового права певного змісту.

Виникнення критичного рівня ризиків та загроз передусім відчула на собі ІТ – індустрія [2], що сформувало специфіку її організації праці.

В сучасних умовах питома вага чинника особистої участі працівника у використанні різного роду технологій на конкретному робочому зростає. Мова про такі процеси як автоматизація, інформатизація тощо. Відповідно, зростає значення стимулювання підвищення кіберкваліфікації працівника,

забезпечення обережного поводження працівника із технічними засобами і власне інформаційними ресурсами роботодавця та ін.

Вищевказане актуалізує роль трудового права у регулюванні саме тих взаємних відносин, які виникають при використанні комп'ютерної техніки, програмного забезпечення та ін.

Наука трудового права не залишає без уваги вплив на розвиток трудового права інформаційно - технологічного розвитку[3]. Проте, розгляд особливостей «кібербезпеки» як явища, яке безпосередньо впливе на зміст трудових правовідносин, не є таким, що відповідає нагальним потребам.

Термін «кібербезпека» попри популярність сприймається неоднозначно. Його правовий зміст потребує окремої уваги з боку представників різних правових наук.

Насамперед, встановлення змісту поняття «кібербезпека» вимагає його порівняння із дотичними до нього поняттями. Зокрема, такими як «інформаційна безпека», «комп'ютерна безпека», «соціальна безпека», «національна безпека» та ін.

Зміст поняття «кібербезпека» складається шляхом поєднання двох складових – «кібер» та «безпека».

Безпосередній зв'язок із понятійним апаратом трудового права має слово «безпека», яка позначає стан відсутності технічних та соціальних загроз, ризиків для функціонування трудових відносин.

До системи трудового права традиційно включаються такі інституційні складові як техніка безпеки, виробнича санітарія, протипожежна безпека.

В сучасному трудовому праві активно розвивається інститут захисту трудових прав, що сприяє виокремленню «безпекових» трудових зав'язків та їх умовно самостійного аналізу.

Окремими складовими системи трудового права є захист персональних даних працівника та захист професійної таємниці (державної, лікарської, адвокатської та ін. таємниці).

Первинну методологічну роль для формування змісту вказаного поняття має слово «кібер» [4].

Окрім загальної вказівки на зв'язок із сферою застосування комп'ютерів це слово змістовного навантаження не має. Видається, що такий контекст є звуженим. Але, саме таке його значення є усталеним та найбільш поширеним.

Слово «кібер» само по собі не може вказати на правовий зв'язок працівника та роботодавця. Однак, його застосування у певних правових словосполученнях дозволяє позначати коло професійних обов'язків працівника або окреслити окремий напрямок діяльності роботодавця.

Відповідно, поняття «кібербезпека» в аспекті трудових відносин слід визначати як сукупність правових зв'язків (прав та обов'язків) працівника та роботодавця, що виникають у зв'язку із необхідністю недопущенням виникнення та/або подоланням існуючих ризиків, загроз, негативних наслідків (наприклад, майнової шкоди тощо) при використанні певних технічних засобів обробки та зберігання інформації.

Питання, які входять до предмету трудового права та стосуються «кібербезпеки», доволі розгалуженні.

Серед них центральне місце посідають відповідні аспекти індивідуальних трудових правовідносин.

Так, «кібербезпекові» навички є складовою трудової функції будь- якого працівника, робота якого пов'язана використанням інформаційних технологій та застосуванням персональних комп'ютерів. В такому вигляді конкретні обов'язки або опис необхідних кваліфікаційних закріплюється у посадових інструкціях працівників.

Індивідуальні зобов'язання працівника щодо усунення загроз для певних об'єктів (кібероб'єктів) визначаються у локальних нормативних актах, ознайомлення працівника з якими є обов'язком роботодавця до початку фактичного виконання роботи, обумовленої у трудовому договорі. Такими локальними нормативними актами, наприклад, є Правила внутрішнього трудового розпорядку, Положення про комерційну таємницю та ін.

Особливий вид «кібербезпекового» індивідуального зв'язку працівника та роботодавця виникає у тих працівників, трудова функція яких передбачає безпосередню роботу із кібер-об'єктами (із інтернет – мережею, із розробкою та використанням програмного забезпечення та ін.).

Наприклад, обов'язок впроваджувати рішення щодо безпеки мережі та забезпечення мережевої безпеки IT – інфраструктури компанії покладається на працівника, посада якого іменуються Network Engineer в компанії «Варгемінг», одного із лідерів ринку free-to-play MMO [5].

Один із спеціальних різновидів трудової функції мають фахівці в галузі боротьби із кібер-небезпекою (загрозами, порушеннями та ін.). Їх робота є подібною до правоохоронної діяльності щодо завдань. Але статус таких фахівців не передбачає повноважень щодо застосування спеціальних оперативних заходів, вжиття заходів кримінально – правового змісту.

Правовий статус працівника включає такий наслідковий «безпековий» елемент як відповідальність. Правова регламентація матеріальної або дисциплінарної відповідальності працівника належить до сфери трудового права. Можливість покласти на працівника негативні наслідки у зв'язку із «кібербезпековими» правопорушеннями має як превентивну та і компенсаційну мету.

Дані види юридичної відповідальності не можна розглядати окремо від інших її видів, які регламентуються кримінальним правом, адміністративним правом, цивільним правом.

Ефективний механізм правового регулювання забезпечення кібербезпеки в частині застосування відповідальності можливий тільки за умови поєднання (кумуляції) різних її видів. Відповідно, розробка єдиної методології застосування відповідальності на підставі кібер-правопорушень вимагає поєднання методологічних засад окремих правових наук (понятійного апарату, конструкцій тощо).

Висновки. «Кібербезпека» як складне явище, що поєднує сукупність захисних дій, є іманентною складовою суспільної організації правці. Це формує певний правоутворюючий потенціал трудового права та стимулює певний напрямок його подальшого розвитку. Правові відносини працівника та роботодавця, пов'язані із «кібербезпекою» (на технологічному, процесному та інших рівнях) мають значну диференціацією. Це відбивається на структурі правових статусах працівників. Перспективним

напрямком правової методології є розвиток єдиного міжгалузевого підходу до регулювання відносин, пов'язаних із «кібербезпекою».

Література:

1. Задерейко О.В., Лигинова Н.І., Троянський О.В. Сучасне кіберсередовище держави як театр бойових дій. У Зб. «Кібербезпека в Україні: правові та організаційні питання : матеріали всеукр. наук. - практ. конф., м. Одеса, 17 листопада 2017 р.». Одеса : ОДУВС, 2017. 204 с.
2. Див. наприклад, Tyler Elliot Bettilyon. Cybersecurity Is About Much More Than Hackinghttps // URL: https://medium.com/s/story/cybersecurity-isnt-just-about-hacks-f11c7ad07660
3. Панасюк О.Т. Техно–футуристическое методологическое эссе о развитии трудового права// WSPÓŁPRACA EUROPEJSKA NR 6(6) 2015 / EUROPEAN COOPERATION Vol. 6(6) 2015. p. 123 – 134
4. Слово «кібер» отримує конкретне контекстне значення, у поєднання із іншими смислами. Морфологічна роль слова «кібер» це префікс. Найбільш поширеним словом, утвореним за його допомогою, є кібернетика.
5. Див. : URL : https://wargaming.com/ru/careers/vacancy_1170316/

Національне законодавство із забезпечення кібербезпеки в Україні

Максимчук І. Р.
студентка 3 курсу
Херсонського факультету
Одеського державного університету внутрішніх справ
Божок С. Г.
старший викладач кафедри адміністративного
права та адміністративного процесу
Херсонського факультету
Одеського державного університету внутрішніх справ
к. ю. н.

Актуальність теми: На сучасному етапі розвитку суспільства наше життя майже неможливо уявити без використання інформаційних технологій. Вони з кожним днем все більше вливаються в життя людини.

Як і в будь-якій сфері, кіберпростір має і негативні сторони. Існує багато загроз у використанні інформаційного простору, таких як: несанкціоноване втручання в роботу комп'ютерних та телекомунікаційних мереж, виготовлення та розповсюдження шкідливого програмного забезпечення, втручання у політичні процеси в країнах та особисте життя громадян, що в переважній більшості носить транснаціональний організований характер.

На жаль, Україну також не оминула проблема, пов'язана з кібербезпекою. Розповсюдження комп'ютерних вірусів, атаки на українські об'єкти фінансового та енергетичного секторів, викрадення інформації – це ще не повний перелік кіберзлочинів, які відомі в Україні.

Водночас набирає нових обертів процес становлення та розвитку національної системи кібербезпеки України. Початок змін в національному законодавстві у сфері кібербезпеки поклала гібридна війна України з Російською Федерацією, у якій застосовується зброя в тому числі й у кіберпросторі.

На даний момент законодавче регулювання кібербезпеки в Україні знаходиться на початку свого формування. Невирішеними є питання державно-приватної взаємодії, триває розробка напрямків до кібероборони, попереду ще великий обсяг роботи, спрямований на нормативно-правове врегулювання у сфері кібербезпеки.

Метою роботи є: дослідження розвитку, удосконалення законодавства у сфері кібербезпеки України.

Об'єктом дослідження є: суспільні відносини щодо кібербезпеки України та розвитку відповідного правового регулювання.

Предметом дослідження є: національне законодавство із забезпечення кібербезпеки в Україні.

Для реалізації державної політики щодо захисту в кіберпросторі державних інформаційних ресурсів та інформації прийнятий Закон від 05.10.17 р № 2163-VIII «Про основні засади забезпечення кібербезпеки України». Цей Закон став основою розвитку державної системи захисту від мережевих погроз.

Зокрема, Закон визначає поняття «кібербезпека» як - захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [1].

Слід зазначити, що адміністративно-правові акти у даній сфері можна поділити на чотири групи:

1) Конституція України і відповідні нормативно-правові акти, які регулюють питання у цій сфері;

2) міжнародно-правові акти, які ратифіковані Верховною Радою України.;

3) нормативно-правові акти органів виконавчої влади;

4) нормативно-правові акти спеціальних суб'єктів забезпечення кібербезпеки [2, с. 119].

Для забезпечення інформаційної безпеки в Україні застосовується досить розгалужена нормативно-правова база. Її складають: Конвенція Ради Європи «Про кіберзлочинність» 2001 року; Закони України «Про інформацію», «Про основи національної безпеки України», «Про Державну службу спеціального зв'язку та захисту інформації України», «Про телекомунікації», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про доступ до публічної інформації», «Про оборону України», «Про засади внутрішньої і зовнішньої політики»; Укази Президента України, зокрема: «Про рішення Ради національної безпеки і оборони України» від 6 травня 2015 року «Про Стратегію національної безпеки України» та «Про рішення Ради національної безпеки і оборони України» від 2 вересня 2015 року; «Про нову редакцію Воєнної доктрини України» [5].

Питання забезпечення інформаційної безпеки та розробки складових державної політики у цій сфері на системному рівні вперше були визначені у рішенні Ради національної безпеки і оборони України «Про невідкладні заходи щодо забезпечення інформаційної безпеки України», введеному в дію Указом Президента України від 23 квітня 2008 року № 377/2008, та у Доктрині інформаційної безпеки України, затвердженій Указом Президента України від 8 липня 2009 року № 514/2009 (втратила силу на підставі Указу Президента України від 6 червня 2014 року № 504/2014). Водночас вказані напрацювання не були своєчасно реалізовані, а система забезпечення інформаційної безпеки, як засвідчив стан протидії інформаційній агресії РФ, залишилась неефективною і такою, що не відповідає національним інтересам України.

Норми національного законодавства у вказаній сфері містять чимало прогалин та колізій, мають суперечливий та безсистемний характер. Тому, є необхідність удосконалення адміністративно-правового регулювання забезпечення інформаційної безпеки України [3, с. 10].

Правове регулювання вжиття заходів з кібербезпеки в Україні в основному було зумовлено вимогами євроатлантичної інтеграції держави і випливало з доктрин, стратегій та настанов НАТО і Євросоюзу.

Зокрема, у п. 2.8 Стратегії національної безпеки, затвердженої Указом Президента України від 12.02.07 р., стан безпеки інформаційно-комп'ютерних систем в галузі державного управління фінансової і банківської сфери, енергетики транспорту, внутрішніх та міжнародних комунікацій охарактеризовано як такий, що наближається до критичного. А у подальшому в п. 4.1 зазначеної Стратегії з метою реалізації державної політики було визнано за необхідне розробку та впровадження національних стандартів та технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих з відповідними європейськими стандартами, у тому числі згідно з вимогами Конвенції про кіберзлочинність. Слід зазначити, що запропонований у першій редакції Стратегії національної безпеки підхід, який з одного боку передбачав пріоритет державного впливу на рівні національних стандартів та технічних регламентів, а з іншого – зумовлював вжиття заходів правового регулювання відповідно до вимог міжнародно-правових актів, взятих на себе міжнародних зобов'язань та вимог гармонізації законодавства до європейських стандартів, був цілком адекватним обстановці та повністю відповідав елементам для створення глобальної культури кібербезпеки, визначеним резолюцією Генеральної асамблеї ООН.

У подальшому Указом Президента України від 08.06.12 р. № 389/2012 було затверджено нову редакцію Стратегії національної безпеки України «Україна у світі, що змінюється». Цей документ доктринального характеру, характеризуючи безпечне середовище, серед чинників впливу на національну безпеку визначав нездатність держави протистояти викликам, пов'язаним із застосуванням інформаційних технологій в умовах глобалізації, насамперед кіберзагрозам. Чинна на той час редакція ст. 8 Закону України "Про основи національної безпеки України" серед загроз в інформаційній сфері визначала:

- прояви обмеження свободи слова та доступу громадян до інформації; поширення засобами масової інформації культу насильства, жорстокості, порнографії;

- комп'ютерна злочинність та комп'ютерний тероризм; розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;

- намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

Таким чином, зазначені новітні виклики та загрози фактично не було визначено на рівні документів стратегічного планування, оскільки комп'ютерна злочинність та комп'ютерний тероризм далеко не повністю охоплюють такі загрози. Серед завдань забезпечення інформаційної безпеки, окрім визначених у першій редакції Стратегії, додатково було зазначено:

- стимулювання впровадження новітніх інформаційних технологій і виробництва конкурентоспроможного національного інформаційного продукту, зокрема сучасних засобів і систем захисту інформаційних ресурсів;

- забезпечення безпеки інформаційно-телекомунікаційних систем, що функціонують в інтересах управління державою, забезпечують потреби оборони та безпеки держави, кредитно-банківської та інших сфер економіки, систем управління об'єктами критичної інфраструктури;

- створення національної системи кібербезпеки.

І нарешті, у чинній редакції Стратегії національної безпеки України, затвердженій Указом Президента України від 26.05.15 р. № 287/2015, серед загроз інформаційній безпеці визначено:

- ведення інформаційної війни проти України;

- відсутність цілісної комунікативної політики держави, недостатній рівень медіакультури суспільства [4].

Отже, сьогодні постає питання про вдосконалення законодавства України у сфері кіберзахисту. Закон від 05.10.17 р № 2163-VIII «Про основні засади забезпечення кібербезпеки України» став основою розвитку державної системи захисту від мережевих погроз. Також важливим є Указ Президента України від 08.06.12 р. № 389/2012, згідно з яким було затверджено нову редакцію Стратегії національної безпеки України. На даний момент Україна продовжує удосконалювати законодавство у сфері кібербезпеки.

Література:

1. Закон України «Про основні засади забезпечення кібербезпеки України». [Електронний ресурс]. Режим доступу : https://zakon.rada.gov.ua/laws/main/2163-19
2 .Демедюк С.В. Адміністративно-правове регулювання відносин у сфері забезпечення кібербезпеки в Україні [Електронний ресурс] *Південноукраїнський правничий часопис*. 2015. № 3. С. 119-123. Режим доступу: http://nbuv.gov.ua/UJRN/Pupch_2015_3_39.
3. Довгань О.Д. Правові засади формування і розвитку системи забезпечення інформаційної безпеки України. [Електронний ресурс]. Режим доступу: file:///C:/Users/u/Documents/Downloads/iblsd_2015_3_3.pdf
4. Доронін І.М. «Правове регулювання забезпечення кібербезпеки у реалізації окремих функцій держави». [Електронний ресурс]. Режим доступу: http://ippi.org.ua/sites/default/files/13_3.pdf
5. Коваленко Н.В. «Про правовий режим кібербезпеки в Україні». [Електронний ресурс]. Режим доступу: http://biblio.umsf.dp.ua/jspui/bitstream/123456789/2286/1/Kovalenko%205.pdf

Правові засади забезпечення кібербезпеки держоргану «Національне агентство з питань запобігання корупції»

Мамедова Е.А.
ад'юнкт Дніпропетровського
державного університету внутрішніх
справ
Мирошниченко В.О.
канд. техн. наук, доцент, професор
Дніпропетровського державного
університету внутрішніх справ

Вітчизняна безпека протягом останнього десятиріччя істотно змінюється, в усьому світі інформаційні технології зробили великий крок вперед, тим самим задав темп і для України. На сьогодні,

у період масового використання всесвітньої мережі Інтернет, набуває актуальності адміністративно-правовий аспект кібернетичної безпеки у державних органах України.

Сприйняття Україною поняття кібербезпеки поки досить загальне, проте ведеться робота по цьому напрямку. Для комплексної боротьби з кібератаками потрібні спільні зусилля держави, міжнародної спільноти та громадян. На разі проблемою кібербезпеки країни займаються різні відомства: Міністерство внутрішніх справ, Державна служба спеціального зв'язку і захисту інформації, Національне агентство з питань запобігання корупції, Національний банк, Служба безпеки України та інші, кожне з них веде статистику відповідних показників та вживає заходи щодо безпеки, проте їхня діяльність охоплює тільки окремі власні сфери відповідальності. Цілісний напрямок та політика у питанні кібернетичної безпеки країни поки відсутні, як і універсальні індикатори заходів, що могли б охарактеризувати рівень кібербезпеки.

Національним агентством з питань запобігання корупції (далі — НАЗК) 10 червня 2016 року прийнято рішення (зареєстровано в Міністерстві юстиції України 15 липня 2016 року за № 958/29088) про початок роботи системи електронного декларування з 1 вересня 2016 року [1]. На сьогоднішній день громадянам України, котрі займають державну посаду, потрібно декларувати статки. Кожного року громадяни України декларують свої статки в електронному форматі, але після періоду декларування, на суди України надходять безліч позовів за порушення вимог фінансового контролю, як від самих громадян та і від контролюючих органів. На що громадяни України поясняють, що не мають ніякого умислу на вчинення адміністративного правопорушення, так само як і не мають ніякого корупційного інтересу при цьому, мети приховати зміни своїх статків не переслідують, оскільки громадянами, котрі реєструють свої електронні декларації, здійснювались неодноразові спроби подати повідомлення про зміни в майновому стані на Інтернет-сторінці НАЗК, з метою його вчасного заповнення і подання, однак не можуть цього зробити через перебої в роботі сервісу, перебоями у внутрішній мережі Інтернет в зв'язку з кібератаками, відсутністю електропостачання в суді, що також підтверджується списками справ призначених до розгляду та актами Тиврівського районного суду Вінницької області за №19 від 26.06.2017 року та №20 від 27.06.2017 року [2]. Це одна з наведених прикладів судової справи через несправність та кібератаки на сервери сайту НАЗК, у той період коли сервери перебувають найбільш завантаженими, а саме у період звітності громадян. На сьогодні НАЗК має дві основні проблеми: це перевантаженість сайту у період звітності та кібератаки, наприклад таке шкідливе ПЗ (Malware) – створення та розповсюдження вірусів і шкідливого програмного забезпечення. Таку кібератаку зазнали багато держорганів України, Malware е хакерська атака вірусом під назвою Petay (також відомий як Petya.A, Petya.D, Trojan.Ransom.Petya, PetrWrap, NotPetya, ExPetr, GoldenEye), котрий був запущений у березні 2016 року. Ця програма котра шифрує файли на жорсткому диску комп'ютера жертви, а також перезаписує і шифрує MBR - дані, необхідні для завантаження операційної системи.

Для того щоб сьогодні НАЗК змогла протидіяти таким кібератакам, на наш погляд потрібно:

1) підвищити рівень кваліфікації фахівців в органах захисту національної безпеки країни;

2) використовувати світовий досвід країн, котрі мають позитивні результати у боротьбі з кіберзлочинністю;

3) постійно оновлювати ліцензоване програмне забезпечення;

4) оновлювати та удосконалювати сервери збереження даних.

Окремі питання використання електронних доказів при розслідувані кіберзлочинів

Сіренко О.В.
доцент кафедри кримінального процесу та
криміналістики
Університет державної фіскальної служби України
к. ю. н.

Кіберзлочин – це кримінальне правопорушення, що вчиняється за допомогою або через комп'ютерні системи, посягає на право захисту від несанкціонованого поширення і використання інформації, негативних наслідків впливу інформації чи функціонування інформаційних технологій, а також інші суспільно небезпечні діяння, пов'язані з порушенням права власності на інформацію та інформаційні технології, права власників або користувачів інформаційних технологій вчасно одержувати або поширювати достовірну й повну інформацію і за яке передбачено кримінальну відповідальність [6, с.48].

«Стрибок» кількості всіх кіберзлочинів відбувся у 2017 році, значною мірою він пов'язаний з вірусом Petya. Відтоді, кількість інформаційних злочинів не зменшується. В 2017 році було зафіксовано 1795 справ, в 2018 – 1023, за останні півроку – 1005. На даний момент в судовому реєстрі є 1500 справ [4].

Зростання кількості кіберзлочинів обумовлюється удосконаленням технічних і програмних засобів, доступних для зловмисників, і посилюється існуванням нелегального ринку з продажу засобів для здійснення кіберзлочинів.

Як зазначають науковці, «кіберзлочини, на відміну від традиційних, мають низку характерних особливостей, серед яких слід зазначити такі: - місце вчинення кіберзлочину, на відміну від традиційних, може знаходитись в різних юрисдикціях – правопорушник активізує кібератаку, наприклад, з Інтернет-кафе однієї країни, бот-мережа знаходиться в іншій, а атакована інформаційна система – у третій; - переважна кількість доказів кіберзлочинів існують в електронній формі (так звані "електронні" або "цифрові" докази). Вони, на відміну від традиційних, можуть швидко знищуватися чи модифікуватися. Для їх отримання, зберігання та аналізу необхідне спеціалізоване обладнання; - внаслідок специфічної природи кіберпростору постраждалий не завжди обізнаний про вчинення кіберзлочину тощо» [3, с.119].

Як зазначають фахівці, «першочерговим завданням слідчого на початковому етапі розслідування кіберзлочинів є аналіз інформаційного середовища вчинення злочину: визначення типу електронно-обчислювальної машини (носія), де зберігалася або оброблялася комп'ютерна інформація, до якої здійснено неправомірний доступ (Web-сервер, персональний комп'ютер, мобільний телефон, електронна кредитна карта), що визначить напрямок всього подальшого розслідування; встановлення типу операційної системи комп'ютера (сервера), до якого здійснено неправомірний доступ (Unix, Linux, Netware, Windows), а також використаного для вчинення злочину програмного забезпечення, що значною мірою допоможе звузити коло можливих підозрюваних; визначення апаратного та програмного забезпечення, яке піддалося впливу під час неправомірного доступу, а також інформації про засоби і знаряддя вчинення такого доступу, що дозволить скласти об'єктивну картину слідів злочину» [2, с.179].

Під час проведення розслідування кіберзлочинів особливу увагу приділяють збиранню доказів. Відповідно до положень кримінального процесуального кодексу, «сторона обвинувачення здійснює збирання доказів шляхом проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій, витребування та отримання від органів державної влади, органів місцевого самоврядування, підприємств, установ та організацій, службових та фізичних осіб речей, документів, відомостей, висновків експертів, висновків ревізій та актів перевірок, проведення інших процесуальних дій, передбачених Кримінальним процесуальним кодексом» [5].

Доказами в кримінальному провадженні є «фактичні дані, отримані у передбаченому цим Кодексом порядку, на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню.

Процесуальними джерелами доказів є показання, речові докази, документи, висновки експертів» [5].

Відповідно до ч. 1 ст. 99, «документом є спеціально створений з метою збереження інформації матеріальний об'єкт, який містить зафіксовані за допомогою письмових знаків, звуку, зображення тощо відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження [5].

До документів, за умови наявності в них відомостей, передбачених частиною першою, можуть належати матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у тому числі електронні).

Електронними доказами є інформація в електронній (цифровій) формі, що містить дані про обставини, що мають значення для справи, зокрема, електронні документи (в тому числі текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи тощо), веб-сайти (сторінки), текстові, мультимедійні та голосові повідомлення, метадані, бази даних та інші дані в електронній формі. Такі дані можуть зберігатися, зокрема, на портативних пристроях (картах пам'яті, мобільних телефонах тощо), серверах, системах резервного копіювання, інших місцях збереження даних в електронній формі (в тому числі в мережі Інтернет) [9].

Електронний документ є досить вразливим, оскільки він може бути легко змінений, знищений тощо. Саме ця його риса, на думку науковців, зумовлює «необхідність створення спеціальних правил фіксації електронної інформації, способів збереження та приєднання їх до матеріалів справи. Зокрема,

на рівні з традиційними правилами поводження із документами, необхідно враховувати технічні особливості збирання, зберігання та використання інформації» [8, с. 82].

Слід погодитись з позицією науковців, які серед неврегульованих та проблемних аспектів використання електронних доказів у кримінальному судочинстві виокремлюють: відсутність чіткого процесуального порядку їх отримання відповідно до кримінального процесуального кодексу України; відсутність підстав визнання електронних доказів недопустимими; відсутність сформованої методики дослідження таких доказів; складності у слідчих під час виявлення та фіксації електронних доказів через недостатність спеціальних знань у слідчих, що зумовлює необхідність залучення спеціалістів для проведення процесуальних дій; відсутність однотипної термінології та урегульованості на законодавчому рівні [1, с.248-249].

Поняття електронних доказів та електронних документів потребує закріплення на законодавчому рівні, а також, з огляду на проблеми, які виникають в процесі виявлення і фіксації доказів через можливість зміни а то і знищення «віртуальних слідів» доказів, нагальним є питання формування методики дослідження електронних доказів, порядок їх збирання та фіксації.

Література:

1. Алєксєєва-Процюк Д.О. Електронні докази в кримінальному судочинстві: поняття, ознаки та проблемні аспекти застосування *Науковий вісник публічного та приватного права.* 2018. Випуск 2. С.247 – 253.

2. Бурбело Б.А. Криміналістичні основи протидії кіберзлочинності. Актуальні питання розслідування кіберзлочинів: матеріали Міжнародної науково-практичної конференції (Харків, 10 грудня 2013 р.). Харків: Харківський національний університет внутрішніх справ, 2013. С. 179–182

3. Гуцалюк М.В. Сучасні тенденції організованої кіберзлочинності *Інформація і право.* 2019. № 1(28). С. 118 - 128

4. Кількість кіберзлочинів в Україні зросла вдвічі за останні п’ять років - Opendatabot. URL: https://mind.ua/news/20203511-kilkist-kiberzlochiniv-v-ukrayini-zrosla-vdvichi-za-ostanni-p-yat-rokiv-opendatabot

5. Кримінальний процесуальний кодекс України: Науково-практичний коментар / Відп. ред.: С. В. Ківалов, С. М. Міщенко, В. Ю. Захарченко. Х.: Одіссей, 2013. 1104 с.

6. Сіренко О.В. Поняття кіберзлочинів та особливості методики їх *розслідування Кібербезпека в Україні*: правові та організаційні питання: матеріали всеукр. наук.-практ.конф., м. Одеса. ОДУВС, 2017. С.48-49

7. Фурман В. Кіберзлочинність. Проблеми доказування Аналітичне видання *“Юрист&Закон”*. Випуск №45. URL: https://artius.ua/novini/statti/ kiberzlochinnist-problemi-dokazuvannya.html

8. Хижняк Є.С. Особливості огляду електронних документів під час розслідування кримінальних правопорушень *Держава та регіони.* №4 (58). 2017. С.80 – 85. URL: http://www.law.stateandregions.zp.ua/archive/4_2017/15.pdf

9. Цивільний процесуальний кодекс України. URL: https://zakon.rada.gov.ua/laws/show/1618-15.

Кібертероризм: поняття та шляхи протидії

Форос Г. В.
доцент кафедри кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішніх справ
к.ю.н., доцент
Ільченко Д.І., Узюм П.А.
курсанти 301 взводу
Одеського державного університету внутрішніх справ

Найбільш вагомою проблемою сучасного світу, що виникає разом із стрімким розвитком інформаційних технологій та глобальної мережі Інтернет, є поява нових видів злочинів, зокрема кібертероризму. Під кібертероризмом розуміється суспільно небезпечна діяльність, що свідомо здійснюється в кіберпросторі (або з використанням його технічних можливостей) окремими особами або організованими групами з терористичною метою та реалізується ними через заздалегідь сплановані й політично вмотивовані кібератаки на ІТС з використанням високих технологій [1, с. 57].

Окремі аспекти явища кібертероризму неодноразово були предметом дослідження у роботах таких зарубіжних та вітчизняних вчених, як М.Делягіна, А.Фороса, Д.Деннінга, В.Ліпкана, І.Міхеєва, К.Герасименка та інших. Саме їх внески мають вагоме значення подальшого висвітлення проблеми.

Головною відмінною рисою кібертероризму від інших видів віртуальних злочинів є безпосередній вплив на суспільство з метою його залякування, паралізації волі членів соціуму, поширенню панічних настроїв, почуття незахищеності. Це досягається шляхом тиражування інформації про загрози насильства, підтримці стану постійного страху з метою досягнення певних політичних чи інших цілей, примусу до певних дій, а також привернення уваги до самої терористичної організації. Кінцевою метою кібернетичної атаки терориста є не тільки демонстрація своїх технічних можливостей, але і спроба за допомогою їх впливати на політичну владу в країні.

Зростання інформаційних технологій дає терористам можливість отримати істотний прибуток при відносно низькому ризику. Вони можуть фінансувати свою діяльність, без використання силових нападів або грабежів банків, які збільшили б ризик виявлення. Для кібертероризму характерно і те, що всі відомі сьогодні хакерські групи і окремі особи не прагнуть афішувати свої дані і виступають виключно під псевдонімом. При цьому слід відрізняти хакера-терориста від простого хакера, комп'ютерного хулігана або комп'ютерного злодія, який діє в корисливих або хуліганських цілях.

Найефективнішою зброєю у боротьбі з цим злочином залишається законодавство, яке потребує постійного вдосконалення. Якщо говорити про міжнародні правові акти в цій сфері, то першим і головним документом, в якому йде про боротьбу з кіберзлочинністю, є Європейська конвенція 2001 року. В Конвенції Ради Європи згадується 4 типи комп'ютерних злочинів, а саме: незаконний доступ; незаконний перехват; втручання в дані; втручання в систему. Згідно з цим документом засобами кібертероризму є: комп'ютерна система, комп'ютерні дані, послуги ІКТ та дані трафіку [2, с. 146].

Кібертероризм як головна складова кіберзлочинності посідає не останнє місце й серед низки загроз національній безпеці та інтересам України. За даними соціологічних опитувань на його поширення нині активно впливають:

1) високий потенціал і професійний рівень українських програмістів, послугами яких охоче користуються навіть такі флагмани програмної індустрії, як «Майкрософт»;

2) здатність молоді швидко опановувати технічні новинки, про які ще вчора вони не мали жодного уявлення;

При цьому до основних чинників, що формують джерела таких загроз, вітчизняні експерти відносять:

• недостатню увагу з боку державних органів до проблем інформатизації;

• відсутність належної державної фінансової підтримки фундаментальних і прикладних вітчизняних досліджень у сфері запобігання та боротьби з кіберзлочинністю

• відставання вітчизняного законодавства в інформаційній галузі від розвинених країн світу в умовах спільного існування у єдиному інформаційному просторі;

• відсутність ефективної політики безпеки комп'ютерних мереж і необхідних програмно-технічних засобів для обмеження доступу до конфіденційної інформації в базах даних;

• розширення можливостей для негативного інформаційного впливу на людину, суспільство та державу за допомогою нових комп'ютерно-телекомунікаційних засобів і технологій, що постійно розвиваються;

• перехоплення електронної пошти, паролів і файлів за допомогою легкодоступних для зацікавлених користувачів програмно-технічних засобів [1, с. 60-61].

Загроза, яка виходить від кібертероризму, величезна, а в деяких випадках, вона може мати незворотній характер. Сучасному суспільству ще тільки належить виробити ефективну систему протидії і боротьби з цим сучасним інформаційним злом.

Отже, протягом тривалого періоду часу благоустрій суспільства та економічна стабільність ґрунтувались на надійній роботі мереж передачі інформації та обчислювальних сервісів. Проте з появою кібертероризму цей процес значно ускладнився внаслідок постійних кібератак на комп'ютерні системи.

В Україні на даний момент не розроблено конкретного нормативно-правового акта, що регулює такий вид злочинності як кібертероризм, тому виникає необхідність у вдосконаленні та доповненні вже існуючого законодавства шляхом переймання досвіду інших країн, а також розробки законів, що відповідають міжнародним стандартам, встановлених у відповідних конвенціях та договорах. Також дієвим напрямом у вирішенні проблеми протидії кіберзлочинності у наш час є міжнародне співробітництво правоохоронних органів у сфері інформаційної безпеки на основі узгодження національного та міжнародного законодавства. основні засади щодо кібертероризму та його протидії.

Література:
1. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. К.: ДУТ, 2015. 288 с.
2. Г.В. Лисиченко, Ю.Л. Забулонов, Г.А. Хміль Природний, техногенний та екологічний ризики: аналіз, оцінка, управління. *Наукова думка*, 2008.

Кіберзлочинність: поняття, види, загрози та ризики

Чижов Д. А.
асистент кафедри приватного права
Інституту управління і права
Національного юридичного університету імені Ярослава Мудрого
доцент кафедри правового забезпечення
Військового інституту
Київського національного університету імені Тараса Шевченка
к. ю. н.

Відповідно до дослідження, здійснюваного Управлінням Організації Об'єднаних Націй з наркотиків і злочинності на тему «Всебічне дослідження проблеми кіберзлочинності та відповідних заходів з боку країн-учасниць, міжнародної спільноти та приватного сектору», можливо виділити 5 груп документів, в які входять документи, розроблені в контексті або під егідою:

- Ради Європи чи Європейського Союзу;
- Організації Об'єднаних Націй (далі – ООН);
- міжурядових африканських організацій;
- Ліги арабських держав;
- Співдружності незалежних держав або Шанхайської організації співробітництва.

Усі ці документи в повній мірі доповнюють один одного, у тому числі в частині, яка стосується підходів та концепцій, описаних в Конвенції Ради Європи про злочинність у кіберпросторі, прийнятій 23 листопада 2001 року в Будапешті, Угорщина (далі – Будапештська конвенція).

На сьогодні Будапештська конвенція є основою для розробки законодавства у сфері боротьби з кіберзлочинами як для загальносвітового законодавства, так і для кожної країни окремо. Будапештська Конвенція потребує від держав: - удосконалювати законодавство для того, щоб компетентні органи мали можливість здійснювати розслідування кіберзлочинів і зберігати електронні докази якнайефективніше, включаючи збирання даних про рух інформації у реальному масштабі часу, термінове збереження і часткове розкриття даних про рух інформації, термінове збереження комп'ютерних даних, арешт і обшук комп'ютерних даних, перехоплення даних змісту інформації; - криміналізувати атаки на комп'ютерні системи і дані (тобто зловживання пристроями, нелегальне перехоплення, незаконний доступ, втручання в дані, втручання у систему), а також правопорушення із використанням комп'ютерів (шахрайство і підробка), правопорушення, пов'язані зі змістом (дитяча порнографія) та правопорушення у сфері авторських і суміжних прав; - розширювати міжнародне співробітництво з іншими країнамиучасницями Конвенції через загальні (взаємна допомога, екстрадиція, добровільне надання інформації) і спеціальні заходи (взаємна допомога щодо доступу до комп'ютерних даних, розкриття та термінове збереження збережених даних про рух інформації, транскордонний доступ до комп'ютерних даних, створення цілодобових мереж). Комітет Конвенції проти кіберзлочинності («Т-CY») був створений для того, щоб допомогти країнамучасницям розглядати необхідність внесення доповнень або протоколів до Конвенції і обмінюватися інформацією.

Крім того, Рада Європи ініціювала Міжнародний проект по боротьбі з кіберзлочинністю, котрий направлений на те, щоб сприяти країнам в питаннях навчання співробітників правоохоронних органів, вдосконалення законодавства, навчання органів прокуратури і суддівського корпусу, вироблення заходів для захисту персональних даних, зміцнення співпраці між державним і приватним сектором, а також захисту дітей від насильства та сексуальної експлуатації.

Власну стратегію щодо вирішення проблем протидії кіберзлочинності розроблено також Європейським поліцейським відомством («Європол»). На сьогодні «Європол» надає членам ЄС аналітичну і слідчу підтримку через свою базу даних злочинів і систему онлайн-розслідувань.

Помітну роль у подоланні проблем міжнародної співпраці у сфері боротьби з кіберзлочинністю відіграє ООН, котра приділяє велику увагу проблемам поширення злочинів, пов'язаних з використання комп'ютерних та інформаційних систем, та боротьби з таким злочинами.

До числа оптимальних заходів у напрямку попередження кіберзлочинності належать розвиток потенціалу органів кримінального правосуддя і правоохоронних органів, прийняття стратегій, законів щодо протидії кіберзлочинності, створення міцної бази знань і співробітництво між органами державного управління, ефективне керівництво, інформаційно-просвітницька діяльність, громадами, приватним сектором і на міжнародному рівні.

Крім того, діяльність кіберзлочинців кваліфікується за статтями Кримінального кодексу України – незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення. Експертами Управлінням ООН з злочинності і наркотиків також зазначається, що визначення поняття «кіберзлочинності» головним чином залежать від того, в яких цілях даний термін буде використовуватися. Засади кіберзлочинності становлять незначне число діянь, направлених проти цілісності, конфіденційності та доступності комп'ютерних систем або даних.

Найпоширеніші злочини - це виведення з ладу комп'ютерних систем компаній і урядових організацій та злом баз даних. Також широко розповсюдженими є крадежі технологій або інновацій і, звичайно, банальна крадіжка грошей. Одна із найбільш поширених схем, коли шахраї крадуть дані зарплатних рахунків співробітників компаній, котрі в подальшому продають їх на чорному ринку.

Варто зазначити, що швидкий розвиток сфери інформаційних технологій безперервно генерує модерні види послуг, в тому числі у фінансовій сфері. Це, в свою чергу, змушує зловмисників вдосконалювати власні здібності та вигадувати нові способи незаконного заробітку в кіберсередовищі.

У типологічному дослідженні MONEYVAL «Кримінальні грошові потоки в мережі Інтернет: методи, тенденції та взаємодія між всіма основними учасниками» розглянуто наступні ризики кіберзлочинності і відмивання злочинних доходів:

- технічні ризики;
- операційні ризики;
- юридичні ризики;
- географічні або юрисдикційні ризики.

Водночас, така класифікацій є дещо узагальненою та потребує більш детального розгляду з урахуванням суті загроз та вразливостей суспільству і державі від кіберзлочинності, наслідків їх реалізації та можливостей їм протистояти чи зменшувати їх вплив.

Виходячи із суті та класифікації кіберзлочинів, можливо виділити наступні загрози суспільству та державі:

- відкритість суспільства та держави. Створена на основі комп'ютерних мереж та інформаційних технологій зручна інфраструктура для міжнародних постачань товарів, надання послуг, переказу коштів між фізичними і юридичними особами, зберігання інформації у мережі Інтернет та під'єднання до неї кожного комп'ютера, надає одночасно широкі можливості як власне кіберзлочинів, так і відмивання грошей від цих або інших злочинів за допомогою комп'ютерних технологій;

- швидкість та невисока вартість злочину. Вищевказана інфраструктура також надає можливість злочинцям швидкого доступу до будь-якої інформації, документів та насамкінець приватної власності, і водночас дешевих, оперативних і практично анонімних платіжних систем, що дозволяє швидко, без додаткових витрат та ефективно приховати сліди злочину та подальшого руху незаконно одержаних доходів;

- висока технологічність. Надзвичайно швидкий розвиток інформаційних технологій та складність цієї сфери поряд з відносно тривалим та бюрократичним підходом до розвитку нормативно-правових баз призводить до значного відставання заходів щодо упередження та боротьби з кіберзлочинністю; - складний характер злочину. Окрім того, що кіберзлочинці одержують фінансові або інші матеріальні вигоди від здійснення злочину, вони використовують комп'ютерні технології, інформаційно-комунікаційні мережі з соціально-психологічних міркувань, зокрема дискредитації урядів і держав, розміщення сайтів терористичної спрямованості, псування і руйнування ключових систем шляхом внесення до них фальсифікованих даних або постійного виведення цих систем з робочого стану (що є свого роду доповненням до традиційного виду тероризму);

- анонімність злочину. Злочинців приваблює відсутність фізичного контакту з жертвою, відносна м'якість покарання в деяких країнах та, безперечно, складність виявлення, фіксування та вилучення криміналістично-значущої інформації у віртуальному просторі;

- транснаціональний та популярний характер злочину. Особливістю даного виду злочинності є те, що підготовка та скоєння злочину, за наявності доступу до мережі Інтернет, може здійснюватись практично з будь-якого місця. А враховуючи, що комп'ютерна техніка та Інтернет-послуги стають доступнішими для все ширшого кола осіб, кіберзлочинність стає все більш популярною.

Кібербезпека вважається політичною, економічною і соціальною загрозою, яка постійно розвивається в усьому світі, розуміється безпека, яка швидко розвивається протягом останнього сторіччя, що вплинуло на безпеку.

Література:

1. Карчевський М. В. Комп'ютерна інформація, як предмет злочину в сфері використання ЕОМ, систем, комп'ютерних мереж та мереж електрозв'язку *Боротьба зі злочинами у сфері комп'ютерної інформації : проблеми та шляхи їх вирішення* : матеріали міжвуз. наук.-практ. конф. 14 груд. 2007 р. Донецьк : Донец. юрид. ін-т, 2012. С. 61-64.
2. Марков В. В. Хакерські атаки на імплантати як один із способів протиправного використання кіберпростору: сутність та види Вісн. Харк. Ун ту внутр. справ. – 2014. – № 2. – С. 139-147.
3. Кримінальний кодекс України [Електронний ресурс] / Офіційний сайт Верховної Ради України. – Режим доступу: http:// zakon1.rada.gov.ua
4. Ращенко Є. Кримінально-правове забезпечення боротьби зі злочинами у сфері використання комп'ютерних технологій Право України. – 2013. - № 10. – С. 87-91.
5. Net Losses Estimating the Global Cost of Cybercrime [Electronic Source] / Center for Strategic and International Studies. – 2014/ - Режим доступу: http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

СЕКЦІЯ 2
АДМІНІСТРАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

Актуальні засади захисту інформації, що обробляється в автоматизованих системах державної прикордонної служби України

Кушнір І.П.
докторант кафедри теорії та історії
держави і права та приватно-правових дисциплін
Національної академії Державної прикордонної
служби України імені Б. Хмельницького
к. ю. н.

Основною невід'ємною складовою та вимогою сучасного цивілізованого суспільства є гарантія інформаційної безпеки. Забезпечення такого стану сприяє гармонійному розвитку як окремої особистості, суспільства, так і міжнародних зв'язків. Впровадження новітніх засобі та методів комунікації, розвиток системи збирання, обробки та зберігання інформації за допомогою інформаційних систем повинні відбуватись рівночасно з втіленням комплексної системи заходів захисту інформації. Особа, що надала інформацію про себе органам влади для обробки, повинна бути впевнена у збереженні цілісності, безпечності обробки та використанні своїх персональних даних.

За останні п'ять років перелік загроз у сфері прикордонної безпеки доповнився гібридними загрозами, які впливають на політичну та економічну обстановку в державі, безпеку і громадський порядок, а також на зростання рівня тероризму та кіберзлочинів. Такі загрози є транскордонними та існують на фоні складної внутрішньої ситуації: повільного розвитку прикордонної інфраструктури, високого рівня корупції, браку мотивованого та навченого персоналу, наявності проблем щодо координації та комунікації суб'єктів інтегрованого управління кордонами, обмеженого фінансування без можливості формування бюджету розвитку [1].

Інформаційні загрози, що виникають у сфері прикордонної безпеки зумовлюють посилення захисту державних кордонів та інтегрування у міжнародну систему безпеки. Питання організації та гарантування безпеки обігу інформації у сфері охорони та захисту державного кордону України стосуються, як персональних даних громадян, що перетинають державний кордон, які проходять службу у Державній прикордонній службі України, службової інформації, а також міжвідомчої інформації що обробляється у інтегрованій міжвідомчій інформаційно-телекомунікаційній системі [2] та автоматизованих інформаційних системах [3; 4]

Система захисту та безпеки обігу інформації у автоматизованих системах Державної прикордонної служби України повинна носити комплексний та безперервний характер. Головними чинниками такого процесу повинні бути: нормативно урегульований, дієвий механізм обробки та захисту інформації; чіткий процес управління та контролю; дотримання усіма користувачами таких систем правового режиму інформації; убезпечення інформації від несанкціонованих дій (у тому числі з використанням комп'ютерних вірусів); своєчасне реагування на кібератаки; пильність та обізнаність користувачів з питань інформаційної безпеки; постійна підготовка, підвищення кваліфікації персоналу Державної прикордонної служби України щодо протидії інформаційним загрозам та володіння навичками й уміннями із захисту електронної інформації.

Література

1. Про схвалення Стратегії інтегрованого управління кордонами на період до 2025 року : розпорядження Кабінету Міністрів України від 24.07.2019 р. № 687-р. *Урядовий кур'єр*. 2019. № 170.
2. Положення про інтегровану міжвідомчу інформаційно-телекомунікаційну систему щодо контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон : наказ Адміністрації Державної прикордонної служби України, Державної митної служби України, Державної податкової адміністрації України, Міністерства внутрішніх справ України, Міністерства закордонних справ України, Міністерства праці та соціальної політики України, Служби безпеки України, Служби зовнішньої розвідки України 03.04.2008 № 284/287/214/150/64/175/266/75. *Офіційний вісник України*. 2008. Ст. 1249.

3. Про затвердження Положення про інформаційно-телекомунікаційну систему прикордонного контролю «Гарт-1» Державної прикордонної служби України : наказ Адміністрації Державної прикордонної служби України від 30.09.2008 № 810. URL : https://zakon.rada.gov.ua/laws/show/z1086-08.
4. Про затвердження Порядку взаємодії інформаційних систем Державної фіскальної служби України та Державної прикордонної служби України щодо обміну інформацією, необхідною для забезпечення контролю при переміщенні осіб та транспортних засобів через державний (митний) кордон України та адміністративний кордон вільної економічної зони «Крим» : наказ Державної фіскальної служби України, Міністерства внутрішніх справ України від 07.09.2017 № 746/759. *Офіційний вісник України*. 2017. № 85. ст. 2585.

Стандарти управління інформаційною безпекою

Рибальченко Л.В.
Дніпропетровський державний університет внутрішніх справ
к.е.н., доцент
Гребенюк А.М.
Дніпропетровський державний університет внутрішніх справ
к.т.н., доцент

Сучасний етап розвитку інформаційних технологій призвів до серйозних змін в житті кожної людини в усьому світі. Але із позитивними змінами виникли і питання різноманітних ризиків, які є небезпечними як для користувачів комунікаційних пристроїв, так і для підприємств з малими та великими мережами, базами, сховищами та банками даних.

В Стратегії національної безпеки України, серед основних загроз національній безпеці, є загрози кібербезпеці і безпеці інформаційних ресурсів: уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак; фізична і моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом [1].

Найважливішою складовою організації є інформація, яка створювалась і накопичувалась роками про покупців, постачальників, бухгалтерські документи, персональні дані співробітників, інформація про технології та інше.

Інформаційна безпека є однією із складових економічної безпеки держави. Із розвитком інформаційних технологій та їх застосуванням в діяльності підприємств, державних структур, сфері послуг та зв'язку, набуває гостра потреба щодо організації сучасних підходів та створенні систем управління та захисту інформаційних систем. Система управління інформаційною безпекою (СУІБ) представляє собою частину загальної системи управління, яка базується на аналізі ризиків та їх прогнозуванні і призначена для проектування, реалізації, контролю, супроводження та вдосконалення заходів у галузі інформаційної безпеки. Складовою інформаційної безпеки є система, яка містить організаційну структуру, політику планування та захисту, обов'язки персоналу, а також ефективний захист її ресурсної складової.

Правильно побудована система забезпечення інформаційної безпеки дає можливість проводити постійний моніторинг за діяльністю підприємства з метою виявлення загроз і профілактики, а також дозволить побудувати ефективну методику боротьби з виникаючими проблемами.

Забезпечення захисту від несанкціонованого доступу, конфіденційність та цілісність інформації є першочерговими завданнями в системі управління інформаційною безпекою підприємства. Розробка і створення комплексних систем захисту інформації є одним з основних напрямків діяльності служби безпеки підприємства.

Загрози інформаційної безпеки зводиться до нанесення збитків підприємству. Більшість великих та малих підприємств, компаній, бізнесу потерпають від знищення, витоку та розголошування інформації, що призводить до великих фінансових збитків.

Для захисту даних від кіберзлочинності, керування інформаційною безпекою та притягнення злочинців до відповідальності, розроблено Міжнародний стандарт управління інформаційною безпекою серії ISO/IEC 27001 - «Інформаційні технології - Методи забезпечення безпеки - Системи управління інформаційної безпеки - Вимоги». Міжнародний стандарт, базувався на BS 7799-2: 2005.

Існують і такі міжнародні стандарти для управління інформаційної безпеки, як:

ISO/IEC 17799: 2005 - «Інформаційні технології - Технології безпеки - Практичні правила управління інформаційної безпеки». Міжнародний стандарт, базувався на BS 7799-1: 2005;

ISO/IEC 27002 - Зараз: ISO/IEC 17799: 2005. «Інформаційні технології - Технології безпеки - Практичні правила управління інформаційної безпеки». Дата виходу - 2007 рік;

ISO/IEC 27005 - Зараз: BS 7799-3: 2006 - Керівництво з управління ризиками ІБ.

Крім цього, ISO 13335 - Міжнародні стандарти безпеки інформаційних технологій, які містять чотири стандарти; ISO / IEC 15408-1: 2009 Інформаційні технології. Методи забезпечення безпеки. Критерії оцінки безпеки IT; CRAMM (метод аналізу та управління ризиками ССТА) – це методологія управління ризиками, у теперішній час є п'ята версія - CRAMM Version 5.0 та багато інших стандартів.

Зараз триває розробка нового стандарту у сфері інформаційної безпеки - ISO/IEC 27552 «Методи захисту. Розширення ISO/IEC 27001 та ISO/IEC 27002 для управління інформацією про конфіденційність. Вимоги та керівні вказівки», який додатково розширює ISO/IEC 27001 для вирішення конкретних потреб у сфері конфіденційності [2].

Висновок. Забезпечення інформаційної безпеки відбувається за трьома напрямками: технічні, адміністративні та організаційні заходи. Так як інформаційна безпека є однією із складових системи економічної безпеки, вона набуває значущості не лише для окремого підприємства чи організації, а й для економічної безпеки держави.

Література:

1. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про національну безпеку України**» :** Указ Президента України від 26.05.2015 № 287/2015. URL www.president.gov.ua/documents/2872015-190.
2. ISO/IEC 27552 - Information technology - Security techniques - Extension to ISO/IEC 27001 and to ISO/IEC 27002 for privacy information management - Requirements and guidelines [DRAFT]. URL https://www.iso27001security.com/html/27552.html

Технологічне насильство як сучасна форма домашнього насильства

Постол О.І.
ад'юнкт кафедри адміністративного права
та адміністративного процесу
Одеського державного університету внутрішніх справ

Домашнє насильство є одним із найпоширеніших порушень прав людини у світі, яке в свою чергу має руйнівний вплив на суспільство. Наразі в нашій державі проблемі домашнього насильства приділяється значна увага, зокрема прийняття Закону України «Про запобігання та протидію домашньому насильству» [1] сприяло значним трансформаціям у сфері запобігання та протидії домашньому насильству. Однак звертає на себе увагу факт відсутності будь-яких згадувань в даному Законі про, вчинення домашнього насильства із застосування сучасних інформаційних технологій та щодо інструментів протидії такому насильству. З погляду на факт розповсюдженості та доступності серед населення смартфонів та технологій відеонагляду, загроза переслідування за допомогою сучасних технологій зростає.

Наразі існує досить велика кількість шпигунських програм та/або додатків з функцією відстеження, які доступні для завантаження, крім того, є і цілком законні додатки, які можуть бути неправомірно використані кривдником. Наприклад, додатки, які призначені для пошуку загубленого телефону, можуть бути використані кривдником для відстеження місця перебування постраждалої особи. Також, додатки, які призначені для моніторингу використання Інтернету дитиною, містять посилання на те, як використовувати додаток для читання видалених повідомлень на смартфоні.

До найпоширеніших правопорушень пов'язаних із технологіями можна віднести такі як: переслідування або залякування шляхом відправки повідомлень; використання технології GPS з метою відстеження пересування особи; моніторинг дій та звичок особи через соціальні мережі.

Наприклад, мобільний телефон містить багато інформації про свого власника, тому важливим є забезпечити безпеку та конфіденційність, особливо у випадку, якщо кривдник використовує технології з метою переслідування або контролю постраждалої особи.

До основних кроків забезпечення безпеки та конфіденційності мобільного пристрою можна віднести наступні:

По-перше, необхідно ввести пароль на мобільний телефон. Це перешкоджає тому, аби кривдник мав доступ до налаштувань небажаних програм або навіть встановлення шпигунського програмного забезпечення.

По-друге, необхідно перевіряти обліковий запис на смартфоні. Для власників Android - обліковий запис Google, для власників iPhone - обліковий запис iCloud. Ці облікові записи часто містять резервну копію телефону та в залежності від налаштувань, можуть містити конфіденційну інформацію, зокрема фотографії, контакти, нотатки, та іншу особисту інформацію.

Важливо зазначити, що дані облікові записи можуть бути доступні і через інші телефони та комп'ютери. Тобто, якщо кривднику відомі ім'я користувача та пароль для облікового запису, він матиме можливість увійти до системи та переглянути інформацію, яка зберігається на телефоні постраждалої особи. Аби запобігти таким діям, необхідно переконатися, що ім'я користувача та пароль облікового запису нікому не відомі, крім того, перевірити наявність підключень інших пристроїв до облікового запису та за їх наявності видалити такі пристрої.

По-третє, важливо знати встановлені додатки на телефоні. Деякі із додатків використовують інформацію з телефону для роботи (наприклад, для додатку Google Maps аби вказати направлення, необхідно знати місце розташування користувача), у той час, інші додатки можуть ділитися інформацією на телефоні більш небезпечними способами. Тому, аби убезпечити витік інформації з телефону необхідно: видалити додатки, які не використовуються, особливо якщо в них є права на доступ до даних; заборонити доступ до даних додаткам, які цього не потребують (наприклад, додатки з іграми, які не пов'язанні із місцем розташування, не потребують інформації щодо місця розташування та не повинні її вимагати; встановити антишпигунські та антивірусні інструменти.

По-четверте, необхідно контролювати підключення до Wi-Fi та Bluetooth. Більшість смартфонів запитують підтвердження щодо підключення вперше до мережі - Wi-Fi або пристрою Bluetooth, однак якщо підключення відбулося один раз, воно автоматично підключатиметься знову, коли пристрій буде знаходитися в межах діапазону. Якщо це не захищена мережа - Wi-Fi або пристрій Bluetooth щодо якого є довіра (наприклад, коли особа має інший пристрій Bluetooth), після завершення підключення необхідно «забути» мережу - Wi-Fi або пристрій Bluetooth.

Важливо зауважити, що найпростішим шляхом для кривдника дізнатися про життя постраждалої особи є соціальні мережі, які з роками набувають все більшої популярності. Сайти соціальних мереж, такі як, Facebook, Instagram, Twitter дозволяють без ускладнень знаходити та стежити за людиною. Якщо в соціальних мережах використовуються облікові записи, то налаштування конфіденційності та налаштування автоматичного обміну даними можуть наражати постраждалу особу на ризик. Аби попередити доступ кривдника до сторінки соціальної мережі важливо: використовувати налаштування конфіденційності аби контролювати хто може бачити особисті данні; налаштувати параметри облікового запису, щоб заблокувати небажаних користувачів, які можуть переглядати сторінку; замінити зображення профілю з власного фото на більш загальне зображення; частіше змінювати пароль облікового запису (наприклад, кожні три місяці); у разі підозри перевірки соціальної мережі, можливо створити обліковий запис з використання анонімного імені та облікового запису електронної пошти.

Не менш важливим для постраждалої особи є конфіденційність спілкування. Наразі найпоширенішими додатками для спілкування є Viber, Telegram, WhatsApp. Аби кривдник не мав можливості читати повідомлення, слід обирати зашифровані повідомлення. У зазначених додатках при використовуванні функції шифрування, навіть при зломі аккаунту читання чатів є неможливим. Важливо, що у додатку Telegram можливо налаштувати повідомлення на «самознищення», які через певний проміжок часу самостійно видаляються.

Важливо зазначити, що під час розгляду у суді справ про адміністративні правопорушення про вчинення домашнього насильства, судді, відповідно до статті 251 КУпАП [4] можуть вимагати доказів наявності адміністративного правопорушення, які окрім пояснень потерпілої особи та свідків, включають показання технічних приладів та засобів. Це можуть бути, фотографії, відеозаписи, текстові повідомлення, електронні листи, повідомлення в соціальних мережах. Ті ж самі вимоги пред'являються при прийнятті рішення по кримінальному провадженню щодо вчинення домашнього насильства. Відсутність доказової бази доволі часто призводить до повернення суддями матеріалів справ на доопрацювання органами поліції або до їх закриття у зв'язку з відсутністю факту правопорушення [5].

Тому для забезпечення доказової бази у випадках домашнього насильства, доцільно за можливості фіксувати та зберегти все, що пов'язано з подією.

З огляду на висвітлене, слід зауважити, що хоча в національному законодавстві існують певні норми, які захищають постраждалих осіб від незаконного втручання технологій в їх особисте життя, однак а ні в Законі України «Про запобігання та протидію домашнього насильства», а ні в інших нормативних актах у сфері запобігання та протидії домашньому насильству не містяться визначення вчинення домашнього насильства з використанням сучасних технологій.

Можливо домашнє насильство вчинене із застосуванням інформаційних технологій можна було б віднести до психологічного насильства, яке в Законі визначено, як форма домашнього насильства, що включає словесні образи, погрози, у тому числі щодо третіх осіб, приниження, переслідування, залякування, інші діяння, спрямовані на обмеження волевиявлення особи, контроль у репродуктивній сфері, якщо такі дії або бездіяльність викликали у постраждалої особи побоювання за свою безпеку чи безпеку третіх осіб, спричинили емоційну невпевненість, нездатність захистити себе або завдали шкоди психічному здоров'ю особи.

Однак, при цьому домашнє насильство, вчинене із застосування інформаційних технологій, може підпадати під економічну форму домашнього насильства, а саме у частині позбавлення або контролю коштів, а також під сексуальну форму домашнього насильства, наприклад, шляхом розповсюдження фотографій сексуального характеру, та навіть під фізичну форму домашнього насильства у частині незаконного позбавлення волі, що стає можливим завдяки новітнім технологіям «розумного будинку».

Тому, на нашу думку, необхідним є виокремлення домашнього насильства вчиненого з використанням інформаційних технологій в окрему форму домашнього насильства - «технологічне насильство», що значно полегшило б його ідентифікацію.

Література:

1. Про запобігання та протидію домашньому насильству: Закон України від 07.12.2017 № 2229-19. URL: http://zakon3.rada.gov.ua/laws/show/2229-19;
2. Кодекс України про адміністративні правопорушення: Кодекс від 07.12.1984 № 8073-X. URL: http://zakon3.rada.gov.ua/laws/show/80731-10;
3. Постол Е.И., Ковалева Е.В. Административная ответственность за совершение домашнего насилля. *Международный научно-практический журнал «Legea si viata»*. – май 2019. - №5/2. С. 83-87.

Кіберзлочинність в Україні: види, наслідки та способи боротьби

Бурцева І.В.
студентка навчальної групи 17ПЗДС-2
Херсонського факультету
Одеського державного університету внутрішніх справ
Божок С.Г.
викладач кафедри адміністративного права
та адміністративного процесу
Херсонського факультету
Одеського державного університету внутрішніх справ

Актуальність: зумовлена тим, що піднята проблема в статті, досить детально вивчається як з теоретичних так і з практичних позицій в нашій країні. Такі поняття як: «кіберзлочинність», «хакери», «комп'ютерний злом», «крадіжка машинного часу» - ці терміни вже перестали бути екзотикою для юристів. Проблеми протидії злочинам у сфері використання комп'ютерної техніки активно обговорюється науковцями, досить швидко розвивається практика застосування відповідних норм законодавства стосовно відповідальність за вчинене. Вивчення стану наукової розробленості зазначеної проблеми забезпечення кібербезпеки показало, що на сучасному етапі спеціального дослідження з цих питань не проводилося. Проте, окремі аспекти такої діяльності , розглядалися в наукових роботах І.М. Забара, О.Ю. Запорожець, В.К. Конах, В.А. Ліпкан, А.М. Орлеан, Є.Б. Тіхомірової та ін.

Метою: даної статті є визначення концептуальних підходів щодо забезпечення безпеки в кіберпросторі, дослідження сучасних правових і організаційних засад кібербезпеки, з'ясування перспективних напрямків удосконалення механізму забезпечення кібербезпеки в Україні.

Основний виклад інформації. Практично кожен чув про кіберзлочинність і, можливо, навіть особисто з нею зіштовхувався. Кіберзлочинність включає в себе різні види злочинів, що здійснюються за допомогою комп'ютера і в мережі Інтернет.

Об'єктом кіберзлочинів є персональні дані, банківські рахунки, паролі та інша особиста інформація як фізичних осіб, так і бізнесу та державного сектору. Кіберзлочинність є загрозою не тільки на національному, а й на глобальному рівні.

На сьогодні комп'ютерні злочини - це одна з найдинамічніших груп суспільно небезпечних посягань . Швидко збільшуються показники поширення цих злочинів, а також постійно зростає їх

суспільна небезпечність. Це зумовлене прискореним розвитком науки й технологій у сфері комп'ютеризації, а також постійним і стрімким розширенням сфери застосування комп'ютерної техніки.

Відповідно до українського законодавства, кібербезпека – це захищеність життєво важливих інтересів людини й громадянина, суспільства та держави у процесі використання кіберпростору, яка забезпечує сталий розвиток інформаційного суспільства і цифрового комунікативного середовища, своєчасне виявлення, запобігання та нейтралізацію реальних і потенційних загроз національній безпеці України у кіберпросторі (п. 5 ч. 1 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України») [1].

У глобальному розумінні, кібербезпекою є реалізація заходів із захисту мереж, програмних продуктів та систем від цифрових атак.

В Україні до кіберзлочинів відносять порушення авторського права і суміжних прав, шахрайство, незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення; ухилення від сплати податків, зборів (обов'язкових платежів), ввезення, виготовлення, збут і розповсюдження порнографічних предметів, незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю.

Об'єктом кіберзлочинів може стати будь-який користувач інтернету.

В Україні політика щодо кібербезпеки покладається на низку державних органів, а саме на Державну службу спеціального зв'язку та захисту інформації України, Національну поліцію України, Службу безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України. В кожному із зазначених органів діють відповідні підрозділи [2].

Найпоширенішими видами таких злочинів є:

- Кардинг – використання в операціях реквізитів платіжних карт, отриманих зі зламаних серверів інтернет-магазинів, платіжних і розрахункових систем, а також із персональних комп'ютерів (або безпосередньо, або через програми віддаленого доступу, «трояни», «боти»).
- Фішинг – вид шахрайства, відповідно до якого клієнтам платіжних систем надсилають повідомлення електронною поштою нібито від адміністрації або служби безпеки цієї системи з проханням вказати свої рахунки та паролі.
- Вішинг – вид кіберзлочинів, у якому в повідомленнях міститься прохання зателефонувати на певний міський номер, а при розмові запитуються конфіденційні дані власника картки.
- Онлайн-шахрайство – несправжні інтернет-аукціони, інтернет-магазини, сайти та телекомунікаційні засоби зв'язку.
- Піратство – незаконне розповсюдження інтелектуальної власності в Інтернеті.
- Кард-шарінг – надання незаконного доступу до перегляду супутникового та кабельного TV.
- Соціальна інженерія – технологія управління людьми в Інтернет-просторі.
- Мальваре – створення та розповсюдження вірусів і шкідливого програмного забезпечення.
- Протиправний контент – контент, який пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості і насильства.
- Рефайлінг – незаконна підміна телефонного трафіку [3].

Повністю захистися від кібер атак неможливо. Проте виконання хоча б мінімальних правил техніки безпеки поводження в мережі значно підвищить шанси, що вас не зламають.

Отже, пропоную ознайомитися з основними правилами:

- користуватися виключно офіційним програмним забезпеченням (ПЗ) і вчасно його оновлювати;
- не завантажувати програмне забезпечення з ненадійних джерел;
- використовувати антивіруси для роботи з комп'ютерами;
- нікому не передавати особисті персональні дані (пін коди карток, паролі до акаунтів тощо), навіть якщо вам намагаються вказати на необхідність таких дій з метою вирішення певного питання;
- створювати складні паролі;
- не здійснювати платіжних операцій у відкритій, незахищеній мережі Wi-Fi;
- не відкривати файли та листи від підозрілих джерел;
- не переходити на підозрілі посилання та за спливаючими вікнами;
- не заходити на ненадійні сайти та не завантажувати з них жодних ПЗ;
- не вставляти у свій комп'ютер флешки та зовнішні диски, якщо не довіряєте повністю їх джерелу;
- періодично здійснювати резервне копіювання важливої інформації;

- тримати свої гаджети в полі зору, коли знаходитися у місцях, де до них може бути доступ сторонніх осіб.

Виконання зазначених засобів безпеки дозволить лише мінімізувати можливість випадкового несанкціонованого проникнення у ваші пристрої та системи. Однак неможливо надати повної гарантії уникнення зламу. Для максимальної мінімізації таких ризиків компаніям рекомендовано користуватися послугами спеціалістів у сфері кібербезпеки з чітким виконанням всіх інструкцій, які вони зазначають. [4]

Висновок: Зрозуміло, що в епоху інформаційного суспільства складно повністю уникнути загроз у кіберпросторі. Цифрова епоха принесла в економіку не тільки позитивні трансформації. Частиною «ціни», яку доводиться платити за інновації в цифровій сфері, є ризики кіберзлочинів, які набувають все більших масштабів. Однак ми сподіваємося, що усвідомлення проблеми державою і бізнесом, створення сучасного правового поля, а також дотримання заходів кібербезпеки значно підвищать рівень стійкості від атак.

Безумовно, неможливо захиститися від усього, але низка превентивних заходів, які вже зараз здатні здійснювати фахівці в кіберсфері та власники бізнесу, можуть запобігти неприємним наслідкам і зберегти гроші.

Проблема профілактики і стимулювання кіберзлочинності в Україні – це комплексна проблема. Сьогодні закони повинні відповідати вимогам, що пред'являються сучасним рівнем розвитку технологій. Пріоритетним напрямком є також організація взаємодії і координація зусиль правоохоронних органів, спецслужб, судової системи, забезпечення їх необхідною матеріально-технічною базою. Жодна держава сьогодні не в змозі протистояти кіберзлочинності самостійно. Нагальною є необхідність активізації міжнародної співпраці в цій сфері. Експерти впевнені: саме хакери в недалекому майбутньому стануть загрозою номер один, змістивши тероризм.

Література:

1. Закон України «Про основні засади забезпечення кібербезпеки України». URL : https://zakon.rada.gov.ua/laws/main/2163-19
2. Конвенція про кіберзлочинність. Конвенція ратифікована із застереженнями і заявами Законом №2824-IV від 7.09.2005 ВВР 2006 №5-6 ст.7
3. Прохоренко В. Кіберзлочинність для України стає актуальним поняттям – НБУ. *Економічна правда*. від 26 лютого, 2013року.
4. Комп'ютерна злочинність. К.: Атіка, 2002.

Система забезпечення кібербезпеки в Україні: сутність та призначення

Семеног А.О.
студентка 3 курсу
Херсонського факультету
Одеського державного університету внутрішніх справ
Божок С.Г.
викладач кафедри адміністративного права
та адміністративного процесу
Херсонського факультету
Одеського державного університету внутрішніх справ

На сьогодні досить актуальним є питання яке стосується кібербезпеки в Україні. Забезпечення належного рівня кібернетичної безпеки є необхідною умовою розвитку інформаційного суспільства. Нині керівництво провідних держав світу приділяє посилену увагу створенню та удосконаленню ефективних систем захисту критичної інфраструктури від зовнішніх і внутрішніх загроз кібернетичного характеру.

В Україні відбувається процес формування системи кібернетичної безпеки. Як складову такої системи варто розглядати єдину загальнодержавну систему протидії кіберзлочинності, пропозиції щодо створення якої ще у 2011 році доручалося розробити Кабінету Міністрів України за участю Служби безпеки [1].

Дослідженням цього питанням займалися багато видатних вітчизняних дослідників, а саме: В.А. Ліпкана, І.В. Тімкіна, Н.Є. Новікова, І.В. Діордіци, С.В. Мельника, В.І. Кащука, В.П. Шеломенцева та інших.

Метою статті є дослідження системи забезпечення кібербезпеки.

Кібербезпека — це процес застосування заходів безпеки з метою забезпечення конфіденційності, цілісності та доступності даних. У широкому сенсі і під системою забезпечення кібербезпеки варто розуміти сукупність організаційно об'єднаних органів управління, а саме: державних органів, громадських організацій, посадових осіб та окремих громадян, які спрямовують свою діяльність на створення умов, для реалізації національних інтересів у кіберпросторі, а також сил, засобів і методів, які використовуються для досягнення даної цілі відповідно до законодавства України .

Система забезпечення кібербезпеки є єдиним державно-правовим механізмом, який в свою чергу за допомогою всіх його суб'єктів діють чітко в межах визначених законодавством. У вузькому сенсі система забезпечення кібербезпеки – сукупність органічної об'єднаних спільними цілями суб'єктів, які здійснюють свою діяльність у кіберпросторі з метою реалізації національних інтересів [2].

Офіційне визначення поняття кібербезпеки міститься в Стратегії кібербезпеки, де, сповідуючи калькований підхід із Закону України «Про національну безпеку України», в якому визначено поняття «національна безпека» - захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз [3].

Кожна держава індивідуально визначає сфери, які вона відносить до кібернетичної безпеки, перелік об'єктів і суб'єктів її забезпечення. Система забезпечення кібербезпеки має бути цілісною і елементи якої (суб'єкти та об'єкти) тісно пов'язані між собою.

У якості основних об'єктів системи забезпечення кібербезпеки слід визначити: особу – її права і свободи на збирання, зберігання, використання та поширення інформації, що реалізовуються за допомогою ІТС; суспільство – та частина його духовних, морально-етичних, культурних, історичних, інтелектуальних і матеріальних цінностей, що формуються з використанням ІТС; державу – її суверенітет і недоторканність у кіберпросторі, спроможність виконувати свої функції за допомогою ІТС.

Кібернетична безпека будь-якої держави призначена на виконання певних дій, спрямованих, перш за все, на захист національних цінностей, реалізацію національних інтересів, забезпечення кібернетичної безпеки, що являє собою організаційне об'єднання державних та недержавних інституцій, а також інших суб'єктів.

Суб'єкти забезпечення кібернетичної безпеки – державні органи, (передусім інституції сфери безпеки і оборони України), органи місцевого самоврядування, підприємства, установи, організації незалежно від форми власності які здійснюють проектування, впровадження та експлуатацію складових критичних об'єктів національної інформаційної інфраструктури або забезпечують їх кіберзахист .

Серед суб'єктів забезпечення кібернетичної безпеки виділяють загальні, до яких відносяться: Президент України; Верховна Рада України; Рада національної безпеки і оборони України; Кабінет Міністрів України; Збройні Сили України; Служба безпеки України; Служба зовнішньої розвідки України; місцеві державні адміністрації та органи місцевого самоврядування тощо. А також виділяють спеціальні суб'єкти, які представленні державними органами, крім загальних функцій, уповноважені на здійснення боротьби з кіберзлочинністю та кібертероризмом: Міністерство внутрішніх справ України; Служба безпеки України; Державна служба спеціального зв'язку та захисту інформації України; Міністерство юстиції України; Генеральна прокуратура України [4, с. 312].

Суб'єкти системи забезпечення кібернетичної безпеки знаходяться у тісній взаємодії між собою, але при цьому кожен з них спеціалізується на вирішенні конкретних завдань і задач відповідно до своєї предметної компетентності та в межах повноважень визначених законодавством. Завдання щодо забезпечення національних інтересів покладаються, передусім, на державу та її інститути, а суспільство і громадяни беруть меншу участь у відповідних процесах. [5].

Таким чином, основним призначенням системи забезпечення кібербезпеки є сприяння у досягненні цілей кібернетичної безпеки, а тому основною функцією даної системи можна визначити забезпечення збалансованого існування інтересів особи, суспільства і держави шляхом здійснення перевірок, діагностування, виявлення та ідентифікацію, запобігання та припинення, мінімізацію та нейтралізацію дії внутрішніх і зовнішніх загроз і небезпек у кібернетичній сфері, а ефективність функціонування системи забезпечення кібербезпеки залежить від досконалості нормативно-правового регулювання. Законодавчо-правову основу забезпечення національної безпеки України становлять Конституція України, Закони України «Про національну безпеку України», «Про Раду національної

безпеки і оборони України», «Про Службу безпеки України, міжнародні договори й угоди, укладені чи визнані Україною, які відповідають національним інтересам України, тощо [6].

Таким чином, за своєю організаційно-функціональною та ресурсною спроможністю система забезпечення кібернетичної безпеки повинна гарантувати інформаційний суверенітет, територіальну цілісність, сталий розвиток, добробут та кібернетичну безпеку громадян.

Література:

1. Ліпкан В.А. Поняття системи забезпечення національної безпеки України *Право і Безпека*. 2003. Т. 2. № 4. С. 57–60.
2. Шеломенцев В.П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2012. Вип. 1. С. 312–320.
3. Закон України «Про національну безпеку України»//Відомості Верховної Ради (ВВР), 2018, № 31, ст.241// URL: https://zakon.rada.gov.ua/laws/main/2469-19.
4. Шеломенцев В.П. Формування законодавчих основ забезпечення кібербезпеки *Інформаційна безпека: виклики і загрози сучасності* : зб. матеріалів наук.-практ. конф., 5 квітня 2013 року, м. Київ. К.: Наук.-вид. центр НА СБ України, 2013. 416 с.
5. Бабич Є.Ю. Забезпечення кібербезпеки в Україні. *Актуальні задачі та досягнення у галузі кібербезпеки* : матеріали Всеукр. наук.-практ. конф., м. Кропивницький, 23–25 листоп. 2016 р. Кропивницький : КНТУ, 2016. С. 77–78.
6. Єрьоміна Л.В. Напрями удосконалення законодавства України у сфері кібербезпеки: термінологічний аспект. *Інформаційна безпека: виклики і загрози сучасності* : зб. матеріалів наук.-практ. конф., 5 квітня 2013 року, м. Київ. К. : Наук.-вид. центр НА СБ України, 2013. 416 с

Забезпечення кібербезпеки в управлінні організацією праці на підприємстві

Титаренко І.В.
кафедра менеджменту
Полтавського університету економіки та торгівлі
к. е. н.

Підвищення рівня інформаційного забезпечення діяльності підприємства надає змогу зростанню оперативності та адекватності процесу прийняття управлінських рішень, нарощенню показників ефективності діяльності підприємства, стабілізації його фінансового стану. Основними складовими для гарантії для формування достовірної інформації для процесу прийняття рішень є безпека таких інформаційних потоків: кібербезпека в управлінні організацією праці на підприємстві. Найвідповідальнішим об'єктом захисту інформації виступає – управлінська інформація, яка уособлює в собі повністю всі перетворена інформація на дані, які в подальшому виступають як результати діяльності, прогнозні показники, що будуть використовуватися для прийняття управлінських рішень. В процесах обробки, проходження та зберігання таких показників на комп'ютерних носіях безпосередню участь беруть спеціалісти, які забезпечують повну взаємодію з використанням такого масиву даних та частково захист такої інформації.

Кібербезпека забезпечує цілісність, якісне зберігання та цільове призначення інформації для апарату управління. Захищеність інформації полягає в забезпеченні комплексу організаційно-технічних заходів та управлінні організації кадрової роботи, спрямованої на збереження комерційної таємниці та налагодження системи управління базами даних таких інформаційних потоків.

Основним способом захисту інформації - є впровадження послідовних рівнів заходів контролю за доступом до комп'ютерної системи та файлів. Застосування засобів захисту, що вбудовуються у програмне забезпечення, повинні бути розроблені з низкою адміністративних заходів на різних рівнях управління підприємства.

Пропонуємо розробити заходи щодо організації праці та її управління таким чином, щоб роль виконання своїх обов'язків кожного працівника різного рівня здійснювалася під управлінням менеджерів відповідного рівня.

Використання знань та навиків в спеціалізованій роботі безпосередньо допомагають, проте їх недостатньо для зосередженого виконання дій, які забезпечать збереження комерційних даних на підприємстві. Таким чином, для ефективного управління та з метою забезпечення безпеки даних на підприємстві, пропонуємо заходи для організації праці, які допоможуть налагодити роботу працівників різних рівнів відповідно до кіпербезпеки. Такими заходами виступають:

- спеціальне навчання працівників, щодо користування комп'ютерною технікою, програмним забезпеченням та електронними носіями;
- проходження спеціальних психологічних тренінгів щодо виявлення неправомірних дій зовнішніх користувачів та інших осіб по використанню комерційних даних;
- здійснення постійного контролю в поточній роботі, в здійснених вчинках та плануванні майбутніх заходів;
- виявлення можливих загроз та їх запобігання в межах комплексу необхідних дій;
- конфіденційність управлінської інформації для працівників, які нею володіють;
- відповідальність кожного працівника за збереження операцій на комп'ютерних носіях;
- обмін інформацією між працівниками щодо безпеки інформації на підприємстві.

Слід відзначити, що управління кібербезпекою входить до загальної системи управління економічною безпекою підприємства, і залежно від розмірів та потужності підприємства.

З метою попередження неправомірного втручання у комп'ютерну інформацію та попередження злочинів із використанням даних пропонуємо створити належну систему захисту цієї інформації, з використанням таких принципів:

- якісне використання та підтримка програмного забезпечення;
- захист конфіденційної інформації;
- персональна відповідальність;
- секретність;
- комплексність заходів;
- контроль доступу до облікових даних;
- розробка правил та процедур на підприємстві по системі безпеки;

Слід відзначити, що до основних напрямків по удосконаленню організаційного забезпечення системи кібербезпеки на підприємстві та якісного управління організацією праці можна запропонувати розробку документу щодо політики правил захисту інформації та інструкції по поведінці працівників апарату управління, а також створення спецслужби та спец комісії щодо регулювання кіберзахисту на підприємстві. Розробка та затвердження нових документів надасть змогу логічній послідовності дій та забезпеченню максимального захисту інформації. Для ширшого розуміння та правомірного використання матеріальних та трудових ресурсів пропонуємо ввести розділ до Наказу про облікову політику підприємства з розкриттям усіх необхідних правил та дій у веденні бухгалтерського обліку, резерву витрат, пов'язаних з кібербезпекою та внутрішнім контролем на підприємстві.

За допомогою вище перелічених заходів щодо безпеки в управлінні організацією праці на підприємстві, можна досягнути високих результатів роботи та системності захисту управлінської інформації.

Література:

1. Про внесення змін до Закону України «Про основи національної безпеки України»: проект Закону України щодо кібернетичної безпеки України від 07.03.13 р. № 2483. URL www.w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=45998
2. Про Національну програму інформатизації : закон України від 4.02.1998 р. №74/98-ВР URL: http://zakon4.rada.gov.ua/laws/show/74/98-%D0 %B2 %D1 %80
3. Дубов Д.В., Ожеван М.А.. Кібербезпека : світові тенденції та виклики для України. К. : НІСД, 2011. 30 с.

Проблеми адміністративно-правового регулювання хмарних технологій в аспекті розповсюдження об'єктів авторських і суміжних прав, виражених у цифровій формі

Жогов В.С.
ад'юнкт кафедри кібербезпеки
та інформаційного забезпечення
Одеського державного університету внутрішніх справ

В останні кілька років хмарні технології увійшли в десятку найбільш популярних стратегічних комп'ютерних технологій, зайнявши вирішальну позицію серед ресурсних інтересів комерційних підприємств і представників бізнесу в силу високої потенціальної можливості знижувати вартість витрат на комп'ютерне та технологічне забезпечення. Представникам же малого бізнесу вони дозволяють вийти на більш високі рівні ринку без необхідності витрачатися на підтримку ефективності

роботи комп'ютерної техніки, а також витрачати істотні матеріальні ресурси на закупівлю програмного забезпечення або технічних носіїв.

Міжнародна інформаційна корпорація (International Data Corporation (IDC) в 2012 р спрогнозувала, що протягом найближчого десятиліття більше 80% нових комерційних додатків для бізнесу буде створюватися винятково на базі хмарних технологій [1]. Європейська комісія також передбачає, що розвиток хмарних технологій буде додавати до ВВП Євросоюзу до 250 млрд євро на рік, а до 2020 р сукупний вплив на економіку за період з 2015 р до 2020 р оцінюється в 600 млрд євро [2].

В одному з досліджень, що стосуються такого способу передачі і обробки інформації йдеться, що основна мета сучасних комп'ютерних технологій полягає у знищенні бар'єрів між інформаційними послугами [3]. Це виражається саме в тому, що сучасні технології не залежать більше від географічного положення провайдера послуг і ефективність ринку таких послуг прямо похідна від швидкості доступу, наданого користувачу, незалежно від місця його знаходження. Такі зміни ускладнили законодавче регулювання захисту об'єктів авторського права, виражених у цифровій формі і, в той же час, вивели їх на міжнародний рівень не тільки в правовому сенсі, а й у фактичному.

Варто підкреслити, що в правових системах різних країн існують схожі норми регулювання відносин в даній сфері. Так, в законодавстві США застосовується доктрина сумлінного використання творів (англ. Fair use) [4] та Закон США «Про захист авторських прав у цифрову епоху» (Digital Millennium Copyright Act) [5]. В країнах ЄС діє Директива ЄС N 2000/31 / ЄС «Про деякі правові аспекти інформаційних послуг на внутрішньому ринку, зокрема, про електронну комерцію» [6].

У той час як законодавство зарубіжних країн зробило крок далеко вперед у питанні регулювання відносин, що формуються при використанні хмарних технологій, постійно доповнює і вдосконалює його з урахуванням швидко мінливих технологічних і соціальних умов надання хмарного сервісу, Україна поки не визначилася у виборі загальної стратегії регулювання таких відносин.

Сьогодні робляться численні спроби створення експертних рад, комісій і робочих груп для створення нормативного правового акта, що регулює відносини, що виникають при використанні хмарних технологій. І до тих пір, поки відсутнє спеціальне регулювання відносин, що виникають при використанні хмарних технологій, до таких відносин доведеться застосовувати існуюче законодавство і тільки в тій частині, яка хоч скільки-небудь може бути застосовна.

Звісно ж, що правове регулювання відносин, що виникають при використанні хмарних технологій, до сих пір є дискусійною темою в багатьох аспектах, в тому числі в питаннях охорони авторського права і суміжних прав на результати інтелектуальної діяльності.

На думку А. Бережного проблеми відсутності чіткого нормативного регулювання відносин, пов'язаних з хмарними технологіями, а також можливі ризики втрати даних або доступності таких послуг не дозволяють повністю покластись на сумлінність постачальника хмарних послуг, що спричиняє необхідність розвитку нормативно-правової бази та механізмів контролю за її дотриманням [7].

При використанні хмарних технологій важливо дотримуватись законодавчих вимог до обробки персональних даних та іншої інформації, що може бути незаконно використана іншими. Крім того, максимально чітко повинен проводитися облік результатів від використання таких послуг, з обов'язковим розмежуванням з постачальником послуг прав на одержувані результати.

Тема «хмар» є дуже актуальною і породжує безліч дискусій та запитань. Недарма, дві доповіді на секції «VII Міжнародного форуму «Інтелектуальна власність - XXI століття», присвячені правовій охороні комп'ютерних програм, так або інакше торкалися проблеми хмарних технологій, що виникають у зв'язку з їх використанням. Зокрема, було відзначено, великий вплив на новий підхід до розуміння авторського права зробило впровадженнях хмарних технологій [8].

На сьогоднішній день в практиці не розроблений механізм визначення, чи правомірно відбувається поширення того чи іншого твору за допомогою мережі Інтернет. Це питання постійно хвилює розуми вчених і авторів. Звісно, визначити правомірність використання твору, викладеного в Facebook, дуже складно, відповідно подальше правомірне використання такого твору з урахуванням норм законодавства ставиться під питання.

Складніша ситуація з неправомірним використанням авторських творів, створених та/або які розповсюджуються при використанні хмарних технологій. Користувач хмарного сервісу вступає у відносини з приводу твору, авторські права на яке належать третій особі, при цьому твір виражено в цифровій формі та створено або розміщено з використанням хмарного сервісу таким чином, що інші користувачі можуть отримати доступ до такого об'єкта в будь-який час і з будь-якого місця, керуючись лише власним бажанням.

Таким чином, виходить, що основні труднощі виникають тоді, коли користувачі мають можливість завантажувати або вивантажувати об'єкти інтелектуальної діяльності та здійснювати їх копіювання та розповсюдження.

З огляду на актуальність тематики, в офісі Microsoft Ukraine було проведено семінар на тему «Використання хмарних технологій у бізнесі», на якому представники компанії розповіли про можливості їхнього програмного забезпечення, а також виступили доповідачі від юридичної фірми «Saenko Kharenko», які стверджують про необхідність обов'язкового законодавчого регулювання цієї сфери, оскільки норми чинного законодавства не адаптовані до регулювання правовідносин із застосуванням сучасних технологій [9]. На нашу думку, до проблем хмарних технологій можна також віднести й відсутність методологічної бази щодо взаємодії контролюючих органів з правоохоронними органами в даній сфері.

Можна сказати, що розвиток «хмарних технологій», розширення їх можливостей та велику кількість сфер використання вимагає від законодавця розробки нормативно-правової бази у сфері хмарних технологій, оскільки розповсюдження конкретно хмарної послуги може виходити за географічні межі країни, в якій вона була створена, оскільки більшість великих хмарних провайдерів є резидентами США, Китаю або Євросоюзу. Тому у деяких сферах діяльності для оцінки можливості використання «хмарних» сервісів слід враховувати спеціальне регулювання, яке передбачає застосування особливих засобів і технологій захисту інформації, наприклад, обмеження зберігання інформації за межами України.

Одночасно з цим розвиваються й місцеві оператори хмарних технологіій, які користуються популярністю в нашій державі, тому й їх діяльність також потребує національного нормативного регулювання.

Таким чином, незважаючи на те, що законодавство в області інтелектуальної власності постійно вдосконалюється, використання стрімко розвиваються технологій може сприяти визнанню чинного законодавства в сфері інтелектуальної власності застарілим, що може зумовити підміну законодавчого регулювання звичаями ділового обороту, договірної практики, щоб хоч якось регулювати ці процеси. У зв'язку з цим ми вважаємо необхідним внести поправки в чинне законодавство в частині забезпечення охорони об'єктів авторського права виражених в цифровій формі при використанні хмарних послуг.

Література:

1. Gens, F. IDC Predictions 2012: Competing for 2020 [Електронний ресурс]. – Режим доступу: http://www.virtustream.com/sites/default/files/IDCTOP10Predictions 2012.pdf.
2. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Unleashing the Potential of Cloud Computing in Europe. Brussels, 27.09.2012. COM (2012) 529 final [Електронний ресурс]. – Режим доступу: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF.
3. Vaquero L. M., Rodero-Merino L., Caceres J., Lindner M. A Break in the Clouds: Towards a Cloud Definition. SIGCOMM Computing Community Review, 2009, vol. 39 (1), p. 50–55.
4. CopyrightAct, UnitedStatesCode/Title17 // Режим доступу: http://www.copyright.gov/title17/.
5. DigitalMillenniumCopyrightAct, DMCA // Режим доступу: https://www.aclu.org/text-digital-millennium-copyright-act-dmca.
6. Directive No. 2000/31/EC of the European Parliament and of the Council of 8 June 2000 «On certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)» // Режим доступу: http://www.wipo.int/wipolex/ru/text.jsp?file_id=181678.
7. Бережной А. Облачные вычисления: Новое или хорошо забытое старое? // Режим доступу: http://samag.ru/archive/article/1214
8. VII МЕЖДУНАРОДНЫЙ ФОРУМ «ИНТЕЛЛЕКТУАЛЬНАЯ СОБСТВЕННОСТЬ – XXI ВЕК»: Журнал «Экономические стратегии» («ЭС») Режим доступу: http://www.inesnet.ru/2014/04/vii-mezhdunarodnyj-forum-intellektualnaya-sobstvennost-xxi-vek/
9. «Хмарні» технології в бізнесреаліях України: Всеукраїнське щотижневе професійне юридичне видання «Юридична Газета» Режим доступу http://yur-gazeta.com/publications/actual/hmarni-tehnologiyi-v-biznesrealiyah-ukrayini.html

Одеський державний університет внутрішніх справ
«Кібербезпека в Україні: правові та організаційні питання»

Захист прав та інтересів особи внаслідок розміщення недостовірної інформації щодо неї в мережі Інтернет

Пелюх Р.Р.
курсант 3 курсу Факультету підготовки
фахівців для підрозділів кримінальної поліції
Одеського державного університету внутрішніх справ
Маковій В.П.
завідувач кафедри цивільно-правових дисциплін
Одеського державного університету внутрішніх справ
к.ю.н., доцент

Сучасна інформаційна епоха дає широкі можливості для вираження власних думок, поглядів і переконань. Інтернет є одним із засобів їх вираження. Проте додаткові можливості створюють передумови порушення особистих немайнових прав інших осіб. Саме тому важливо знати способи захисту прав, порушених поширенням недостовірної інформації в мережі Інтернет.

Недостовірною вважається негативна інформація, яка викладена неправдиво, не відповідає дійсності, тобто містить відомості про події та явища, яких не існувало взагалі або які існували, але відомості про них неповні або перекручені. Спробуємо знайти відповідь на питання: що ж розуміється під терміном «негативна» («негативний»), яким чином розуміти словосполучення «негативна інформація»?

У словнику С.І. Ожегова, наприклад, роз'яснено, що «негативный — то же, что отрицательный, противоположный позитивному» (с. 345), а «отрицательный» — это: 1) «заключающий отрицание, отвергающий что-нибудь»; 2) «дурной, плохой» [1. с. 411].

Такий загальний зміст терміну, що аналізується, але, по-перше, цей термін не являється юридичним, доки його роз'яснення відсутнє в законі або не розтлумачене компетентним органом (навіть якщо він згадується в орфографічному, юридичному словнику); по-друге, для цього конкретного випадку він є занадто суб'єктивним і, безперечно, при його застосуванні призведе до різночитань чи навіть помилок.

Так, наприклад, як «негативна» може суб'єктивно сприйматись інформація, яка в загальному розумінні не є такою, і буде абсурдним доведення її достовірності. Те саме стосується й оцінюючих суджень — тобто висловлювань, які фактичних даних не містять, зокрема критика, оцінка дій, вживання мовних засобів на зразок сатири, гіпербол, алегорій, відомих практиці Європейського суду з прав людини (далі — Європейський суд), юрисдикція якого з усіх питань, що стосуються тлумачення і застосування Конвенції про захист прав і основних свобод людини (ратифікована Законом від 17 липня 1997 р. № 475/97-ВР; далі — Конвенція) є обов'язковою.

Конституцією України кожному гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань. Разом з тим відповідно до статті 68 Конституції України кожен зобов'язаний неухильно дотримуватися Конституції та законів України, не посягати на права і свободи, честь і гідність інших людей. Обов'язок не поширювати про особу недостовірну інформацію та таку, що ганьбить її гідність, честь чи ділову репутацію відповідає праву на свободу думки і слова, на вільне вираження своїх поглядів і переконань. У зв'язку з цим передбачено судовий захист права спростовувати недостовірну інформацію про себе і членів своєї сім'ї. Нікому не дозволяється зазнавати втручання в особисте і сімейне життя особи, збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом.

Суди при вирішенні справ про захист гідності, честі та ділової репутації повинні забезпечувати відповідний баланс між конституційним правом на свободу думки і слова, правом на вільне вираження своїх поглядів та переконань, з одного боку, та правом на повагу до людської гідності, конституційними гарантіями невтручання в особисте і сімейне життя, судовим захистом права на спростування недостовірної інформації про особу, з іншого боку.

Спростування недостовірної інформації — це визнання інформації неправдивою у формі, яка є ідентичною чи адекватною до форми поширення неправдивої інформації. Під терміном «поширена» ч. 1 ст. 22 Закону України «Про інформацію» розуміється інформація, що поширюється до необмеженого кола осіб.

Стосовно розгляду питання «цифрового середовища» справа виглядає не з легких. Як зазначає Тарасенко Л.Л., визначення поняття «цифрове середовище» у законодавстві України немає. Цифрове середовище – це ширше поняття, ніж мережа Інтернет. Цифрове середовище включає в себе веб-сайти, електронні документи, файли, в тому числі оцифровані об'єкти інтелектуальної власності, які

використовуються на відповідних пристроях, що не передбачають паперової форми документообігу. Отже, використовуючи це визначення, ми можемо поширювати його на сукупність усіх об'єктів цивільних правовідносин, що існують в оцифрованому виді (мережа Інтернет, трансляція телепередач тощо) [2].

Суди повинні, при розгляді справ зазначеної категорії, враховувати сукупність обставин, що викладені в п.15 постанови «Про судову практику у справах про захист гідності та честі фізичної особи, а також ділової репутації фізичної та юридичної особи» №1 від 27 лютого 2009 р.

Позивач може самостійно обрати спосіб захисту особистого немайнового права, зокрема права на повагу до гідності та честі, права на недоторканість ділової репутації. Законом, який регламентує конкретні цивільні правовідносини визначено, що особа, право якої порушено, може обрати як загальний, так і спеціальний способи захисту свого права. У зв'язку з цим суди повинні брати до уваги главу 3 Цивільного кодексу України, в якій встановлений спосіб захисту особистого немайнового права, а також інші способи відповідно до змісту цього права, способу його поширення та наслідків, що їх спричинило це порушення. До таких спеціальних способів захисту відносяться, наприклад, спростування недостовірної інформації та/або право на відповідь (стаття 277 ЦК), заборона поширення інформації, якою порушуються особисті немайнові права (стаття 278 ЦК) тощо.

Відмінності між поняттями «спростування» та «відповідь» проявляються у наступному: а) при спростуванні поширена інформація визнається недостовірною, а при реалізації права на відповідь – щодо поширеної інформації та обставин порушення особистого немайнового права без визнання її недостовірною особа має право на висвітлення власної точки зору; б) спростовує особа, яка поширила недостовірну інформацію, а відповідь дає особа, стосовно якої поширено таку інформацію.

Відповідно до ч. 2 ст. 277 ЦК, право на відповідь, а також на спростування недостовірної інформації щодо особи, яка померла, належить членам її сім'ї, близьким родичам та іншим зацікавленим особам, тобто фактично необмеженому колу осіб, що є додатковою гарантією захисту особистих немайнових прав, які належать фізичній особі довічно.

При поширенні такої недостовірної інформації стосовно малолітніх, неповнолітніх чи недієздатних осіб, їх законні представники вправі звернутися з відповідним позовом до суду.

У разі поширення недостовірної інформації, що порушує особисті немайнові права юридичної особи або її структурного підрозділу, позов вправі пред'явити орган цієї юридичної особи.

Способами захисту гідності, честі чи ділової репутації від поширення недостовірної інформації можуть бути, крім права на відповідь та спростування недостовірної інформації, також і вимоги про відшкодування збитків та моральної шкоди, заподіяної такими порушеннями як фізичній, так і юридичній особі. Зазначені вимоги розглядаються у відповідності до загальних підстав щодо відповідальності за заподіяння шкоди.

При розгляді питання про відшкодування моральної шкоди додаткової уваги заслуговує постанова Пленуму Верховного Суду України від 31 березня 1995 року N 4 «Про судову практику в справах про відшкодування моральної (немайнової) шкоди» (зі змінами, внесеними постановою від 25 травня 2001 року N 5).

Крім того, при визначенні розміру моральної шкоди судам необхідно дотримуватися засад справедливості, добросовісності та розумності. При цьому визначений розмір грошового відшкодування має бути співмірний із заподіяною шкодою і не повинен призводити до припинення діяльності засобів масової інформації чи іншого обмеження свободи їх діяльності.

Отже, можна стверджувати, що цивільним законодавством та судовою практикою напрацьовано засоби захисту прав та інтересів особи внаслідок розміщення недостовірної інформації щодо неї в мережі Інтернет. Ця особа має право на відповідь чи спростування недостовірної інформації через того ж поширювача такої інформації в мережі Інтернет, а також відшкодування моральної шкоди. Значна кількість проблем вирішується з урахуванням судової практики, однак наявні інші колізії та прогалини у цій сфері, які мають потребу бути усунутими в межах наукових досліджень цивільно-правової спрямованості.

Література:

1. Ожегов С.И. Толковый словарь : под ред. проф. Л.И. Скворцова: Мир и образование, 2014. 1376 с.
2. Кохановська О.В. Проблеми захисту честі, гідності й ділової репутації особив Цивільному кодексі України: Актуальні проблеми. 2017. 8с.

Одеський державний університет внутрішніх справ
«Кібербезпека в Україні: правові та організаційні питання»

Здійснення авторських прав в Інтернеті

Ребрик О.О.
курсант 3 курсу Факультету підготовки
фахівців для органів досудового розслідування
Одеського державного університету внутрішніх справ
Маковій В.П.,
завідувач кафедри цивільно-правових дисциплін
Одеського державного університету внутрішніх справ
к.ю.н., доцент

Інтернет-технологія дозволяє завантажувати, зберігати та поширювати щодо необмеженого кола осіб різні види інформації, в тому числі і такі об’єкти, які охороняються авторським правом. Проте, така «свобода висловлювання» може завдавати шкоди іншим правам людини, що є неприпустимим. Саме тому правила, які охороняють твори та їх авторів від протиправних посягань з боку інших осіб, є важливими.

Сутність зазначених порушень така ж, як і поза сферою мережі. Основна відмінність полягає в тому, що простота копіювання і нематеріальна сутність об'єктів авторського права в Інтернеті не дозволяють так само просто вирішити проблему доказу порушення авторських прав.

Сучасні дослідники переважно розглядають переведення об'єкта авторського права (суміжних прав) у цифрову форму як відтворення (О.М. Пастухов, В.С. Дроб'язко й Р.В. Дроб'язко). В.О. Калятін виділяє навіть окремий різновид відтворення - «цифрове відтворення», що, на відміну від «аналогового відтворення», різко збільшує можливості відтворення твору [1].

Авторське право на твір виникає внаслідок факту його створення. Для виникнення і здійснення авторського права не вимагається реєстрація твору чи будь-яке інше спеціальне його оформлення, а також виконання будь-яких інших формальностей.

Цивільне законодавство передбачає можливість у судовому порядку вимагати захисту порушеного авторського права, визнання дій такими, що порушують авторське право, стягнення компенсації та моральної шкоди за порушення авторського права тощо (ст. 16 ЦК України, ст. 52 Закону України “Про авторське право і суміжні права”). Ефективним швидким засобом припинення дій, що порушують авторське право, є застосування запобіжних заходів та заходів забезпечення позову (Розділи V-1, Х ГПК України, ст.ст. 151-154 ЦПК України). В Україні наявний значний досвід судової практики забезпечення захисту авторського права і суміжних прав, порушених у мережі Інтернет [2; 3, п. 31].Приклад із судової практики полягає в тому, що п*озивач* є власником виключних майнових авторських та виключних майнових суміжних прав на твори А1, А2, А3, А4, А5, А6, А7, А8. Вказане підтверджується наявністю рядом укладених *Позивачем* ліцензійних договорів. *Відповідачем 1* було неправомірно розповсюджено вищевказані твори шляхом розповсюдження за Інтернет адресами www.goodok.mts.com.ua і www.muzon.ua, у формі Мобільного контенту. Факт використання зазначених творів зафіксовано *Позивачем* шляхом відеозапису скачування творів із сайтів *Відповідача 1*, та шляхом замовлення мелодій внаслідок направлення СМС-повідомлень. Рішенням Господарського суду м. Києва від 30.06.15 позов задоволено частково, стягнуто з Відповідача 1 на користь Позивача 12 180 грн. компенсації за порушення виключних майнових прав інтелектуальної власності [3].

Розміщення творів у мережі Інтернет у вигляді, доступному для публічного використання, є способом подання творів до загального відома публіки таким чином, що її представники можуть здійснити доступ до творів з будь-якого місця і у будь-який час за їх власним вибором (див. пункт 9 частини 3 статті 15 Закону України «Про авторське право і суміжні права»). Тобто таке розміщення є правомірним лише з дозволу автора чи іншої особи, яка має авторське право.

Згідно зі статтею 1 Закону «Про авторське право і суміжні права» відтворенням є виготовлення одного або більше примірників твору, відеограми, фонограми в будь-якій матеріальній формі, а також їх запис для тимчасового чи постійного зберігання в електронній (у тому числі цифровій), оптичній або іншій формі, яку може зчитувати комп'ютер [4].

Якщо у зв'язку з таким розміщенням у мережі Інтернет порушуються майнові права суб'єкта авторського права, визначені статтею 15 Закону «Про авторське право і суміжні права», то це дає підстави для судового захисту авторського права (пункт «а» статті 50 Закону «Про авторське право і суміжні права») [3].

Якщо авторські права порушено в Інтернеті, автор твору може захистити їх в досудовому порядку, або подати позов до суду.

Починаючи з березня 2017 року в Україні діє спеціальний порядок припинення порушень авторського права і (або) суміжних прав з використанням мережі Інтернет (див. статтю 52-1 Закону України «Про авторське право і суміжні права»; далі по тексту — Порядок). Зазначений Порядок є досудовим і поширюється на: аудіовізуальні твори; музичні твори; комп'ютерні програми; відеограми; фонограми; передачі (програми) організацій мовлення.

При порушенні будь-якою особою авторського права і (або) суміжних прав, вчиненому з використанням мережі Інтернет, особа, права якої порушено має право звернутися до власника веб-сайту та (або) веб-сторінки, на якому (якій) розміщена або в інший спосіб використана відповідна електронна (цифрова) інформація, із заявою про припинення порушення. Заява про припинення порушення подається в порядку, передбаченому статтею 52-1 ЗУ «Про авторське право і суміжні права».

Для того, що б захист авторського права був можливим, законодавець поклав на власників веб-сайтів та веб-сторінок низку обов'язків, в тому числі, по оприлюдненню інформації про себе.

Якщо є підстави вважати, що права суб'єкта авторського права і суміжних прав порушені у мережі Інтернет – він поряд із застосуванням інших заходів захисту прав може направити до провайдера, котрий забезпечує ймовірному порушнику його прав послуги з розміщення Інтернет-сайта або окремих матеріалів (файлів), щодо яких існує підозра у порушенні авторських та суміжних прав на своєму обладнанні, спеціальне повідомлення.

На підставі Закону «Про авторське право і суміжні права» допускається унеможливлення доступу виключно до електронної (цифрової) інформації, зазначеної в заяві про припинення порушення.

Власник веб-сайту, веб-сторінки не несе відповідальності за порушення авторського права і (або) суміжних прав, вчинені з використанням мережі Інтернет, якщо він вчасно (тобто не пізніше 48 годин з моменту отримання заяви про припинення порушення) унеможливив доступ до електронної (цифрової) інформації, щодо якої подано заяву, та надав заявнику і постачальнику послуг хостингу інформацію про вжиті заходи [5].

Особа може здійснювати захист свого авторського права і (або) суміжних прав у вищенаведеному порядку, визначеному статтею 52-1 Закону України «Про авторське право і суміжні права». Проте, у разі недосягнення успіху під час позасудового вирішення спору, чи у випадку, коли наведений порядок не поширюється на ті чи інші об'єкти авторського права, особа може звернутись до суду.

Наведене надає можливість окреслити основні засоби захисту авторського права, а також сформулювати їх визначення. Окремо зважено на позитивні моменти змін до чинного законодавства у цій сфері. Результати даного дослідження можуть стати корисними для подальших наукових та практичних розробок в сфері захисту авторських прав в умовах розвитку цифрових, зокрема Інтернет-технологій та інформаційного суспільства.

Література:

1. Сопілко І. М., Пономаренко О.В. Технічні засоби захисту авторських прав в мережі Інтернет: проблематика використання. *Юридичний вісник*. 2012. №4. С. 85–88.
2. Про застосування судами норм законодавства у справах про захист авторського права і суміжних прав: постанова Пленуму Верховного Суду України від 04.06.10 р. № 5.

3. Судова практика вирішення спорів, пов'язаних із неправомірним використанням об'єктів авторського права і суміжних прав в мережі Інтернет [Електронний ресурс] Режим доступу до ресурсу: http://www.me.gov.ua/Documents/Detail?lang=uk-UA&isSpecial=True&id=9e4662a7-e339-4942-87a9-3de33288c0c6&title=SudovaPraktikaVirishenniaSporiv-PoviazanikhIzNepravomirnimVikoristanniamObktivAvtorskogoPravaISumizhnikhPravVMerezhiInternet.
4. Ващинець І.І. Цивільно-правова охорона авторських прав в умовах розвитку інформаційних технологій: автореф. дис. на здобуття наук. ступеня канд. юрид. наук: спец. 12.00.03. 21 с.
5. Ващинець І.І. Цивільне право і цивільний процес, сімейне право; міжнародне приватне право. К.: Нац. акад. наук України. Ін-т держ. і права ім. В. М. Корецького, 2006. 20 с.

СЕКЦІЯ 3
ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ В БОРОТЬБІ З КІБЕРЗЛОЧИННІСТЮ

Грохольський В. Л.
професор кафедри кібербезпеки
та інформаційного забезпечення ОДУВС
д. ю. н., професор

Аналіз та прогнозування криміногенної ситуації підрозділами кримінальної поліції України

Діяльність кримінальної поліції повинна ґрунтуватися на глибокому і всебічному аналізі й оцінці різних явищ, процесів, факторів, що відносяться до правоохоронної сфери, і на його підставі необхідно прогнозувати (передбачати) розвиток криміногенної ситуації та планувати заходи протидії. Аналіз надає можливість своєчасно виявляти проблеми, тенденції, протиріччя в організації протидії злочинності, правильно оцінювати і вести пошук шляхів і засобів їх вирішення, обґрунтовувати прийняття управлінських рішень.

Така діяльність у підрозділах кримінальної поліції повинна здійснюватися комплексно, з використанням інформації інших служб (підрозділів) поліції, інших правоохоронних і контролюючих органів, яка становить оперативний інтерес і без якої неможливо оцінити ситуацію, що склалася, здійснити об'єктивний аналіз, прогнозування і планування, об'єктивно оцінити діяльність підлеглих, сформулювати проблему, визначити цілі і завдання, прийняти рішення і проконтролювати його виконання.

Незважаючи на ґрунтовні дослідження зазначених питань, ця проблема постійно знаходить своє відображення у відомчих нормативно-правових та організаційно-розпорядчих актах і потребує постійного удосконалення, яке без наукового обґрунтування буде мало ефективним.

Інформаційно-аналітична діяльність забезпечує: а) вивчення причин і умов, що сприяють проявам злочинності, і осіб від яких слід очікувати вчинення злочинів, учасників і лідерів злочинних формувань; б) одержання й аналіз оперативної інформації про процеси і тенденції, що відбуваються в злочинному середовищі, концентрацію такої інформації в електронних масивах і використання для проведення слідчих (розшукових) і адміністративних заходів відносно таких осіб; в) організацію системи інформаційного обміну з іншими підрозділами поліції, іншими правоохоронними і контролюючими органами, здійснення заходів щодо забезпечення підрозділів кримінальної поліції обґрунтованою і достовірною інформацією з метою попередження злочинів, виявлення і притягнення до відповідальності осіб, які вчиняють злочини, знешкодження організованих злочинних формувань; г) виявлення й оцінку проблем, що виникають у практичній діяльності; д) вироблення оптимальних варіантів управлінських рішень по окремим проблемам і заходів щодо їх вирішення; е) прогнозування кінцевих результатів намічуваних заходів. Сьогодні, на жаль, у багатьох підрозділах кримінальної поліції такий вид комплексного аналізу не проводиться, а там де проводиться, то досить поверхневий.

Ґрунтуючись на результатах комплексного аналізу криміногенної ситуації, підрозділи кримінальної поліції повинні планувати свою роботу, маючи мету досягти бажаний її рівень – розкриття вчинених злочинів, збільшити виявлення та притягнення до відповідальності осіб, що вчиняють злочини, втягують у кримінальну діяльність неповнолітніх, створюють злочинні формування тощо.

А. Л. Берг обґрунтовано вважав, що вищий тип управління - це управління на основі прогнозування [1, с. 60], яке потрібно для того, щоб мати можливість на науковому рівні розробляти перспективні проблеми, а аналізи і прогнози - це наукове передбачення напрямків розвитку системи, хоча і ймовірного характеру, оскільки при їх здійсненні використовується інформація і про майбутні явища, тобто про ті, котрих поки ще немає. Але чим більш точно і повно проаналізована інформація, чим більш вірна методика застосовується при цьому, тим більша імовірність підтвердження прогнозу в майбутньому. Такий прогноз ґрунтується на даних аналізу минулого і нинішнього стану об'єкта з урахуванням закономірностей його розвитку.

Прогнозування використовується також для вироблення правильної програми дій і прийняття управлінських рішень, що забезпечують досягнення найкращих результатів при виконанні поставлених завдань. Тому воно пов'язано з плануванням. Загальним для них є, по-перше, те, що вони звернені до майбутнього, по-друге, є продуктом розумової діяльності. Але план відрізняється від прогнозу тим, що він являє собою не просте передбачення майбутнього, а і директиву для діяльності підрозділу кримінальної поліції. Йому притаманні владність, обов'язковість і конкретність заходів, що викладаються, засобів і методів роботи для досягнення поставлених цілей, а прогнозування має

можливий (імовірний) характер, воно лише рекомендує деякі заходи, тому відноситься до попередньої, науково-аналітичної стадії роботи. Проте прогнозування передбачає глибокий аналіз явищ і процесів, причин того чи іншого положення, тим самим зменшуючи невизначеність, науково обґрунтовуючи можливі зміни в діяльності підрозділів кримінальної поліції в найближчому майбутньому. Воно дозволяє передбачати зміни в обсязі роботи, а значить, планувати очікувані зміни в організаційно-штатній чисельності, його структурі, спеціалізації працівників тощо.

Обов'язковою умовою належної організації аналітичної роботи є чітко здійснюваний облік необхідних для неї відомостей, своєчасний і повний їх збір. Ефективному управлінню може служити тільки систематизована інформація, тобто логічно ув’язані відомості, що відображають негативні і позитивні сторони явищ. Інформація повинна бути точною і зрозумілою.

Аналіз і прогнозування в діяльності підрозділів кримінальної поліції є обов'язковою функцією. Однак, анкетування керівників показує, що близько 25% з них, аналіз стану криміногенної ситуації на території обслуговування проводять за різними методиками, часто поверхово, роблячи неточні висновки. Це відбувається, на наш погляд, з двох причин: 1) через невміння проводити комплексні аналізи; 2) через небажання проводити їх.

Підрозділи кримінальної поліції у своєму розпорядженні мають різні джерела інформації – гласні і негласні. В окремих випадках вони можуть, і повинні, використовувати інформацію інших підрозділів поліції, інших правоохоронних і контролюючих органів. Однак, як показують дослідження, 30 % керівників підрозділів кримінальної поліції не використовують дані інших служб поліції.

Слід відмітити, що одною з умов прийняття оптимальних управлінських рішень - їхня забезпеченість необхідною інформацією. Інакше можна прийняти хибне (невірне) рішення. До того ж, поставлені завдання будуть вирішуватися іншим шляхом, з надмірною витратою сил і засобів, більшою затратою часу і ресурсів. Дієвість побудованих на такій інформації управлінських рішень буває невисокою.

Теорія і практика боротьби зі злочинністю виробила ряд вимог, яким повинна відповідати інформація: по-перше, – відповідність інформації компетенції суб’єкта управління, його завданням і функціям; по-друге, – оптимальність (необхідність і достовірність) інформації; по-третє, – достовірність і точність інформації; по-четверте, – своєчасність надходження інформації; по-п’яте, – комплексність і систематизація [2, с. 120-121].

Начальнику кримінальної поліції, що не є кримінологічним центром, виправдано застосовувати такий метод дослідження, як вивчення оперативних і статистичних даних, що наддасть можливість:

1) за результатами аналізу надати характеристику стану, рівня, структури, динаміки криміногенної ситуації і якості діяльності підрозділів кримінальної поліції по боротьбі зі злочинністю, тобто даються відповіді на питання, що є, яке положення справ (описова функція);

2) виявляються статистичні зв'язки, залежності, співвідношення, закономірності в стані, структурі і динаміці злочинності і роботі підрозділів кримінальної поліції, правоохоронних, контролюючих і судових органів (пояснювальна функція);

3) визначаються тенденції розвитку злочинності і складається прогноз, тобто приблизне уявлення про те, що очікується, які перспективи (прогностична функція);

4) виявляються дані, що свідчать про збільшення чи зниження кількості скоєних злочинів, позитивних сторонах і недоліках у роботі підрозділів кримінальної поліції, інших підрозділів органів поліції, щоб на підставі цих даних розробити заходи по розповсюдженню позитивного досвіду, чи по усуненню недоліків, тобто підготувати дані для того, щоб вирішити, що потрібно робити, які заходи вжити (управлінська функція).

Аналіз і прогнозування криміногенної ситуації повинні завершуватися складанням підсумкового документа (довідка, огляд тощо), в якому викладаються відомості: про характер узагальнення, його цілі; період, узятий для аналізу; зміст інформації і методах її одержання; результати узагальнення, висновки і пропозиції.

Таким чином можна зробити висновок, що науково обґрунтовано і правильно налагоджена й організована аналітична діяльність у підрозділах кримінальної поліції дасть можливість здійснювати прогнозування розвитку криміногенної ситуації на території обслуговування, підвищить ефективність прийняття управлінських рішень і виконання управлінських функцій. Можна сказати, що наскільки буде якісним аналіз і прогнозування криміногенної ситуації, настільки будуть правильними й управлінські рішення щодо протидії злочинності.

Література:

1. Берг А.И., Черняк Ю.И. Информация и управление. М.: Економіка. 1966. 64 с.
2. Бандурка А. М., Давыденко Л. М. Преступность в Украине: причины и противодействие: монография. Харьков: Гос. спец. изд-во «Основа». 2003. 368 с.

Perspectives and issues of using the biometricalsystems in crimes combatting

Vladislav COJUHARI
Head of the Department of Policing on Preventing and Combating Crime
Ministry of Internal Affairs, Republic of Moldova
E-mail: vladislav.cojuhari@mai.gov.md

INTRODUCTION

Today it is witnessing the process where person's physical traits are combined with control systems and informational networks. At the same time biometrics is one of the most fascinating ways to solve a crime. As some scholars conclude, it is an automated way to establish the identity of a person on the basis of his or her physical finger print, face, hand/finger geometry, iris, retina, ear, etc.) and behavioural characteristics (signature, voice, gait, odour, etc.). Biometric as a modern technology, helps to crime prevention by associating the sample to the person's personal traits stored in a certain database, both bringing and verifying the percentage of the similarity for the identity of persons (identification).

1. THE TYPES OF BIOMETRIC IDENTIFIERS

Biometrics represents the process by which a person's unique physical and other traits are detected and recorded by an electronic device or system *(a.n., after or simultaneously stored)* for the purpose of confirming identity. The strong part of biometric authentication resides in the fact that every person can be accurately identified by his or her physical or behavioural traits.

The two main types of biometric identifiers depend on either physiological characteristics or behavioural characteristics [1]. Physiological identifiers relate to the composition of the user being authenticated and include facial recognition, fingerprints, finger geometry (the size and position of fingers), iris recognition, vein recognition, retina scanning, voice recognition and DNA matching.

Behavioural identifiers include the unique ways in which individuals act, including recognition of typing patterns, walking gait and other gestures. We mention that most of the national law enforcement agencies, through the time, collected such data, mostly manually, storing it in archives that could be accessed in certain cases. Some of these behavioural identifiers can be used to provide continuous authentication instead of a single one-off authentication check [2].

One of the biggest privacy issues of using biometrics is the fact that physical attributes like finger geometry and retina scanning are generally static and cannot be modified. This is in distinction to factors like passwords (*something you know*) and tokens (*something you have*), which can be replaced if they are breached or otherwise compromised.

At the same time biometrics represent the most perspective path to prevent and combat the crimes. Due to the possibility of the automated way in recognising the person on the basis of his or her physical finger print, face, hand/finger geometry, iris, retina, ear, etc.) and behavioural characteristics (signature, voice, gait, odour, etc.). Biometric technology contributes to crime detection by associating the traces to the persons stored in the database, ranking the identity of persons and selecting subdivision of persons from which the trace may originate [ibidem]. Accordingly, for example most of the countries have database of former offenders that can be easily checked and identified in case of recidivism.

2. THE STRUCTURE OF A BIOMETRICAL SYSTEM

Nowadays, biometric system represents the pattern recognition device that acquires physical or behavioural data from an individual, extracts a salient feature set from the data, compares this feature set against the features set stored in the database and provides the result of the comparison. Therefore, a biometric system is composed of four modules [3]:

I. **Sensor module:** component that acquires the raw biometric data of an individual by scanning and reading.

II. **Quality assessment and feature extraction module:** For further processing, the quality of the acquired raw data is first assessed. The raw data is subjected to signal enhancement algorithm to improve its quality. This data is then processed and a set of salient features extracted to represent the underlying trait. This feature set is stored in the database and is referred as template.

III. **Matching and decision-making module:** In this module, the extracted templates are then matched against the stored templates and a matching score is given. On the basis of the matching score, the identity of a person is validated or ranked.

IV. **System database module:** This module acts as storage of biometric system. During the enrolment process, the template extracted from raw biometric data is stored in the database along with some biographic information (such as name, address, etc.) of the user.

In same order of ideas, all biometrical systems can be classified into two main categories that are: (I) Identification and (II) Verification.

In the identification mode, the biometric system establishing the identity of an individual by searching the templates of all the individuals whose identification details are stored in the database. In this process, the system conducts a 1/N (*one to many*) comparisons to prove the identity of a person.

In the verification mode, the biometrics information of an individual, who claims certain identity, is compared with his own biometric template stored in the system database. This is also referred as 1/1 (*one to one*) comparison.

That is why biometrics systems are strategically important in crime prevention due to the modules and techniques of biometrics helping in analysing the evidence by overcoming the limitations of human cognitive abilities, the subjective approach, and thus increases efficiency and effectiveness of investigation. In addition, this is an instrument that could be used complementary with other forms of evidence and/or, independently when other means of collecting evidence and investigation cannot provide a certainty in criminal proceedings regarding the identity of the offender or his guilt.

3. APPLICATIONS OF THE BIOMETRICAL SYSTEMS

Today we see biometrics permeating various segments of our society. Applications include smartphone security, mobile payment, border crossing, national civil registry and access to restricted facilities.

Without a doubt, biometric technology is already creating a significant impact on our society. Biometric recognition has also become an integral part of identity management systems around the world, especially in developing countries where a large number of people lack formal identity documents to prove who they are [4], including classic means such as passports or identity cards.

There are certain person recognition applications where it is very difficult to impose constraints on how the biometric trait should be acquired. A classic example of unconstrained sensing environment is video surveillance. Persistent video surveillance is deemed to be a successful deterrent against crime and, consequently, surveillance cameras have rapidly proliferated around the world, especially in large metropolitan areas.

For example, it has been estimated that there are more than 1 million CCTV (closed circuit television) cameras in the city of London alone and around 4.9 million of them are spread across the UK [5]. Almost all the existing CCTV cameras in use are passive in nature in the sense that they merely record the video footage of the monitored location, and the archived video is analysed by human operators only after a crime has been committed and reported. Real-time video processing and recognition is seldom carried out either to predict or detect an incident or to identify the offender. The primary challenge in automated real-time video surveillance is how to detect ‘persons of interest’ in a video and then identify them using face recognition systems [6].

Biometric systems are becoming increasingly important for identifying known and suspected terrorists. The use of emerging biometric technologies as a tool to counter terrorist attacks and fight crime is on the rise and two driving forces are behind this breakthrough. The first was the realization that 7 out of the 19 hijackers in the September 11 attack were known to the authorities. These terrorists had used false identity papers to gain entry to the United States. If there was a biometric system in place, these terrorists could have been identified that they were using someone else’s identity to gain entry and could have been stopped [7].

4. CONCLUSION

Under the current conditions of global political and economic instability, chaotic migration processes, an extremely important issue is combating crime and terrorism, ensuring security by using biometrical systems for protecting people's lives and health. The two immediate recommendations can be suggested:

1. Implementing biometrics control systems and surveillance ensuring prevention of crime and prosecution of offenders, balancing between rights of victims vs interest of perpetrators.
2. Developing and connecting machine learning engine with biometrics systems in order to enhance real time identification.

Bibliography:

1. Saini M., Kapoor A.K., Biometrics in Forensic Identification: Applications and Challenges. J Forensic Med 1, 108, 2016
2. Margaret R., Biometrics, 2017, available on: https://searchsecurity.techtarget.com/definition
3. Jain A.K., Flynn P., Arun A.R., Handbook of biometrics, 2007
4. Alan Gelb, Julia Clark (2013) Identification for Development: The Biometrics Revolution.
5. Barrett D., One surveillance camera for every 11 people in Britain, says CCTV survey, The Telegraph, 2013
6. Meuwly D,, Veldhuis R., Forensic biometrics: from two communities to one discipline. In Proc. Int. Conf. of the Biometrics Special Interest Group (BIOSIG), IEEE: Darmstadt, Germany, 6–7 September, 2012
7. Thakkar D., Fighting Crime and Tackling Terrorism with the Help of Biometric Technology, 2017

Одеський державний університет внутрішніх справ
«Кібербезпека в Україні: правові та організаційні питання»

Ефективність систем інформаційної безпеки у навчальному та науковому державному закладі

Бабенко К.А.
студент магістратури 2 курсу
Одеського національного політехнічного університету

В нашій країні відбуваються колосальні зміни, які обумовлюються перетворенням постіндустріального на інформатизоване суспільство. В Україні обраний курс на всебічну та всеохоплюючу діджиталізацію. Інтенсивно здійснюється процес цифрової трансформації суспільства, а відповідно підприємств та установ усіх форм власності. Відповідно до діючої державної стратегії особливо це торкнеться державних установ та закладів, в тому числі і освітніх та наукових. З часом це призведе до повної відмови від паперового документообігу, із заміною документообігу на електронні і цифровані данні. У результаті установи отримують спрощений доступ громадян до різних реєстрів, оперативний обмін інформацією електронними мережами. Для реалізації цього курсу в країні створено окреме відомство - Міністерство цифрової трансформації. Воно вже презентувало бренд "держава в смартфоні". За словами керівництва відомства, додатки, сайти і перші сервіси стануть доступні он-лайн в найближчі місяці і їх список постійно буде розширюватися.

Ідея державної влади блага – спростити доступ простих громадян до необхідної їм інформації, виключити чи мінімізувати вплив на цей процес чиновників; перевести величезний обсяг інформації в одиниці і нулі – мову зрозумілу комп'ютеру [1]. Багато прихильників цих тенденцій, але є і противники такого поспіху. Аргументи останніх вагомі, вони криються в деталях – які гарантії забезпечення захисту систем інформаційної безпеки, конфіденційності особистих даних? Чи стоїть на порядку денному розробка сучасної Концепції комплексного захисту інформації в Україні? І ці питання є небезпідставними, оскільки сучасна організація режиму інформаційної безпеки є критично важливим стратегічним чинником розвитку будь-якої вітчизняної установи.

Виникають і інші питання, наприклад, а чи готові державні установи до грандіозних планів держави по діджиталізації. Отже, не розуміючи на якій стадії підготовленості як технічно, так і організаційно зараз знаходяться державні установи та заклади, спеціалісти не зможуть прорахувати сили і засоби, необхідні державі для забезпечення цього процесу. Більше того, на жаль, необхідність системного підходу до питань забезпечення безпеки у використанны інформаційних технологій до сьогодні не усвідомили користувачі сучасних інформаційних систем [7].

У цій частині нашого дослідження ми у загальних рисах проаналізували ефективність систем інформаційної безпеки на прикладі державного закладу - науково - дослідного інституту нашої країни. В процесі дослідження проаналізували критерії захищеності інформаційних потоків, інформаційних процесів та інформаційних ризиків закладу; надали оцінку ефективності системи захисту інформації (далі СЗІ) і свої рекомендації для усунення вразливості СЗІ в закладі.

Відповідно до чинного законодавства України і вимог окремих нормативних документів Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" та Закону України "Про захист персональних даних" обов'язковому захисту інформації підлягає: інформація, що є власністю держави, або інформація з обмеженим доступом, вимоги по захисту якої встановлені законом, в т.ч. персональні дані громадян. Комплексна система захисту інформації - взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації. [2;3].

Згідно з класифікації організаційно – правових форм господарювання термін «державної організації (установи, закладу)» визначено наступним чином. «Організації, заклади, установи – організаційні структури, які не займаються підприємницькою діяльністю. Фінансування робіт, пов'язаних з їх діяльністю, здійснюється за рахунок асигнувань, що виділяються з державного бюджету або з місцевого бюджету адміністративно – територіальних одиниць [4].

Сьогодні існують два підходи щодо оцінки поточного стану інформаційної безпеки підприємства чи закладу, а саме "дослідження знизу догори" та "дослідження згори донизу". Використання першого підходу полягає у тому, що адміністратори починають перевіряти систему захисту на усі відомі їм види атак. Підхід "сгори донизу" ґрунтується на детальному аналізі усіх відомих схем зберігання та обробки даних. Спочатку визначають інформаційні об'єкти та потоки захисту, а потім досліджують сучасний стан систем інформаційного захисту з метою визначення реалізованих методик захисту інформаційних ресурсів, а також їх стан та рівень [5].

Для оцінки поточного рівня захисту інформації досліджуваного нами об'єкта (надалі Інститут) ми визначили стан інформаційної безпеки за допомогою підходу "дослідження згори донизу". У процесі вивчення всю інформацію, яку використовує Інститут ми поділили на «інформаційні потоки» яки

«прив'язані» до конкретних видів діяльності Інституту. Такий розподіл дозволив нам визначити вагомість той чи іншої інформації в процесі виконання Інститутом своїх основних функцій и виконати аналіз захищеності інформації від небажаних впливів. Далі ми зробили класифікацію всіх інформаційних потоків, визначивши критерії захисту інформації, відповідно до їх конфіденційності, вимог до доступності та цілісності, своєчасності та цінності.

Нагадаємо, що «інформаційний потік» - це генеруюча сукупність відомостей (повідомлень, даних) незалежно від форми їх подання, циркулюючих в системі. А також між системою і зовнішнім середовищем, призначених для реалізації сигнальних і керуючих функцій [6].

Після цього ми проаналізували інформаційні процеси в декількох науково-дослідних інститутах у містах Харкова та Одеси з метою вивчення процесів створення, збору, обробки, накопичення, зберігання, пошуку, розповсюдження, споживання та захисту інформації при використанні цих процесів за допомогою природних і технічних засобів. У ході дослідження сучасного стану систем інформаційного захисту у навчальних та науково-дослідних закладах ми дійшли висновку, що сучасні методики захисту інформаційних ресурсів використовуються неефективно. «Оцінка ризиків», дала підстави визначити високий ризик загроз інформаційної безпеки навчальних та наукових закладів або інформаційної небезпеки потенційно можливої (ймовірної) втрати частини (або якості) інформаційного ресурсу. Підсумкова оцінка (за 10- бальною шкалою оцінювання) системи захисту інформації Інститутів: 3,3, що характеризує досліджені системи в якості дуже неефективних.

У ході дослідження ми виявили системні недоліки у захисті інформації наукових та начальних установ, які зводяться до наступного.

1. Як правило, на рівні наукового і навчального інституту відсутній системний підхід до захисту інформації. Це простежується, як у ігноруванні фундаментальних основ «Концепції інформаційної безпеки», так і у відсутності «Регламента інформаційної безпеки». Така ситуація відкриває можливості до витоку конфеденційної, цінної наукової інформації не лише до конкурентів, а і для осіб, які можуть завдати шкоду науковому чи навчальному закладу.

2. Найчастіше система захисту навчального та наукового закладу носить фрагментарний або хаотичний характер, не має ознак комплексності, охоплює лише окремі аспекти діяльності закладу.

3. У навчальному та науковому закладі в основному відсутня документація (інструкції, настанови), які регламентують порядок функціонування системи захисту інформації; відсутній механізм контролю за виконанням вимог СЗІ.

4. У навчальних та наукових закладах не забезпечується належним чином цілісність і конфеденційність інформації: відсутній регламент із контролю та зберіганням конфеденційної інформації; не обмежений доступ до носіїв конфеденційної інформації співробітників навчального чи наукового закладу; не регламентований порядок зберігання інформації під час її передачі та обміну; відсутній регламент, що регулює правомочність доступу і обробки співробітниками конфеденційної інформації (результати отриманих наукових результатів, персональні данні тощо).

5. При наявності великих обсягів розроблених документів у навчальних та наукових закладах не передбачений процес їх архівації та зберігання.

6. Під час прийому співробітників на роботу у контакті не формулюються індивідуальні вимоги щодо захисту інформації, яка має ознаки конфіденційності, авторську приналежність, інтелектуальну власність закладу тощо.

7. Як правило, локальна вичислительна мережа (ЛВС) реалізується простим поєднанням комп'ютерів за допомогою LAN-кабеля. Вся інформація, що обробляється або зберігається у комп'ютерах не захищена, навіть паролями доступу. Відповідна техніка протягом робочого дня знаходиться в умовах, які не виключають можливості доступу третіх осіб, що не виключає повного знищення, копіювання або несанкціоноване тиражування інформації.

Висновки. Дослідивши ефективність системи захисту інформації випадково відібраних державних наукових та навчальних закладів, ми побачили відсутність єдиного системного підходу до цього процесу.

Ми пропонуємо. Для того, щоб не допустити витоку, перекручування, тиражування або присвоєння конфіденційної інформації третіми особами в Істиутті необхідно розробити « Концепцію інформаційної безпеки» і єдиний Регламент інформаційної безпеки, в який увійдуть існуючі регламенти та інструкції, а також всі знову розроблювальні документи з інформаційної безпеки.

Перед розробкою системи технічних рішень необхідно розробити організаційну політику безпеки. Ця політика, перш за все, повинна описувати порядок надання і використання прав доступу користувачів.

Необхідно створити систему допуску співробітників до «інформаційних потоків», що включає в себе процеси ідентифікації, аутентифікації і авторизації.

На рівні держави настав час розробити єдину сучасну системну Концепцію комплексного захисту інформації в Україні для державних організацій, установ та закладів.

Література:

1. Диджитализация – процесс цифровой трансформации общества. URL: https://mentamore.com/socium/didzhitalizaciya.html. (дата звернення: 10.09.2019).
2. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від від 05.07.94. N 81/94-ВР.Відомості Верховної Ради України. 1994. N 31. Ст.287. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80 (дата звернення: 10.09.2019).
3. Про захист персональних даних: Закон України від 1 червня 2010 р. № № 2297-VI. Відомості Верховної Ради України. 2010, № 34, ст. 481. URL: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 10.09.2019).
4. Класифікація організаційно-правових форм господарювання URL: https://zakon.rada.gov.ua/rada/show/vb288217-94(дата звернення: 10.09.2019).
5. Кононова В. О., Харкянен О. В., Грибков С. В. Оцінка засобів захисту інформаційних ресурсів. Вісник Національного університету 2014. № 806. С. 99-105. URL: http://nbuv.gov.ua/UJRN/VNULPKSM_2014_806_18. (дата звернення: 10.09.2019).
6. Словарь - справочник по информационной безопасности для парламентской ассамблеи ОДКБ / под общ ред. М.Л. Вуса и М.М. Кучерявого. Санкт Петербург: СПИИРАН; Изд-во «Анатолия», «Полиграфические технологии», 2014. 96 с.
7. Защита от хакеров Web приложений / Джефф Форристал, Крис Брумс, Дрю Симонис, Брайн Бегнолл, Майкл Дайновиц, Джей Д. Дайсон, Джо Дьюлэй, Майкл Кросс, Эдгар Даниелян, Дэвид Г. Скабру ; пер. с англ. В. Зорина. Москва: Компания АйТи ; ДМК Пресс. 496 с.

Вразливості Android-смартфонів

Гавриш О.С.
старший викладач кафедри ЕтаІБ
Дніпропетровського державного
університету внутрішніх справ

Дослідники виявили можливість стежити за власниками Android-смартфонів і таємно керувати їх пристроями. Під загрозою власники як мінімум 10 моделей телефонів, включаючи Google Pixel 2, Huawei Nexus 6P і Samsung Galaxy S8 +.

Проблема полягає в системному інтерфейсі, який взаємодіє з радіомодулем пристроїв. Цей компонент забезпечує обмін даними з стільниковими вишками для дзвінків і виходу в Інтернет. Для коректної роботи радіомодулів потрібно практично необмежений рівень привілеїв, що відкриває доступ до інших апаратним елементам смартфона і додатків.

Саме цим і скористалися експерти з університетів Айови - вони взяли радіомодуль під контроль, відправляючи йому так звані AT-команди через підключаємі аксесуари. Щоб знайти потенційно небезпечні повідомлення, дослідники застосовували оригінальну утиліту ATFuzzer. Вона аналізує граматику службових команд, визначаючи можливості для маніпуляцій.

Таким чином фахівці знайшли чотири некоректні команди, які використовуються при Bluetooth з'єднанні та 13 - при з'єднанні по USB. Вони дозволяють шпигувати за користувачами або вести DoS-атаки на їх смартфони.

Набір шкідливих можливостей змінюється від пристрою до пристрою. Так, в разі Samsung Galaxy S8 + експерти змогли дізнатися IMEI, прослуховувати і перенаправляти дзвінки. Інші смартфони не сприймали такі команди, але дозволяли відключати інтернет-доступ і телефонний зв'язок.

Повну версію дослідження експерти пообіцяли представити в грудні на конференції з безпеки комп'ютерних додатків ACSAC 2019.

Для проведення атаки зловмисникові потрібно встановити віддалене підключення до цільового пристрою. Зробити це можна за допомогою Bluetooth- або USB-аксесуарів. Дослідники підкреслили, що саме по собі застосування вразливостей технічної складності не представляє.

Вони повідомили про свої знахідки виробникам, проте проблему визнали тільки в Samsung. Розробники дали назви вразливостям CVE-2019-16400 і CVE-2019-16401, пообіцявши усунути їх в майбутніх оновлення.

В Google дослідникам повідомили, що деякі описані можливості входять в специфікацію Bluetooth, а інші неможливо відтворити на актуальних версіях Pixel. Представники Huawei утрималися від коментарів.

Раніше дослідники розповіли про застарілі технології SIM-карт, які відкривають несанкціонований доступ до мобільних телефонів та IoT-пристроїв. За оцінками фахівців, атака Simjacker загрожує мільярду абонентів в 29 країнах світу [1].

Незабаром експерти виявили схожий метод атаки, побудований на іншому компоненті SIM-карт. В обох випадках маніпуляції з пристроями йдуть через службові повідомлення, які неможливо виявити через стандартний інтерфейс.

Фахівці університетів з Айови також попереджали про помилки протоколів LTE 4G і LTE 5G, які теоретично загрожують більшості стільникових абонентів. Уразливості дозволяють зламувати захищені канали зв'язку, щоб відстежувати місце розташування мобільних пристроїв і викликати в них критичні збої.

Література:

1. Исследователи научились шпионить за пользователями Android [Електронний ресурс]. Режим доступу: https://threatpost.ru/android-devices-hackable-via-at-commands/34802/

До питання протидії комп'ютерній злочинності в кібернетичному просторі

Курило В. І.
завідувач кафедри адміністративного та фінансового права
Національного університету
біоресурсів і природокористування України
д. ю.н., професор, заслужений юрист України

Ми живемо в епоху інформаційного суспільства, коли комп'ютери і телекомунікаційні системи охоплюють всі сфери життєдіяльності людини і держави. Але людство, поставивши собі на службу телекомунікації та глобальні комп'ютерні мережі, не передбачало, які можливості для зловживання створюють ці технології. Сьогодні жертвами злочинців, що орудують в віртуальному просторі, можуть стати не тільки люди, а й цілі держави. При цьому безпека тисяч користувачів може виявитися в залежності від декількох злочинців. Кількість злочинів, скоєних в кіберпросторі, зростає пропорційно числу користувачів комп'ютерних мереж, і, за оцінками Інтерполу, темпи зростання злочинності, наприклад, в глобальній мережі Інтернет, є найшвидшими на планеті [1]. За даними міжнародної служби щодо забезпечення безпеки в сфері кіберзагроз Symantec Security, кожну секунду в світі піддаються кібератаці 12 осіб, а щорічно в світі реєструється близько 556 млн кіберзлочинів, збиток від яких становить понад 100 млрд дол. США [2].

Під кіберзлочинністю розуміється сукупність злочинів, що здійснюються в кіберпросторі за допомогою комп'ютерних систем або комп'ютерних мереж, а також інших засобів доступу до кіберпростору, в рамках комп'ютерних систем або мереж, проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних [3, с. 57-58]. Згідно з рекомендаціями експертів ООН термін «кіберзлочинність» охоплює будь-який злочин, який може відбуватися за допомогою комп'ютерної системи або мережі, в рамках комп'ютерної системи або мережі, проти комп'ютерної системи або мережі. В принципі він охоплює будь-який злочин, який може бути здійснено в електронному середовищі. Інакше кажучи, до кіберзлочинів відносяться такі суспільно небезпечні діяння, які вчиняються з використанням засобів комп'ютерної техніки щодо інформації, яка обробляється і використовується в Інтернеті. Логічним наслідком даного визначення є поняття самого діяння. Кіберзлочини – це винні, досконалі, суспільно небезпечні і кримінально карані втручання в роботу комп'ютерів, комп'ютерних програм, комп'ютерних мереж, несанкціонована модифікація комп'ютерних даних, а також інші протиправні суспільно небезпечні діяння, вчинені за допомогою комп'ютерів, комп'ютерних мереж і програм. Як відомо, одним із першоджерел, що регулює правову взаємодію країн, є Хартія ООН [4]. Даний документ був прийнятий більш 50 років тому і звичайно не передбачав тоді правовий захист від кібератак. Проте багато держав намагаються застосувати цей документ для правової оцінки кібернападів. Найбільш придатними є статті 51 і 41 [4]. Так, стаття 51 говорить, що ніхто не може заборонити нації або групі націй організувати самозахист, якщо сталася збройна атака. Однак тут виникає питання: чи є кібератака збройною атакою? Навіть якщо встановлено, що атака сталася з підрозділів збройних сил. Бангкокська декларація [5], яка стала результатом діяльності XI

Конгресу ООН із запобігання злочинності та кримінального правосуддя, також свідчить про актуальність проблеми кіберзлочинності. У декларації наголошується, що в період глобалізації швидкий розвиток інформаційних технологій і нових систем телекомунікацій та комп'ютерних мереж супроводжується зловживанням цими технологіями в злочинних цілях, а також наголошується на необхідності розробки національних заходів і розвитку міжнародного співробітництва щодо протидії кіберзлочинності.

На посилення вищезазначеного, підкреслимо, що у Північноатлантичному договорі НАТО використовуються такі терміни, як «озброєна атака», «територіальна цілісність», «політична незалежність» тощо [6]. Терміни «самозахист», «допомога», «колективна допомога» використовуються тільки в контексті збройного нападу. Стаття 12 Північноатлантичного договору дозволяє державам-членам НАТО проводити спільні консультації з аналізу договору, якщо є «фактори, які загрожують миру і стабільності». Ця стаття може бути використана як механізм, за допомогою якого кібератаки, колективний захист і гео-кібербезпека можуть розглядатися країнами НАТО [7, с. 20]. Після подій, що відбулися в 2007 р. міністр оборони Естонії Яак Аавіксоо відзначав в ЗМІ, що даний договір НАТО не може пояснювати і допомагати в разі кібернападів, і жоден міністр оборони країни НАТО не буде кваліфікувати кібератаку як військовий напад на його країну. Рада Європи в 2001 р. прийняла Конвенцію про кіберзлочинність [8], яка пропонує різні способи для спільної правової роботи країн за оцінкою кібератак і заходів щодо їх відображення. Конвенція передбачає прийняття сторонами законодавчих та інших заходів, які дозволять кваліфікувати як злочин такі діяння, як протизаконний доступ до комп'ютерної системи, протизаконне перехоплення даних, вплив на дані та на функціонування комп'ютерної системи, протизаконне використання пристроїв, підроблення та шахрайство з використанням комп'ютерних технологій, правопорушення, пов'язані з дитячою порнографією, правопорушення, пов'язані з порушенням авторського права і суміжних прав, а також замах, співучасть чи підбурювання до вчинення зазначених злочинів (статті 2-11 Конвенції [8]). Дана Конвенція набула чинності 01.07.2004 р. і є єдиним зобов'язуючим міжнародним інструментом у цій галузі. В останні роки на засіданнях Організації договору колективної безпеки (ОДКБ) регулярно стали розглядатися питання, що стосуються кібербезпеки. Так в 2009 р. на території країн-членів ОДКБ була проведена широкомасштабна операція «Проксі» з протидії кіберкриміналу [9, с. 113]. Ця кампанія спрямована на виявлення і припинення в національних сегментах Інтернету інформаційних ресурсів кримінального характеру.

Як бачимо, вивчення комп'ютерної злочинності в кібернетичному просторі дозволяє зробити висновок про те, що дане явище характеризується різноманітністю об'єктів злочинного посягання. Об'єктом комп'ютерних злочинів виступає ціле коло суспільних відносин, які знаходяться під охороною держави у сфері національної, громадської, інформаційної безпеки; економіки; конституційних прав і свобод людини і громадянина; дотримання честі і гідності особи тощо. Специфічність комп'ютерних злочинів у тому, що поряд з правовідносинами у фізичному світі, вони існують і у віртуальному. Динаміка зареєстрованих комп'ютерних злочинів в Україні свідчить, що з року в рік їх число збільшується, і з упевненістю можна стверджувати, що дана тенденція буде зберігатися найближчим часом. Серйозні результати у протидії комп'ютерній злочинності можна досягти шляхом міжнародного вирішення проблем боротьби з транснаціональними комп'ютерними злочинами і їх переслідування у судовому порядку.

Література:

1. Орлов О.В., Онищенко Ю.М. Попередження кіберзлочинності – складова частина державної політики в Україні. *Теорія та практика державного управління.* Вип. 1 (44). URL: www.irbis-nbuv.gov.ua/.../cgiirbis_64.exe?
2. Managing cyber risks in an interconnected world. Key findings from The Global State of Information Security Survey 2015 [Electronic resource]: United States Department of Labor. URL: http://www.dol.gov/ebsa/pdf/erisaadvisorycouncil2015security3.pdf
3. Бойченко О.В. Міжнародне співробітництво правоохоронних органів держав в галузі забезпечення інформаційної безпеки. *Форум права.* 2009. № 2. С. 56–62.
4. Окінавська хартія глобального інформаційного суспільства. URL: http://zakon5.rada.gov.ua/laws/show/998_163.
5. Бангкокская декларация «Взаимодействие и ответные меры: стратегические союзы в области предупреждения преступности и уголовного правосудия». URL: http://www.un.org/ru/documents/decl_conv/declarations/bangkok_declaration.shtml.
6. Довідник НАТО. Office of Information and Press. NATO. 1110 Brussels. 2001. 608 с.

7. Андріянова Н.М. Аналіз практики проведення операцій НАТО з підтримання миру і безпеки. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняхівського.* 2017. Випуск № 3(61). С.19–23.
8. Конвенція про кіберзлочинність. Міжнародний документ від 23.11.2001. Конвенцію ратифіковано із застереженнями і заявами Законом № 2824-IV (2824-15) від 07.09.2005 // ВВР. 2006. № 5–6. ст.71.
9. Клевакина Е.В. Организация Договора о коллективной безопасности в контексте национальных интересов стран-участниц. *Вестник международных организаций.* 2013. № 2 (41). С.112–129.

Підвищення ситуаційної поінформованості наземних роботизованих комплексів на підтримку мережецентричної концепції ведення бойових дій

Дідик В.О., Коркін О.Ю.
ад'юнкти Військової академії
Симоненков В.М.
науковий співробітник Наукового центру Військової академії
Коновець В.І.
провідний науковий співробітник НДЦ ЗС України "Державний океанаріум"
Інституту ВМС Національного університету "Одеська морська академія
к. т. н., с.н.с.

Аналіз досвіду сучасних бойових дій у локальних збройних конфліктах та в зоні проведення операції Об'єднаних сил свідчить про необхідність удосконалення існуючих тактичних систем оперативного обміну інформацією.

Вирішення цієї проблеми частково можливе за допомогою впровадження завадозахищених автоматичних систем на полі бою, які засновані на комплексному використанні глобальних навігаційних супутникових систем, систем електронної картографії, автоматичного цифрового радіозв'язку та передачі даних.

За досвідом провідних військових фахівців світу вважається що саме мережецентрична концепція ведення бойових дій передбачає високий рівень застосування наземних роботизованих комплексів (НРК) на полі бою.

В країнах-членах НАТО розробка і створення роботизованих засобів та відповідних технологій регламентуються низкою програмних документів, у яких головна увага приділяється питанням сумісності та підвищення рівня їх автономності під час застосування.

Слід зазначити, що саме наявність достовірної навігаційної інформації визначає рівень автономності мобільного робота в просторі та обумовлює ефективність та функціональні можливості НРК в цілому. Однак, широке застосування систем супутникової навігації у військовій сфері виявило низку недоліків, передусім, використання фазомодульованих сигналів, які на той час вважалися найбільш захищеними від завад.

На сьогодні розроблені та активно застосовуються зразки придушувачів сигналів супутникових навігаційних систем, наприклад, на виставці "Зброя та безпека" у жовтні 2019 року ПАТ "Холдингова компанія "Укрспецтехніка" представила комплекс "Анклав" призначений для створення перешкод для прийомних навігаційних систем GLONASS, NAVSTAR GPS, BeiDou та Galileo в радіусі 20-40 км.

Нещодавно, представники армії США, зі складу Європейського командування в Німеччині, повідомили про експериментальне встановлення на легкі броньовані машини Stryker GPS-приймачів з антеною проти завад. Також, цьому питанню присвячене низку вітчизняних дослідницьких робіт, в яких запропоновані варіанти застосування цифрових антенних решіток (АР) для більш ефективного вирішення навігаційних завдань в умовах складної завадової обстановки. З технічної точки зору, АР – це антенна система, що являє собою множину антенних елементів із цифровими каналами, у якої використаються технології цифрового формування характеристик спрямованості.

Завдяки формуванню великих інформаційних масивів, під час цифрової обробки характеристик АР, можливе використання методів ефективного аналізу та перетворення даних шляхом використання програмних (обчислювальних) фільтрів. У ході досліджень, було проведено імітаційне моделювання завадозахищених приймачів глобальних супутникових навігаційних систем.

Така інформаційно-навігаційна система з технологією АР у складі автономних (напівавтономних) НРК здатна забезпечити високу ефективність прийому слабких супутникових навігаційних сигналів та значно підвищити ситуаційну поінформованість в складних завадових та швидкоплинних умовах бойової обстановки.

Одеський державний університет внутрішніх справ
«Кібербезпека в Україні: правові та організаційні питання»

Використання інформаційних технологій організованими злочинними формуваннями

Доценко О. С.
професор кафедри управління та роботи з персоналом
Національної академії внутрішніх справ
кандидат юридичних наук, доцент

Розвиток інформаційних технологій свідчить про високий рівень інтелектуального потенціалу суспільства, прагнення до удосконалення регулювання суспільних відносин, поліпшення використання наукових досліджень в повсякденному житті для спілкування, обміну ідеями, поглядами, творчим та інтелектуальним надбанням тощо. Водночас, цими позитивними змінами досить часто користуються злочинці, особливо організовані злочинні формування.

Джаред Коен, засновник і директор наукового центру Google Ideas зазначає, що Інтернет є невловимим і таким, що без упину змінюється, щосекунди стає все більшим і складнішим. Це джерело колосального добра і страхітливого зла. Інтернет – це найграндіозніший в історії експеримент, де корениться анархія. Ця нова здатність вільного самовияву та безперешкодного руху інформації створила багатий віртуальний ландшафт. Брак контролю призводить до Інтернет-шахрайства, залякування і переслідування, створюються сайти груп ненависті та форуми, де спілкуються терористи. І це тільки початок [1, с. 9].

Використання інформаційних технологій для вчинення злочинів сьогодні прийнято називати кіберзлочинами. В Угоді про асоціацію України з ЄС визначено, що боротьба з кіберзлочинністю є елементом безпекової політики [2], задля чого доцільно вжити низку законодавчих, організаційних, кадрових та навчальних заходів. Актуальність вказаних питань знайшла своє відображення в Стратегії національної безпеки України, відповідно до якої необхідно підвищити спроможність правоохоронних органів щодо розслідування кіберзлочинів; створити систему підготовки кадрів у сфері кібербезпеки; здійснювати міжнародне співробітництво у сфері забезпечення кібербезпеки [3].

Слід зазначити, що єдиного визначення кіберзлочинності не існує, і Конвенція Ради Європи проти кіберзлочинності не містить такої дефініції. Але, аналіз нормативно-правових актів і думок науковців дає можливість говорити, що кіберзлочини – це кримінальні правопорушення, які вчиняються з використанням комп'ютерної техніки (комп'ютерів, пристроїв та іншого обладнання), інформаційних технологій, комп'ютерних систем та мереж з порушенням встановленого порядку інформаційної безпеки, незалежно від предмету посягання та сфери застосування.

До основних ознак кіберзлочинності можна віднести: безпосереднім місцем вчинення злочину є віртуальний світ; наслідки можуть бути як віртуальні, так і реальні (матеріальні та моральні); віддаленість місця настання наслідків від місця безпосереднього вчинення злочинних дій; транскордонний характер злочинних дій; ускладнена процедура ідентифікації особи злочинця; цифровий характер слідової інформації; ліцензований або шкідливий програмний продукт як засіб вчинення злочину; багатовидовий предмет посягання (інформація, власність, мораль, безпека тощо); значні розміри завданої шкоди.

У Кримінальному кодексі України міститься ряд статей, якими передбачається кримінальна відповідальність за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Зокрема, це: несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361); створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361-1); несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361-2); несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362); порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється (ст. 363); перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (ст. 363-1) [4].

Варто зазначити, що окрім названих складів злочинів, окремі статті КК України в диспозиції також містять вказівку на спосіб вчинення злочину - з використанням комп'ютеру чи інформаційних (автоматизованих) систем: ч. 3 ст. 190 КК України – «шахрайство, вчинене у великих розмірах, або шляхом незаконних операцій з використанням електронно-обчислювальної техніки»; ст. 200 КК України «Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення», «підробка документів на переказ, платіжних карток чи інших засобів доступу до банківських рахунків, електронних грошей, а так само придбання, зберігання, перевезення, пересилання з метою збуту підроблених документів на переказ, платіжних карток або їх використання чи збут, а також неправомірний випуск або використання електронних грошей»; ч. 4 ст. 301 КК України «Ввезення, виготовлення, збут і розповсюдження порнографічних предметів» йдеться про «примушування неповнолітніх до участі у створенні … комп'ютерних програм порнографічного характеру»; ст. 376-1 «Незаконне втручання в роботу автоматизованої системи документообігу суду» [4].

Очевидно, що наведеним переліком не вичерпується кількість видів злочинів, які можуть вчинятися з використанням інформаційних технологій. Як свідчить слідча та судова практика, організовані злочинні формування використовують інформаційні технології для вчинення злочинів проти життя і здоров'я (доведення до самогубства), проти власності, проти порядку управління, національної безпеки, у сфері моральності, з метою підробки документів тощо.

Так, на Харківщині поліція викрила ОЗГ, яка підробляла документи державного зразка. До складу злочинної групи входило сім громадян, які підозрюються у причетності до понад 100 випадків підроблення документів державного зразка (свідоцтва реєстрації транспортних засобів, посвідчень водія, довіреностей, паспортів тощо) з різними засобами захисту. Під час обшуку вилучено комп'ютерну техніку, спеціальне обладнання для друку, гроші та готові підробки. Виготовлені документи збувалися на території України. Реалізацію та підбір «замовлень» на виготовлення документів зловмисники здійснювали через Інтернет. Кожен із учасників групи відповідав за свій певний напрям злочинної діяльності. За оперативною інформацію кількість таких випадків може сягати 400.

Водночас слід зазначити, що кіберзлочини мають транснаціональний характер, і місце вчинення злочину та настання наслідків не обмежуються наявними державними кордонами. Тому, виявлення кримінальних правопорушень, що вчиняються з використанням комп'ютерних технологій, викликало занепокоєння не лише окремих держав, але стало предметом стурбованості й міжнародних інституцій. Наявна загроза полягає в тому, що глибокі зміни, спричинені переходом на цифрові технології, конвергенцією і глобалізацією комп'ютерних мереж, супроводжуються використанням їх для здійснення кримінальних правопорушень.

Усе частіше об'єктами кібератак та кіберзлочинів стають інформаційні ресурси фінансових установ, підприємств транспорту та енергозабезпечення, державних органів, які гарантують безпеку, оборону, захист від надзвичайних ситуацій та ін. Новітні інформаційні технології застосовуються організованими злочинними формуваннями не лише для скоєння традиційних видів злочинів, але і для розробки скоєння принципово нових видів злочинів, притаманних суспільству з високим рівнем інформатизації. Що у свою чергу потребує удосконалення чинного законодавства України щодо боротьби з кіберзлочинністю.

Література:

1. Шмідт Е., Коен Дж. Новий цифровий світ; пер. з анг. Ганна Лелів. Львів: Літопис, 2015. 368 с.
2. Угода про асоціацію України з Європейським Союзом від 27 червня 2014р. *Офіційний вісник України*. 2014. № 75. Том 1.
3. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»: Указ Президента України від 26.05.2015 р. № 287. *Офіційний вісник Президента України*. 2015. 03 черв. (№ 13).
4. Кримінальний кодекс України. *Відомості Верховної Ради України*. 2001. № 25-26. Ст. 131 (із змінами).

Одеський державний університет внутрішніх справ
«Кібербезпека в Україні: правові та організаційні питання»

Комп'ютерні засоби для боротьби з крадіжками вантажів на залізничному транспорті України

Фоменко Андрій Євгенович
ректор Дніпропетровського державного університету внутрішніїх справ
кандидат юридичних наук, заслужений юрист України
Вишня Володимир Борисович
професор кафедри економічної та інформаційної безпеки
Дніпропетровського державного університету внутрішніїх справ
д. т. н., професор

Залізничний транспорт України сьогодні є однією з найважливіших галузей господарства, що забезпечує нормальне функціонування промислового й сільськогосподарського виробництва, безперебійну й надійну доставку вантажів. Номенклатура вантажів, що приймаються до перевезень на залізниці різноманітна, але основними вантажами, які транспортуються, є залізняк і кольоровий залізняк, метал (металовироби і брухт), кам'яне вугілля, будівельні матеріали.

Разом з тим галузь стикається з суттєвими проблемами, що обумовлені крадіжками вантажів при їх транспортуванні та на зупинках потягів [1, 2]. Треба відмітити, що сьогодні це не є проблемою однієї нашої країни. З таким же явищем зіштовхуються правоохоронні органи сусідніх країн, зокрема Росії, Молдови, Польщі, Німеччині, Нідерландів.

Вітчизняні та закордоні вчені [3, 4] вважають, що головною причиною недостатньої ефективності боротьби з крадіжками вантажів на залізницях, є відсутність доказової бази здійснення крадіжки на конкретній ділянці залізниці й часу його здійснення, оперативного контролю за вантажами, що транспортуються на шляху від постачальника до одержувача.

Шляхи вирішення сформульованої авторами проблеми боротьби з викраданням вантажів на залізниці бачаться в розробці комп'ютерної мережі технічного контролю й супроводу вантажів. У рамках викладеної концепції пропонується обладнати на вузлових, стикових і великих залізничних станціях вагоконтрольні пункти (ВКП), які б здійснювали зважування вагонів з високоліквідним вантажем, у русі, без розчеплення вагонів. По цій мережі, у напрямку руху потягу з вантажами, від одного ВКП до іншого повинна передаватися інформація натурного аркуша на потяг, а саме, порядковий номер розміщення вагона з вантажем у складі потягу, вага вагону й вантажу, станції відвантаження й призначення. Результати зважування вантажу на ВКП пересилаються на наступний вагоконтрольний пункт у напрямку руху потягу для подальшого контролю схоронності вантажу, що транспортується

У випадку розбіжності показань вагоконтрольного пристрою на ВКП й супровідної інформації на вантаж фіксується нестача вантажу у вагоні й відповідна інформація про це пересилається до підрозділу поліції й управлінню залізниці. Тобто, маємо приклад оперативного реагування на факт здійснення злочину, що дозволить по "свіжим" слідам більш ефективно його розкривати й розслідувати, приймати правильні управлінські й організаційні рішення [5]. Запропонована ідея захищена Патентом України № 8927 «Спосіб контролю схоронності вантажоперевезень на залізниці» [6] і реализована у вигляді мережі на рис.1.

Виконані авторами дослідження дозволили сформулювати вимоги до матеріально-технічного забезпечення ВКП, метрологічних параметрів вимірювальних приладів, запропонувати впровадження конкретних технічних засобів контролю вантажу, супроводжувальної та накопичувальної документації, необхідних форм контрольних документів.

Для виконання мережною функцій, покладених на неї поліцією, вторинна апаратура ВКП повинна містити: спеціалізований програмно-налагоджуємий пристрій для виміру й обробки сигналу датчиків навантаження і виділення маси вантажу, що транспортується; пристрій для ідентифікації осей вагона і відсікання локомотива (локомотивів); комп'ютер для збереження й обробки інформації про вантажі і поїзди, ведення історії процесу, формування повідомлення при виявленні невідповідності маси вантажу у вагоні (наявності викрадання); принтер для реєстрації протоколів і форм на паперовому носії; модем – для обміну повідомленнями зі станціями відправниками й одержувачами вантажів, іншими ваговимірювальними пунктами на шляху проходження потягів; автономне джерело напруги.

В рамках викладеного пропонується інформаційну підтримку електронної мережі, що зорієнтована на контроль та супроводження вантажоперевезень на залізниці з метою попередження та розкриття викрадань вантажів, виділити у вигляді завершеної структури середовища інформаційно-обчислювальної техніки і використання хмарних обчислень АІС «Оріон-Вантажі».

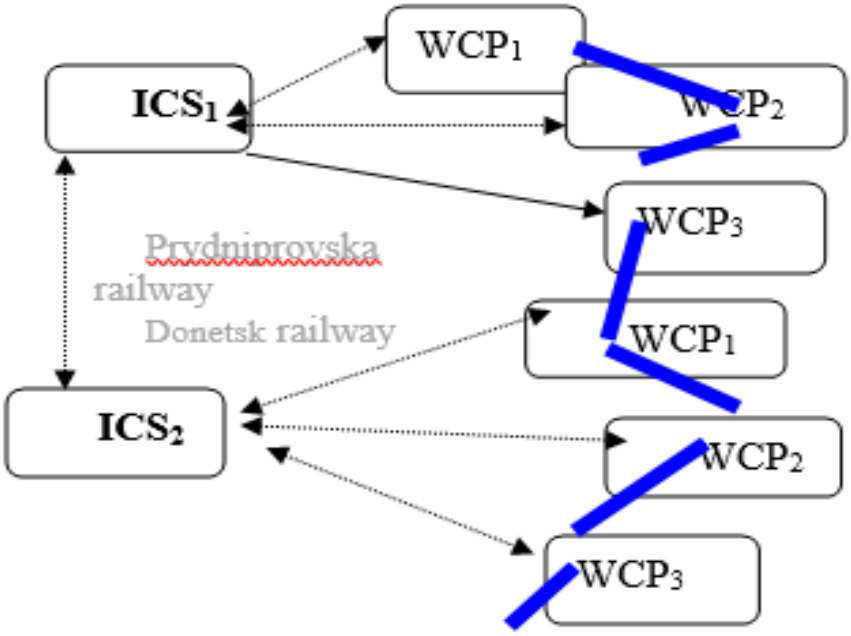


Рис. 1. Загальна схема мережі контролю та супроводженню вантажоперевезень на залізниці: де WCPi – ВКП, розміщені на стикових і вузлових станціях залізниці; ICSi – інформаційно-обчислювальні центри залізниць; сині відрізки – залізничні колії.

Нижче ми викладемо, як впровадження мережі підвищить ефективність розкриття та розслідування крадіжок вантажів.

Відомо, що характер невідкладних слідчих дій і оперативно-розшукових заходів щодо розкриття і розслідування викрадань багато в чому визначається змістом типових слідчих ситуацій, які складаються на момент одержання повідомлення про злочин. Впровадження мережі електронного супроводження вантажоперевезень дозволить оперативно виявляти факт викрадання вантажу на вагоконтрольних пунктах, через які слідує потяг. Тобто, основним видом повідомлень про крадіжку вантажу буде інформація ВКП [7].

Таким чином в якості кваліфікаційної ознаки типових слідчих ситуацій виступає ВКП, що сповістив про злочин і яких в нашому випадку може бути лише три (рис.2):

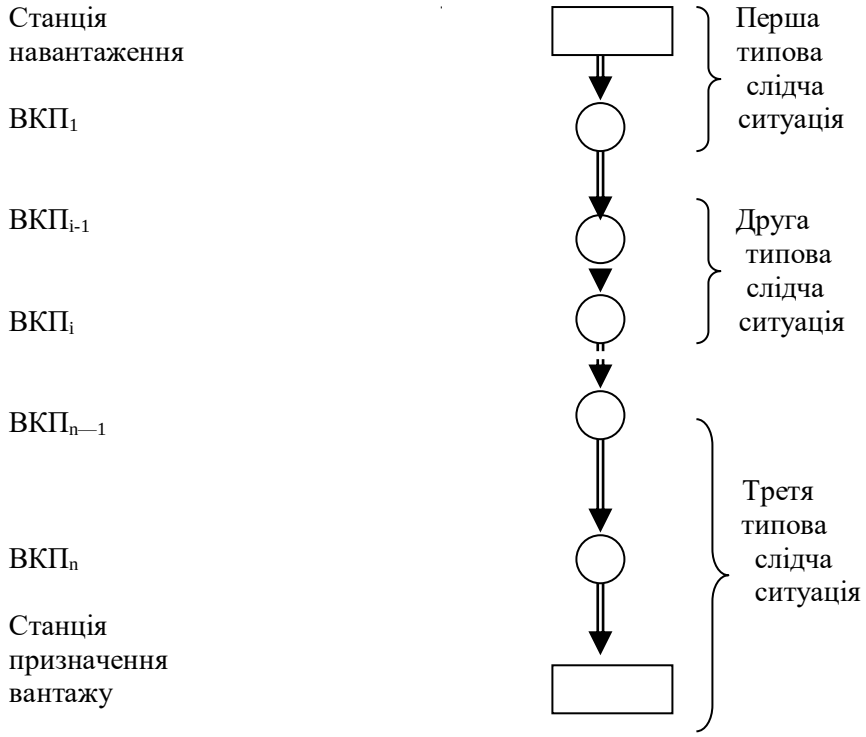


Рис.2. Класифікація типових слідчих ситуацій при впроваджені комп'ютерної мережі контролю вантажоперевезень

1) крадіжка, інформація про яку надійшла з першого ВКП (ВКП1) на шляху потягу після його відправлення зі станції навантаження або сортування вантажу;

2) крадіжка, інформація про яку надійшла з чергового ВКП (ВКПі) на шляху руху потягу;

3) крадіжка, яку виявлено під час вивантаження вантажу, але зведення ВКП, у тому числі і останнього перед станцією призначення, не вказували на факт розкрадання.

Остання слідча ситуація перекриває також випадок, коли розкрадання вантажу виявлено при перевірці вантажу на пункті комерційного огляду, але ВКП, обладнаний на станції не сповістив про це. Нагадаємо, що згідно проекту впровадження мережі ВКП, останні повинні бути створенні на усіх станціях, де здійснюється комерційний огляд вантажів

Перша типова слідча ситуація може виникати у випадках:

а) крадіжки вантажу на станції відвантаження або сортування:

• при навантажені вагону (викрадачем у змові з матеріально - відповідальною особою відправника вантажу);

• після завершення операцій з вагоном (навантаження, сортування) і очікуванні відправки потягу зі станції (любою особою, у тому числі працівником залізниці, ВОХОР та інше).

Примітка: Випадок крадіжки вантажу особисто вантажниками нами не розглядається, як не реальний, із-за присутності при навантаженні вагону матеріально-відповідальних осіб.

б) крадіжка вантажу на станції особами, що мають доступ до супровідних документів на вантажі, шляхом невірного їх оформлення або підробки (масковане розкрадання);

в) крадіжка вантажу на дільниці залізниці між станцією навантаження (сортування) вантажу і першим ВКП (ВКП1). В свою чергу таке розкрадання може бути вчинено:

• на перегоні;

• на станціях при зупинках потягу.

Друга типова слідча ситуація наступає:

а) крадіжка вантажу вчинена на дільниці залізниці між двома сусідніми ВКП (ВКПі та ВКПі-1, де і - номер ВКП, з якого отримана інформація про факт крадіжки);

б) крадіжка вантажу вчинена на більшій дільниці залізниці, наприклад між ВКПі та ВКПі-2, але з ВКПі-1 не надходила інформація про наявність викрадання. Останнє можливо у випадку:

• несправності апаратури на ВКПі-1, що не дало можливості здійснити контроль вантажу;

• наявності змови працівника ВКПі-1 та злочинців.

Як окремий випадок, друга типова ситуація при отриманні зведень про факт крадіжки вантажу з ВКП2 може трансформуватися в першу.

Третя типова слідча ситуація можлива за умови:

а) крадіжка вчинена на дільниці залізниці між станцією призначення вантажу і станцією розміщення останнього ВКП (ВКПn).

Як у першій і другій ситуаціях ця дільниця може складатися з перегонів і станцій зупинок потягу;

б) крадіжка вантажу вчинена на дільниці залізниці між ВКПn та ВКПn-1, якщо з ВКПn поступили недійсні данні за причини, наведені для другої типової ситуації;

в) крадіжка скоєна безпосередньо на станції - одержувачу вантажу:

• при вивантажені вантажу (викрадачем у змові з представником одержувача вантажу);

• під час відстою, очікуванні вивантаження вантажу (любою особою, у тому числі працівником залізниці, ВОХОР та інше).

Наявність маскованого розкрадання лише в першій типовій слідчій ситуації свідчить про те, що така крадіжка буде вже на першому, в напрямку руху потяга, ВКП, що суттєво прискорить розкриття злочину. В той же час, наявність у різних ситуаціях блоків з єдиним наповненням вказує на можливість призначення одних і тих же слідчих дій.

Треба відмітити, що існуюча та запропонована класифікації типових слідчих ситуацій не є взаємовиключними, а доповнюють друг друга. Дійсно, не виключено випадок викриття крадіжки вантажу оглядачами потягу при зупинці останнього на станції, яка знаходиться між двома ВКП (перша типова слідча ситуація попередньої класифікації).

Але, якщо ця крадіжка не була зафіксована працівником залізниці або іншою особою, то, після проходження потягу через найближчий ВКП, наступить вже друга слідча ситуація (за запропонованою класифікацією).

У другій та третій типових слідчих ситуаціях може виникати необхідність проведення додаткової технічної експертизи на наявність не санкціонованого доступу до обладнання ВКП, втручання в роботу апаратури або щодо технічної справності пристроїв зважування та передачі інформації. Це дуже важлива слідча дія, бо від її результатів залежить розширення зони пошуку слідів злочину ще на одну дільницю між ВКП.

Висновок. Наведені в доповіді результати дослідження полягають в тому, що авторами вперше сформульовані принципи побудови мережі комп'ютерної контролю та супроводженню вантажоперевезень на залізниці, що, за рахунок більш чіткого визначення місця скоєння злочину, підвищить ефективність розкриття злочину. Розроблена нова класифікація типових слідчих ситуацій, в залежності від місця отримання інформацій про нестачу вантажу (ВКП), дозволяє вірно визначати набір невідкладних слідчих дій при розслідуванні крадіжки вантажів на залізниці.

Література

1. Results of work of the bodies and units of the Ministry of Internal Affairs of Ukraine for the control of theft of goods and disassembly of rolling stock at the Pridniprovs'ka railway. [Text]. Dnipro: BWRW of the Ministry of Internal Affairs of Ukraine. (in Ukrainian).
2. Kroon L., Maroti, G., & Nielsen, L., (2014). Rescheduling of railway rolling stock with dynamic passenger flows. *Transportation Science*, 49(2), 165-184pp
3. Lomako M., Timoshenko P.Yu. Application of technical instrumentality in the activity of operational officers of internal affairs for the prevention and documentation of offenses. K.: 2004, p.17-26.
4. Forensic methodology for investigating certain types of crimes. Edited by A.P Rezvan M.: IMC GUK of the Ministry of Internal Affairs of Russia. 2002 p.225-226.
5. Vishnya V.B., Specialize in the development of the cradle of wardens in the hall of transport [Text], V.B. Vishnya., *Scientific Herald of Dnipropetrovsk State University of Internal Information:* Collection of Sciences works-2015. №2. 315-322pp
6. The way of the control of the burial-ground vantage-carrying on the hall. [Text]: *Declaration. patent* № 8927. Ukraine. IPC 7 B61L13 / 00 / O.V.Vishnya. - No. 200503376; Declared on April 11, 2005; 15.08.2005, Bul. № 8. (in Ukrainian).
7. Vishnya V.B., Typical investigative situations for the investigation of robbery abductions in the use of the network of control of freight transportation on the railways [Text], V.B.Vishnya, O.V. Zelenina, *Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs*: Coll. sciences works. 2017. No. 1 WITH. 221-226pp. (in Ukrainian).

Способи та методи попередження та протидії легалізації доходів, одержаних у сфері кіберзлочинності

Ковтун В.О.
курсант 2 курсу групи Ф4-202 факультету № 4 (кіберполіції)
Харківського національного університету внутрішніх справ
Світличний В.А.
доцент кафедри інформаційних технологій та кібербезпеки
Харківського національного університету внутрішніх справ
к.т.н., доцент

Поняття «кіберзлочинність» вперше з'явилось в американській, а потім і в іншій іноземній літературі на початку 1960-х рр. і визначалося як порушення чужих прав та інтересів по відношенню до автоматизованих систем обробки даних [1].

Згідно з Законом України «Про основні засади забезпечення кібербезпеки України» кіберзлочинність - сукупність кіберзлочинів. Кіберзлочин (комп'ютерний злочин) – 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].

Найбільш поширеними способами відмивання злочинних доходів, які використовують в своїй діяльності кіберзлочинці, є:

- перерахування коштів на карткові та корпоративні рахунки фізичних осіб з подальшим зняттям готівкою, в тому числі через банкомати тощо;
- переміщення коштів через рахунки фізичних та юридичних осіб, з подальшим придбанням товарів та послуг через Інтернет;
- переведення коштів в електронні гроші та подальше обготівковування або придбання товарів;
- обмін/розміщення коштів на електронних гаманцях [3].

Попередження кіберзлочинності базується на заходах спрямованих на зниження ризику здійснення таких злочинів та нейтралізацію шкідливих наслідків для суспільства та приватного сектору. Ефективна протидія кіберзлочинам повинна поєднувати комплекс правових (законодавчих), технічних, організаційних та інформаційних заходів [4].

Вдосконалення нормативно-правового забезпечення у сфері попередження та протидії легалізації доходів, пов'язаних із злочинами у сфері кіберзлочинності, можливе за наступними напрямами:

- внесення змін до КК України в частині посилення відповідальності за злочини у сфері комп'ютерних та інформаційних технологій;
- визнання електронних документів та інших даних у якості доказової бази при розслідуванні кіберзлочинів;
- введення сертифікації електронних платіжних засобів;
- обов'язку банків встановити антискімингові пристрої на всіх банкоматах тощо.

З метою попередження кіберзлочинів банківськими установами можуть впроваджуватись наступні технічні та організаційні заходи:

- періодичний огляд банкоматів для виявлення незаконно встановлених пристроїв;
- вимоги щодо двофакторної/двоканальної аутентифікації;
- обов'язкове інформування клієнтів про кожну проведену операцію;
- підтвердження платежу в телефонному режимі тощо.

У зв'язку з цим, значну користь у попередженні кіберзлочинності, мають інформаційно-просвітницькі заходи щодо нових ризиків та загроз в інформаційних та комп'ютерних системах [5].

Висновки: протидія кіберзлочинам поєднує комплекс правових, технічних, організаційних та інформаційних заходів, при цьому роль кожного з цих заходів не може бути визначена пріоритетною чи другорядною. При цьому ефективна протидія відмиванню злочинних доходів та зниження рівня злочинності в цій сфері можливі завдяки своєчасному виявленню фінансових операцій, що можуть бути пов'язані з відмивання доходів, одержаних у сфері кіберзлочинності, та ефективному співробітництву між державним та приватним сектором.

Література:

1. Н. Міщук Кіберзлочинність як загроза інформаційному суспільству. *Вісник Львівського університету - Серія економічна* URL: http://publications.lnu.edu.ua/bulletins/index.php/economics/article/view/5886/5899
2. «Про основні засади забезпечення кібербезпеки України» : Закон України від 05.10.2017 // БД «Законодавство України / ВР України. URL: https://zakon.rada.gov.ua/laws/show/2163-19/ed20171005#n15
3. Схеми: Легалізація коштів від кіберзлочинів // Академія фінансового моніторингу 05.04.2019 URL: https://finmonitoring.in.ua/sxemi-legalizaciya-koshtiv-vid-kiberzlochiniv/
4. Про затвердження Типологій легалізації (відмивання) доходів, одержаних злочинним шляхом, у 2013 році : Наказ від 25.12.2013 № 157. БД «Законодавство України / ВР України. URL: https://zakon.rada.gov.ua/rada/show/v0157827-13
5. Департамент фінансових розслідувань Державна служба фінансового моніторингу України Кіберзлочинність та відмивання коштів URL: http://www.sdfm.gov.ua/content/file/Site_docs/2013/20131230/tipolog2013.pdf

Рекомендації щодо основних шляхів створення належного рівня захищеності Єдиної інформаційної системи МВС України

Кудінов В.А.
професор кафедри інформаційних технологій та кібербезпеки
Національної академії внутрішніх справ
к. ф.-м. н., доцент

Станом на сьогодні минуло майже 50 років від початку процесу інформатизації в системі Міністерства внутрішніх справ (далі – МВС) України. За цей час накопичений чималий досвід використання різних інформаційних та інформаційно-телекомунікаційних систем оперативно-розшукового та інформаційно-довідкового призначення. З 2005 року в системі МВС України, на

виконання Указу Президента України від 20 жовтня 2005 року № 1497/2005, вживаються заходи щодо створення та впровадження різноманітних інтегрованих інформаційних систем [1].

Останніми роками в країні здійснюється реформа МВС України.

Відповідно до Стратегії розвитку органів системи МВС України на період до 2020 року передбачено здійснити заходи щодо об'єднання і захисту інформаційних ресурсів органів системи МВС у межах єдиного інтегрованого інформаційного середовища [2]. Тому в МВС, відповідно до Концепції інформатизації МВС України та центральних органів виконавчої влади, діяльність яких спрямовується та координується Кабінетом Міністрів України через Міністра внутрішніх справ України (далі – ЦОВВ), на 2016-2020 роки [3], Концепції програми інформатизації МВС України на 2018-2020 роки [4], вживаються заходи щодо створення Єдиної інформаційної системи (далі – ЄІС).

При цьому МВС України, відповідно до покладених на нього завдань: забезпечує належне функціонування ЄІС, формує та підтримує в актуальному стані інформаційні ресурси, що входять до неї, здійснює обробку персональних даних в межах повноважень, передбачених законом, забезпечує режим доступу до інформації, надає інформаційні послуги (п.п. 17 п. 4); організовує розроблення нових видів технічних засобів захисту інформації, засобів комп'ютерної техніки, програмного забезпечення тощо (п.п. 38 п. 4); забезпечує в межах повноважень захист інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом (п.п. 45 п. 4) [5].

Станом на сьогодні затверджено Положення про ЄІС МВС України [6].

Єдина інформаційна система МВС – це багатофункціональна інтегрована автоматизована система, що безпосередньо забезпечує реалізацію функцій її суб'єктів, інформаційну підтримку та супроводження їх діяльності і становить сукупність взаємозв'язаних функціональних підсистем, програмно-інформаційних комплексів, програмно-технічних та технічних засобів телекомунікації, які забезпечують логічне поєднання визначених інформаційних ресурсів, обробку та захист інформації, внутрішню та зовнішню інформаційну взаємодію [6].

Структура ЄІС складається з постійно діючих: центральної підсистеми; функціональних підсистем; транспортної мережі передачі даних; центрів обробки даних, телекомунікаційних мереж суб'єктів ЄІС; комплексних систем захисту інформації (далі – КСЗІ) підсистем ЄІС з підтвердженою в установленому законодавством порядку відповідністю. Останні забезпечують захист інформації шляхом здійснення комплексу технічних, криптографічних, організаційних та інших заходів і використання засобів захисту інформації, спрямованих на недопущення блокування доступу до інформації, несанкціонованого ознайомлення з нею та/або її модифікації [6].

Власником і розпорядником ЄІС є держава в особі МВС. Володільцем інформації, що обробляється в центральній підсистемі ЄІС МВС, є МВС. Володільцями інформації, що обробляється у функціональних підсистемах ЄІС МВС, є відповідні суб'єкти ЄІС МВС, тобто ЦОВВ, які забезпечують захист інформації від випадкової втрати або знищення, незаконної обробки та незаконного доступу до інформації. Адміністратором ЄІС МВС є державне підприємство зі сфери управління МВС, яке забезпечує розроблення та здійснення заходів щодо захисту ЄІС та інформації, що міститься в ній [6].

Необхідно відмітити, що на Департамент інформатизації МВС покладено завдання щодо організації роботи з проектування, створення, експлуатації та модернізації КСЗІ в інформаційних ресурсах ЄІС МВС України [7].

Як відомо, одним з важливих напрямів ефективного функціонування ЄІС МВС України є забезпечення її захищеності. Побудова КСЗІ в ній повинно дозволити запобігти або ускладнити можливість реалізації загроз порушення цілісності, доступності та конфіденційності інформації, а також належного функціонування ресурсів з її обробки, знизити потенційні збитки у разі їх здійснення, локалізацію та ліквідацію наслідків їх впливу [8; 9]. Враховуючи трьохрівневу ієрархічну модель організації функціонування ЄІС МВС України, КСЗІ повинна забезпечити на кожному їх структурному рівні функціонування інформаційних систем класу «2», а функціонування в цілому – як інформаційної системи класу «3» [10]. Тобто, побудова КСЗІ в ЄІС МВС України передбачає об'єднання в єдину систему всіх необхідних заходів та засобів захисту від різних загроз безпеці інформації на всіх етапах її життєвого циклу [8; 9; 11; 12].

З метою створення належного рівня захищеності Єдиної інформаційної системи МВС України нами, на підставі вивчення літературних джерел, зокрема [3; 4; 6; 8-12], пропонуються такі рекомендації щодо основних шляхів:

1) удосконалити нормативно-правову базу в сфері функціонування цієї системи, а саме, розробити та прийняти в установленому порядку: а) Положення про комплексну систему захисту інформаційних ресурсів МВС та ЦОВВ; б) Інструкцію про порядок авторизованого доступу користувачів до відомчих інформаційних ресурсів, а також їх використання; в) Інструкцію про порядок обміну інформацією з іншими державними органами;

2) запровадити авторизований доступ користувачів до інформаційних ресурсів виключно в межах функціональних завдань з веденням аудиту їх дій з інформаційними об'єктами ЄІС МВС та її функціональних підсистем;

3) запровадити сучасні захищені сервіси на основі хмарних технологій в центрах обробки даних МВС та ЦОВВ;

4) запровадити сучасні єдині та уніфіковані підходи до технічного, криптографічного, організаційного та інженерного захисту інформації, в тому числі до інформації з обмеженим доступом;

5) модернізувати телекомунікаційну інфраструктуру ЄІС з метою підвищення її надійності, відмовостійкості, захищеності, керованості та продуктивності;

6) забезпечити резервне копіювання та зберігання інформації, що міститься в інформаційних ресурсах Єдиної інформаційної системи МВС.

При цьому основними результатами реалізації даних рекомендацій очікується забезпечення високого рівня надійності та безвідмовності функціонування ЄІС, гарантований рівень безпеки інформаційних її ресурсів при наданні до них широкого доступу авторизованих користувачів.

Література:

1. Про першочергові завдання щодо впровадження новітніх інформаційних технологій : Указ Президента України від 20 жовт. 2005 р. № 1497/2005. URL: http://zakon3.rada.gov.ua/laws/show/1497/2005.
2. Про схвалення Стратегії розвитку органів системи Міністерства внутрішніх справ на період до 2020 року: Розпорядження Кабінету Міністрів України від 15 лист. 2017 р. № 1023-р. URL: https://zakon.rada.gov.ua/laws/show/1023-2017-%D1%80/conv.
3. Про затвердження Концепції інформатизації Міністерства внутрішніх справ України та центральних органів виконавчої влади, діяльність яких спрямовується та координується Кабінетом Міністрів України через Міністра внутрішніх справ України, на 2016-2020 роки : Наказ МВС України від 14 черв. 2016 р. № 511.
4. Концепція програми інформатизації Міністерства внутрішніх справ на 2018-2020 роки, затверджена рішенням колегії МВС від 05 лист. 2018 р. № 18км : Наказ МВС України від 11 груд. 2018 р. № 1004.
5. Про затвердження Положення про Міністерство внутрішніх справ України : Постанова Кабінету Міністрів України від 28 жовт. 2015 р. № 878. URL: http://zakon2.rada.gov.ua/laws/show/878-2015-%D0%BF/conv.
6. Про затвердження Положення про Єдину інформаційну систему Міністерства внутрішніх справ та переліку її пріоритетних інформаційних ресурсів : Постанова Кабінету Міністрів України від 14 лист. 2018 р. № 1024. URL: https://zakon.rada.gov.ua/laws/show/1024-2018-%D0%BF.
7. Про затвердження Положення про Департамент інформатизації Міністерства внутрішніх справ України : Наказ МВС України від 31 січ. 2018 р. № 70. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/MVS819.html.
8. Кудінов В.А. Організація комплексу заходів захисту апаратно-технічних засобів та програмного забезпечення системи оперативного інформування МВС України. *Сучасна спеціальна техніка*. 2011. № 4. С. 54-59.
9. Кудінов В.А. Оцінка ефективності комплексної системи захисту інформації в системі оперативного інформування МВС України. *Сучасна спеціальна техніка*. 2011. № 1. С. 91-96.
10. Кудінов В. А. Напрями подальшого розвитку методології оцінки рівнів захищеності інтегрованої інформаційно-телекомунікаційної системи оперативного інформування МВС України у зв'язку з набуттям чинності нового КПК України. *Сучасна спеціальна техніка*. 2013. № 1. С. 126-130.
11. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу : Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28 квіт. 1999 р. № 22.
12. Кудінов В.А., Хорошко В.О. Корпоративна мережа ОВС України та моделі її захисту від порушників безпеки. *Захист інформації*. 2004. № 1. С. 26-35.

Одеський державний університет внутрішніх справ
«Кібербезпека в Україні: правові та організаційні питання»

Методи оцінки безпеки комп'ютерних систем

Махницький О.В.
старший викладач кафедри ЕтаІБ
Дніпропетровського державного
університету внутрішніх справ

Тестування на проникнення (жарг. Пентест) - метод оцінки безпеки комп'ютерних систем або мереж засобами моделювання атаки зловмисника. Процес включає в себе активний аналіз системи на наявність потенційних вразливостей, які можуть спровокувати некоректну роботу цільової системи, або повна відмова в обслуговуванні. Аналіз ведеться з позиції потенційного атакуючого і може включати в себе активне використання вразливостей системи. Результатом роботи є звіт, який містить в собі всі знайдені вразливості системи безпеки, а також може містити рекомендації щодо їх усунення. Мета випробувань на проникнення - оцінити можливість його здійснення і спрогнозувати економічні втрати в результаті успішного здійснення атаки. Випробування на проникнення є частиною аудиту безпеки. Спеціаліст проводить випробування на проникнення називається пентестером. Результатом проведення випробування на проникнення як правило є звіт, який містить виявлені в ході аналізу уразливості та практичні рекомендації по їх усуненню.

У сучасному світі існує величезна кількість різних інформаційних систем. Щорічно в них знаходять тисячі нових вразливостей. Тільки тест на проникнення дає розуміння, наскільки захищена інформаційна система, яка може мати дуже важливе значення для сучасного бізнесу.

Тест на проникнення або пентест - це метод оцінки рівня кібербезпеки IT-інфраструктури, що полягає в імітації атаки зловмисників на інформаційну систему. У процесі такої контрольованої атаки відбувається виявлення потенційних вразливостей. За результатами проведення пентеста складається звіт, що містить в собі всі виявлені вразливості в системі кібербезпеки. Такий звіт також включає в себе ряд рекомендацій щодо усунення виявлених вразливостей.

Тест на проникнення дає можливість реально оцінити, наскільки успішною або, навпаки, неуспішною може бути атака хакерів на IT-інфраструктуру компанії. Завдяки цьому, можна спрогнозувати економічні втрати в разі, якщо атака буде успішною, а захист виявиться неефективною. На даний момент єдиний спосіб перевірити рівень ефективності кіберзахисту - це проведення тесту на проникнення. Альтернативного способу немає.

Пентести поділяють на два види: Black Box і White Box.

При використанні Black Box, фахівці, які проводять тест на проникнення, нічого не знають про IT-інфраструктурі, вони просто імітують атаку хакерів.

Якщо використовується White Box, фахівці, які проводять тест на проникнення, отримують від замовника всю необхідну інформації про IT-інфраструктурі.

Експерти в області кібербезпеки усього світу сперечаються про переваги і недоліки того або іншого виду, але всі сходяться на думці, що краще провести обидва види пентеста. Це надасть найбільш повний результат і максимально об'ємну інформацію про уразливість системи. Провідні фахівці нашої компанії солідарні з такою думкою.

Кращий варіант - це спочатку провести тестування Black Box, а потім White Box. Щоб знайти уразливості, експерти, які проводять пентест, повинні вивчити IT-інфраструктуру компанії, що перевіряється не гірше, а іноді і краще, ніж її розробники. Тест на проникнення рекомендується проводити як зовні, так і всередині IT-інфраструктури. Пентест також може включати в себе перевірку персоналу методом соціальної інженерії.

Може виникнути природне запитання, навіщо потрібно перевіряти персонал?

Зловмисник може бути і співробітником компанії. Просто необхідно перевірити, що може зробити співробітник усередині компанії. Чи може він зламати систему, змінити свої привілеї, отримати доступ до конфіденційної або до фінансової інформації? Пентест дасть відповіді на всі ці питання.

Важливо перевіряти співробітників на обізнаність в елементарні правила інформаційної безпеки. Це може бути зроблено за допомогою пентеста по соціальному вектору. Завдяки цьому з'ясується, наскільки співробітники компанії пильно ставляться до вкладень, посиланнях з неперевірених джерел і дзвінків від сторонніх людей.

Важливий момент! При замовленні пентеста необхідно переконатися в тому, щоб компанія використовувала світові і кращі методології, а фахівці, які будуть проводити тест на проникнення, були кваліфікованими і компетентними. Досвід і знання фахівця грають ключову роль в якості пентеста.

Пентест необхідний таким галузям бізнесу:

Банкам і фінансовим організаціям;

Телекомунікаційним компаніям;

Торгово-індустріальним компаніям;

Стартапам;

Логістичних центрів.

Загалом, пентест необхідний всім компаніям, за умови, що керівництво і власники стурбовані кібербезпекою свого бізнесу. Досвідчені і далекоглядні керівники замовляють пентест для свого бізнесу, а не чекають, коли все уразливості в системі кібербезпеки знайдуть хакери!

Види тестів на проникнення:

Тест на проникнення, заснований на технічних методах. В рамках нього ми знаходимо і експлуатуємо уразливості обладнання і ПЗ. Ми використовуємо інструменти автоматичного і ручного тестування, які детектирует IPS / IDS замовника. Тому цей вид пентеста проводиться на заздалегідь певні системи в узгоджене зі службою ІБ час.

Тест на проникнення, заснований на методах соціальної інженерії. Ми перевіряємо рівень обізнаності співробітників замовника в питаннях інформаційної безпеки. Цікавість, жадібність і бажання розважитися - кращі інструменти зловмисників, якими вони успішно користуються. Для планування атак ми користуємося інструментами The Social Engineering Framework і Social Engineer Toolkit (SET).

Социотехническими пентест. Він поєднує переваги перших двох і допомагає виявити найбільше число ймовірних напрямків атак і вразливостей.

Тести відрізняються за ступенем інформованості пентестера про засоби захисту, мережевої інфраструктури, апаратному та програмному забезпеченні замовника.

Існує методика тестування, яка базується на Draft Guideline on Network Security Testing (від NIST), Open-Source Security Testing Methodology (OSSTM) і The OWASP Testing Framework. об'єктами досліджень виступають:

Сайти та веб-додатки; СУБД; Мережеві служби і сервіси (електронна пошта, проксі, VoIP, FTP та ін.); Протоколи різних рівнів мережної моделі OSI; Мережеве обладнання; Бездротові технології.; Засоби захисту інформації; Серверні і призначені для користувача операційні системи;Прикладне ПО.

Використання інформаційних технологій в розслідуванні злочинів

Мельнікова О.О.
викладач кафедри кібербезпеки
та інформаційного забезпечення ОДУВС
кандидат юридичних наук
Дзіковська Н.Р.
курсант 4 курсу факультету підготовки
фахівців для органів досудового розслідування

В епоху глобалізації та загальної інформатизації суспільства все більш актуальним стають дослідження проблем інформаційних технологій в широкому соціогуманітарному контексті. У сфері кримінального судочинства найбільш актуальні і затребувані питання, в першу чергу пов'язані з використанням функціональних можливостей інформаційних, зокрема комп'ютерних, технологій.

В останні роки інформаційні технології дуже міцно увійшли в наше повсякденне життя. Поняття «інформаційні технології» об'єднує процеси, методи пошуку, збору, зберігання, обробки, надання, поширення інформації та способи їх здійснення. Інформаційні технології мають важливе значення для розвитку, тому що, з огляду на важливість інформації, саме рівнем розвитку таких технологій визначається потенціал подальшого прогресивного руху в усіх напрямках життя суспільства.

У зв'язку з розвитком науки і техніки, широким поширенням комп'ютерних та інформаційних технологій вчинення злочинів виходить на новий рівень. Сьогодні все більше набувають поширення злочини в сфері комп'ютерної інформації, найбільш масовими з яких є шахрайство і крадіжка грошових коштів з рахунків фізичних та юридичних осіб. Крім цих злочинів, за допомогою комп'ютерних засобів злочинці можуть здійснювати підготовку до вчинення злочинів, що призводить до тяжких наслідків і створює загрозу для життя чи здоров'я людей (наприклад злочинів проти статевої недоторканності неповнолітніх, скоєних з використанням мережі інтернет та мобільного зв'язку або суїцидальні дії неповнолітніх, з використанням соціальних мереж) тому дослідження закономірностей злочинної діяльності в даній сфері допомагає правоохоронним органам не тільки успішно розслідувати вже скоєні злочини, а й здійснювати діяльність щодо попередження таких злочинів. Злочини в інформаційній

сфері, як і злочини у фізичному середовищі, залишають після себе сліди, на які криміналістам слід звернути особливу увагу.

Характерною рисою віртуальної інформації з точки зору доведення є те, що вона може виступати в якості як сліду злочину, так і носія такого сліду, тобто слідоносія. Будучи слідом, комп'ютерна інформація, як і будь-який слід, відображає факт взаємодії матеріальних об'єктів. Однак при цьому така інформація має відмінну якість: комп'ютерна інформація легко може бути змінена або знищена, причому перераховані дії можуть проводитися дистанційно.

Автори, які вивчають питання розслідування злочинів у комп'ютерній сфері або з використанням комп'ютерної техніки, мережі Інтернет і мобільного зв'язку, вказують про необхідність вилучення матеріальних слідів, а саме: слідів рук з поверхонь клавіатури, елементів системного блоку, модему [1]. Однак слід зауважити, що доцільно такі сліди вилучати лише в тих випадках, коли злочинець користувався чужим електронним пристроєм.

Важливо відзначити, що при отриманні інформації про злочин, вчинений з використанням мережі Інтернет та мобільного зв'язку, існують певні труднощі, пов'язані з самою природою такої інформації. Так віртуальні сліди слід віднести до особливої форми слідовідображення, зафіксованих на електронних носіях. Оскільки такі сліди існують не в фізичному, а в кіберпросторі, для їх збирання, перевірки і оцінки необхідно залучення осіб, що володіють спеціальними знаннями в даній галузі. Слід також зазначити, що фіксація даних слідів повинна проводитися своєчасно і правильно, оскільки вони легко можуть бути змінені або знищені. Необхідно постійно вдосконалювати наявні методи роботи з віртуальними слідами, а також вести дослідні роботи зі створення нових методів [2].

У контексті теми роботи актуальною є проблема використання допоміжних і комунікаційних інформаційних технологій. Не тільки комп'ютерна техніка, а й мобільні телефони, смартфони, електронні книги, навігатори і багато інших пристроїв є джерелами величезної кількості інформації (а в разі розслідування злочину - кримінально-релевантної і криміналістично значимої інформації) про життя людини, його контактах, взаєминах, місцезнаходження і т.п., існуючої і використовуваної в електронній формі.

В останні роки механізму слідоутворення в електронному цифровому середовищі для різних форм подання вихідної кримінально-релевантної інформації: програмних файлів, електронних документів, акустичної, відео (статистичної і динамічної) і т.п. приділялося достатньо багато уваги.

Перспективним напрямком наукової спеціалізації, на нашу думку, сьогодні є напрям, який розглядає аспекти зіставлення нових «цифрових слідів» не тільки тим чи іншим процесам слідоутворення, а й суб'єктам, які використовують нові інформаційні технології безпосередньо в злочинних цілях або опосередковано в повсякденному житті. Цей напрямок досліджує наукову і практичну задачу непроцесуального ототожнення особистості засобами нових інформаційних технологій, коли для ототожнення залучається комплекс цифрової інформації, що породжується людиною в його повсякденній діяльності.

Стосовно інформаційних технологій в цілому і нових цифрових слідів зокрема дана проблема може бути розділена на ряд приватних питань, а саме:

1. Використання біометричної інформації для аутентифікації користувачів в технічних комп'ютерних системах і зворотна задача її декодування і використання в розслідуванні злочинів.

2. Використання техніко-криміналістичних особливостей систем автоматизації підготовки документів з метою непроцесуального ототожнення особистості.

3. Використання даних територіально орієнтованих систем відеоспостереження та мобільного зв'язку для непроцесуального ототожнення особистості.

4. Використання даних мережевих електронних ресурсів (соціальних мереж, електронної пошти, форумів і т.п.) для непроцесуального ототожнення особистості

Звісно ж, що перерахованими групами проблем, поставлена актуальна для сучасного цифрового інформаційного суспільства завдання непроцесуального ототожнення особистості не обмежується, і перелік їх вимагає подальшого обговорення і уточнення.

Література:

1. Бідняк Г.С. Теорія і практика використання спеціальних знань при розслідуванні шахрайств: монограф. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2019. 152 с.

2. Особливості розслідування злочинів, пов’язаних із незаконним обігом наркотичних засобів чи психотропних речовин із використанням сучасних телекомунікаційних та інших технологій: науково-методичні рекомендації / О.О. Юхно, Т.П. Матюшкова, В.А. Коршенко, Ю.В. Гнусов, В.В. Носов, Лисенко А.М., Мітрухов П.М., Фоміна Т.Г. За заг. ред. доктора юридичних наук, професора О.О. Юхна. [Серія «Бібліотечка слідчого і детектива: проблеми кримінального процесу»]. Х.: 2019. 48 с.

Роль спеціаліста у технічному забезпеченні проведення слідчих (розшукових) дій

Павлова Н.В.
доцент кафедри криміналістики, судової медицини та психіатрії
Дніпропетровського державного університету внутрішніх справ
к. ю. н., доцент

Під час проведення слідчих (розшукових) дій в нагоді може стати технічна допомога слідчому з боку фахівців, які, використовуючи сучасні технічні можливості фіксації доказової інформації, розвантажать слідчого і спрямують його зусилля на тактичну складову.

Так, за умов належного застосування фото- відео- фіксації цифровою технікою, під час проведення обшуку, огляду, слідчого експерименту тощо, досягається максимальна фіксація ходу та результатів слідчої дії, з максимальною зосередженістю слідчого на тактичній складовій. Після чого спільно зі слідчим можна переглянути записи при низькому темпі перегляду, звертаючи увагу на важливі моменти.

До того ж, згідно із ч. 2 ст. 104 КПК України, якщо допит фіксується за допомогою технічних засобів, текст показань може не вноситися до відповідного протоколу за умови, що жоден з учасників процесуальної дії не наполягає на цьому. У такому разі у протоколі зазначається, що показання зафіксовані на носії інформації, який додається до нього. В таких випадках особливо доцільно залучати спеціаліста для застосування ним науково-технічних засобів, а саме звуко- та відеозапису, оскільки слідчий насамперед має підтримувати психологічний контакт з допитуваною особою. А фіксувати технічними засобами проведення допиту має запрошений спеціаліст [1, с. 190].

Обов'язковим, на нашу думку, є запрошення спеціаліста й у випадку проведення допиту та пред'явлення для впізнання у режимі відеоконференції. Проведення вказаних слідчих дій у такому форматі доцільно для забезпечення оперативності досудового розслідування у випадках, коли через поважні причини учасник процесу не має можливості прибути за місцем провадження досудового розслідування. Роль спеціаліста полягає у технічному забезпеченні проведення слідчих дій у режимі відеоконференції. Так, У п. 3 статті 232 КПК України мова йдеться, що використання у дистанційному досудовому розслідуванні технічних засобів і технологій повинно забезпечувати належну якість зображення і звуку, а також інформаційну безпеку [2].

Про обов'язковість належної якості зображення та звуку вказано і в інструкції «Про порядок роботи з технічними засобами відеозапису ходу і результатів процесуальних дій, проведених у режимі відеоконференції під час судового засідання (кримінального провадження)», затвердженої наказом Державної судової адміністрації України від 15 листопада 2012 року № 155. До того ж, згідно п. 3.2.3. цього нормативного документа, учасникам судового процесу (кримінального провадження) має бути забезпечена можливість чути та бачити хід судового засідання (судового провадження), ставити запитання і отримувати відповіді, реалізовувати інші надані їм процесуальні права та виконувати процесуальні обов'язки, передбачені процесуальним законодавством. Для якісної організації запису всі учасники судового засідання (судового провадження) повинні висловлюватися голосно і виразно [3].

У цьому розрізі, С.О. Книженко підкреслює, що проведення конференції забезпечується за допомогою комп'ютерної техніки, комп'ютерних технологій та мережі Інтернет. Наприклад, сучасний нетбук з вбудованою вебкамерою та можливістю відеозапису може бути використаний для проведення вказаних слідчих (розшукових) дій тільки за умови сучасного технічного оснащення. У зв'язку з цим, виникає та потребує розв'язання питання щодо якості обладнання, яке використовується для аудіо- чи відеозапису ходу слідчих (розшукових) дій. При проведенні дистанційного досудового розслідування слідчому доцільно використовувати техніку високого класу, оскільки це дозволить забезпечити належну якість аудіо- чи відеозапису, відсутність різного роду шумів, спотворень звуку та зображення. Комп'ютер має бути обладнаний вебкамерою (вмонтованою чи окремою), яка дозволятиме приймати/передавати зображення та звук високої якості. Постає питання, якою має бути швидкість з'єднання з Інтернетом, щоб забезпечити належну якість зображення і звуку, мінімізувати час, необхідний для проведення слідчої дії в режимі відеоконференції, підвищити їх ефективність, а також який вид програмного забезпечення можна використовувати. Як вважає вчений, такі програми можуть створюватися спеціально для проведення дистанційного досудового (судового) розслідування, або можна використати звичний для всіх Skype [4]. З огляду на це, саме спеціаліст в змозі забезпечити технічні можливості проведення допиту у зазначеному форматі.

Особливо важливою є участь спеціаліста, якщо вилучається інформація, що міститься в комп'ютерах, мобільних телефонах, інших електронних пристроях. Нерідко комп'ютерна техніка, мобільні телефони захищені паролем, який ускладнює доступ до інформації від сторонніх осіб. В

даному випадку до огляду зазначеної техніки необхідно залучати фахівця, який зможе надати допомогу щодо увімкнення зазначеної техніки. Спеціаліст у галузі комп'ютерних технологій може надати консультацію з приводу побудови комп'ютерної програми, її роботи, місцезнаходження інформації, яка цікавить слідчого, способах її вилучення із пам'яті комп'ютера, проведення певних операцій за допомогою комп'ютера. Технічна допомога спеціаліста стане в нагоді й під час огляду веб-сторінок та веб-сайтів, акаунтів користувачів у соціальних мережах з подальшим зберіганням та роздруківкою скриншоту із криміналістично значимою інформацією. Огляд веб-сторінки, на якій розміщено сайт певної компанії, з проведенням подальшого експертного дослідження у сфері телекомунікації, надає змогу вивчити зміст інформації стосовно діяльності певних суб'єктів, які мають відношення до події кримінального правопорушення, а також зафіксувати IP-адресу комп'ютерного обладнання, з якого здійснювалось управління веб-сайтом та визначити Інтернет-провайдера, який надавав доступ до веб-сайту.

Література:

1. Яремчук В.О. Роль спеціаліста в проведенні допиту: URL: http://plaw.nlu.edy.ua (дата звернення 26 лютого 2019).
2. Кримінальний процесуальний Кодекс України від 13 квітня 2012 року № 4651-VI. URL: http://zakon3.rada.gov.ua (дата звернення 25 лютого 2019).
3. Про затвердження Інструкції про порядок роботи з технічними засобами відеозапису ходу і результатів процесуальних дій, проведених у режимі відеоконференції, під час судового засідання (кримінального провадження): Наказ державної судової адміністрації України від 15 листопада 2012 року N 155: URL: http://ligazakon.ua/ (дата звернення 12 лютого 2019).
4. Книженко С.О. Особливості допиту в режимі відео конференції під час досудового розслідування. *Вісник ХНУ імені В. Н. Каразіна*. № 1062., серія «Право». вип. № 14, 2013 р.

Особливості діяльності правоохоронних органів України в рамках сучасних інформаційних технологій

Первій В. Ю.
ад'юнкт Дніпропетровського державного
університету внутрішніх справ
Мирошниченко В. О.
канд. техн. наук, доцент, професор
Дніпропетровського державного
університету внутрішніх справ

Однією з провідних функцій держави є забезпечення охорони прав та законних інтересів громадян, фізичних та юридичних осіб від протиправних посягань, забезпечення принципу законності, а також охорони встановленого в державі правопорядку. Кожне з цих завдань якраз і виконується за допомогою правоохоронної діяльності, що реалізується відповідними органами держави. На сьогодні усі етапи розвитку соціуму неминуче призводять до модернізації правоохоронної сфери, а розвиток технологій вимагає від органів внутрішніх справ по-новому підходити до виконання повсякденних обов'язків, регулярно оновлювати методологію створення умов для безпечного існування людей [1].

Досліджуючи правоохоронну діяльність в Україні, зокрема, діяльність підрозділів Національної поліції України, важко уявити їх роботу без інформаційної підтримки та інформаційного забезпечення, накопичення та систематизації інформації в базах даних. І тому, для повного розуміння теми дамо визначення термінам – «Інформаційне забезпечення органів поліції» та «Сучасні інформаційні технології». Інформаційне забезпечення органів поліції – це комплекс методів, заходів, засобів різного характеру, які забезпечують створення та функціонування інформаційних технологій (ІТ), а також їх ефективне використання для вирішення покладених на поліцію завдань. Інформаційні підсистеми як складові системи інформаційного забезпечення призначені для збирання, накопичення, зберігання та обробки інформації з певних напрямів обліків і орієнтовані на використання в діяльності більшості правоохоронних структур, мають загальний характер і належать до загальновідомчих. 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. Давши визначення цим термінам ми чітко бачимо, що сучасні інформаційні технології – це матеріал для інформаційного забезпечення органів поліції, тобто сучасні

ІТ полегшують роботу поліції у сферах боротьби зі злочинною діяльністю. Зокрема, як сучасна особливість діяльності правоохоронних органів – це боротьба з кіберзлочинністю [2].

Діяльність правоохоронних органів у протидії кіберзлочинності є наразі актуальною, оскільки в наш час суспільство користується інтернетом, комп'ютерними технологіями та мобільними засобами, і ці елементи сучасного світу прямо впливають на людей у позитивному та негативному аспекті. Позитивом є те, що за допомогою комп'ютерів або телефонів мережа Інтернет є доступною всім. У Законі України "Про телекомунікації" дано визначення поняттю Інтернет – це всесвітня інформаційна система загального доступу, яка логічно зв'язана глобальним адресним простором та базується на Інтернет-протоколі, визначеному міжнародними стандартами. Тобто, це великий потік інформації та швидкий пошук відповідей на численні запитання. З негативної точки зору це нова хвороба, яка виникла не так давно і дістала назву комп'ютерна залежність, наприклад: від різноманітних ігор та соціальних мереж, але у цьому віртуальному світі існують і віртуальні злочини. І тому у цій сфері як вірус розвивається та поширюється кіберзлочинність. За допомогою вище наведених засобів скоюються такі злочини, як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему, незаконне використання пристроїв та комп'ютерних паролів, кодів доступу або інших подібних даних. Зокрема, ці злочини характеризуються найвищим ступенем латентності, при цьому збиток, що наноситься ними, часом є досить значним. Однак наразі, на жаль, розслідування таких злочинів є важкою роботою, оскільки, це реальна можливість анонімності злочинця, а також можливість залишитися на відстані багатьох тисяч кілометрів від своєї жертви. І тому можна встановити те, що в епоху інформаційних технологій неможливо почуватися захищеним у кіберпросторі, а також з розвитком технологій стрімко зростає кількість злочинів у цій сфері, а тому з впевненістю можна стверджувати, що саме «кіберзлочини» у XXI столітті будуть одними з найчисельніших.

У протидію цим злочинам в Україні існує і працює Кіберполіція України. Департамент кіберполіції Національної поліції України є міжрегіональним територіальним органом Національної поліції України, який входить до структури кримінальної поліції Національної поліції та відповідно до законодавства України забезпечує реалізацію державної політики у сфері боротьби з кіберзлочинністю, організовує та здійснює відповідно до законодавства оперативно-розшукову діяльність. Проаналізувавши нормативну базу, що стосується діяльності цього підрозділу, можна констатувати, що до завдань кіберполіції входить реалізація державної політики у сфері протидії кіберзлочинності, завчасне інформування населення про появу нових схем кіберзлочинців, впровадження програмних засобів для систематизації кіберінцидентів та реагування на запити закордонний партнерів, які будуть надходити по каналах Національної цілодобової мережі контактних пунктів. А також відслідковувати тенденції розвитку інформаційних технологій, які існують у правоохоронній сфері, удосконалення форм та методів управління системами інформаційного забезпечення, централізація та інтеграція комп'ютерних даних, впровадження новітніх комп'ютерних інформаційних технологій для ведення кримінологічних та криміналістичних обліків, розбудова та широке використання ефективних та потужних комп'ютерних мереж, застосування спеціалізованих засобів захисту інформації, налагодження ефективного взаємообміну кримінологічною інформацією на міждержавному рівні. Все це забезпечує суттєве підвищення рівня боротьби зі злочинами такого рівня [3].

Отже, підсумовуючи, можна сказати, що у наш час правоохоронні органи зіткнулися з новою сферою злочинності – кіберзлочинністю. Оскільки кіберпростір – це середовище, яке надає можливості для здійснення комунікацій та реалізації суспільних відносин, утворене в результаті функціонування сумісних комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет або інших глобальних мереж передачі даних. І тому сьогодні неможливо уявити сучасний світ без комп'ютерів, засобів комунікації та новітніх технологій. Ці засоби все частіше використовуються у злочинній діяльності. Інформаційні технології в діяльності підрозділів Національної поліції України дозволяють удосконалити механізми управління, забезпечують належне функціонування правоохоронних органів, а саме, оперативно отримувати доступ до певних відомостей, необхідних для виконання їх службових завдань, кваліфіковано здійснювати їх аналіз, використовувати досягнення науково-технічної думки для оптимізації слідчих дій. Розвиток комп'ютерних технологій дає змогу для створення нових методів роботи, підвищення професіоналізму кожного працівника. Саме тому, інновації – це запорука розвитку правоохоронної системи, інструмент, який стає реальною зброєю у боротьбі зі злочинністю.

Література:

1. Закон України «Про Національну поліцію»: станом на 12.02.2019 р. Київ: Правова Єдність. 2019.
2. Інформаційні технології в правоохоронній діяльності Посібник / В.А Кудінов., В.М.Смаглюк, Ю.І. Ігнатушко, Іщенко В.А. К.: НАВСУ, 2018. 82с.
3. Офіційний сайт Кіберполіції URL: https://cyberpolice.gov.ua/contacts/. (дата звернення: 09.11.2019 р.)

Інформаційні системи протидії функціональній нестабільності програмного забезпечення

Петрівський В.Я.
аспірант
Київський національний університет ім. Тараса Шевченка,
Шевченко В.Л.
Український науковий центр розвитку інформаційних технологій
Міністерства освіти і науки України
д.т.н., професор
Шевченко А.В.
інженер-програміст
Український науковий центр розвитку інформаційних технологій
Міністерства освіти і науки України

На сучасному етапі розвитку інформаційних систем та технологій в цілому збільшується значного поширення набуває кіберзлочинність. Цілями атак виступають як приватні особи чи підприємства так і державні структури. Метою даних злочинів є вилучення, пошкодження, зміна даних. Одним із інструментів є спеціалізоване програмне забезпечення. Тому необхідно забезпечити стійкість програмного забезпечення відносно атак під час проектування інформаційних систем. Також має місце випадки ненавмисного порушення захисту інформації. Під час аналізу спільних позицій даних порушень доцільно використовувати концепцію функціональної стійкості. Відповідно до [1, с. 160], "функціональна стійкість" – здатність системи виконувати свої функції під час заданого проміжку часу, за умови впливу потоку експлуатаційних збоїв, навмисних пошкоджень, втручанні у обмін та оброку інформації, помилок обслуговуючого персоналу. Функціональна нестабільність – нездатність системи задовольнити вищесказані умови функціональної стійкості. Нефункціональний стан – це стан, у якому система набула функціональної нестабільності. Виходячи з визначення функціональної стабільності, причини дисфункцій можуть бути як зовнішніми так і внутрішні, навмисні та ненавмисні.

Відповідно до закону Меткалфа, чим більше пов'язані між собою вузли мережі, тим більше її перевага та функціональність. Але з іншого боку, чим більше з'єднань, тим більший ризик функціональної нестабільності через кібератаки чи помилки. Тому випадки порушення інформаційної безпеки збільшуються принаймні вдвічі швидше, ніж темпи зростання інформаційних технологій [2-4, с. 6-7]. Основними причинами інцидентів є [5] зловмисне програмне забезпечення – 53%, цільові атаки – 36%, помилки та непередбачувані дії персоналу – 29%, погрози з боку третьої сторони (постачальники, партнери) – 26%, помилки в промисловому програмному забезпеченні – 21%, саботаж або навмисна фізична шкода ззовні – 17%, диверсія або навмисне фізичне пошкодження – 13%, збій програмного забезпечення – 9%. Цілі інформаційних атак [4] є не лише ліквідація інформаційних систем, але також економічні втрати, удари по іміджу, підрив довіри, просування необхідного інформаційного змісту. Небезпека з внутрішніх та ненавмисних причин велика, тому що інформаційна система для них повністю відкрита. До 40% злому банківської інформаційної системи було пов’язано з дії інсайдерів [2, 3]. Більше 300 мобільних програми, що поширюються через офіційні магазини, містять шкідливі код [5]. 71% нападів залишаються невиявленими [3]. Це зумовлює розробку інструментів протидії дисфункціональні стани відповідних інформаційних систем.

Конкретні технічні пристрої для моніторингу дисфункціональних станів у інформаційній системі розглядається в [6, с. 293]. Недоліками аналізованих рішень є часткові та неоднакові результати. Засоби захисту потребують значних витрати. Тому загальна стратегія оптимального фінансування системи безпеки необхідна на етапі проектування інформаційної системи. Критерій оптимальності – це мінімальний загальний збиток від інцидентів та додаткових витрат на захист. У літературних джерелах діапазон витрат на захист інформації визначають в межах 10-20%, що є занадто невизначеним діапазоном [2-4, с. 5-7]. В інших джерелах специфікація існуючих діапазонів проводиться триточковим методом (мінімальний, номінальний, до нього додається максимум), а розв'язки задаються за допомогою усереднення методом рівномірного розподілу або бетадистрибуції [7, с. 170, 317]. Підвищення рівня безпеки мережевих інформаційних систем від дисфункціональних станів на етапі проектування шляхом оптимізації витрат на захист за критерієм мінімізації загальних втрат описано у роботі [8, с. 37-39].

Література:

1. Mashkov O.A. Estimation of functional stability of distributed information-control systems / Mashkov O.A., Barabash O.V. // Physical-mathematical modeling and information technologies. - 2005, vp.1, p.157-163.

2. PwC presents the results of a global study on information security issues, the prospects for 2015. // Official Pricewaterhouse Coopers Website [Online]. Available: http://www.pwc.ru/en/press-releases/2015/cyber-security-press-release.html.
3. The Global State of Information Security® Survey 2016. Turnaround and transformation in cybersecurity // Official Pricewaterhouse Coopers Website [Online]. Available: https://www.pwc.com/gx/en/ issues/cyber-security/information-security-survey.html.
4. Shevchenko V.L. Best Global Practices in Information Security Management and Their Impact on the Economic Stability of the State // Modern Information Protection. - №4. - Kyiv: SUT, 2015. - pp. 4-9.
5. Cybercrime in the world. The state of cybercrime in various regions of the world // Tadviser site - Access mode [Online]. Available: http://www.tadviser.ru/index.php.
6. Shevchenko A. Dynamic Objects Emergency State Monitoring by Means of Smartphone Dynamic Data / Shevchenko A., Bychkov O., Shevchenko V. // 2017 14-th International Conference The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM). Proceeding. - Polyana, February 21-25, 2017. - p.292-294. http://ieeexplore.ieee.org/document/7937138/ DOI: 10.1109/CADSM.2017.7916138.
A Guide to the Project Management Body Of Knowledge (PMBOK GUIDE). Sixth edition. ISBN: 978-1-62825-184-5. - Project Management Institute Inc.: Pennsylvania, USA - 2017.– 756 p.
Victor Shevchenko, Alina Shevchenko, Ruslan Fedorenko, Yurii Shmorhun, Asadi Hrebennikov Designing of Functionally Stable Information Systems Optimal for a Minimum of Losses CADSM 2019, 15th International Conference on the Experience of Designing and Application of CAD Systems (CADSM), February 26 – March 2, 2019, Polyana-Svalyava (Zakarpattya), UKRAINE Lviv Polytechnic National University, UKRAINE Lodz University of Technology, POLAND IEEE Ukraine Section, IEEE Ukraine Section (West), MTT/ED/AP/EP/SSC Societies Joint Chapter Part Number: CFP19508-USB ISBN: 978-1-7281-0053-1 pp.36-40. очикується Scopus, IEEE.

Сучасна система запобігання корупції в Україні та її вдосконалення

Полінкевич О.В.
Університет державної фіскальної служби України (м.Ірпінь)
факультет Навчально-науковий інститут права
Супрун-Ковальчук Т.М.
доцент кафедри кримінального права та кримінології
Університету державної фіскальної служби України (м.Ірпінь)
к.ю.н.

На сьогоднішній час корупція є поширеним явищем, буквально в кожній країні світу, але проявляється вона в різних масштабах своєї дії. В одній країні корупція є дуже розвиненою, а в іншій - є малорозвиненою і проявляється в незначних чи поодиноких випадках. Інакше кажучи, явище корупції є дуже проблемним і загострюючим у сучасному світі, тому, що якими тільки методами не боролися проти корупції, а викорінити її зовсім не вдалося ще жодній країні світу. Саме тому, сьогодні розробляються різні системи та програми запобігання корупції в різних країнах світу, де не виключенням є і Україна. Адже в Україні корупція розвинена практично в усіх сферах суспільства, внаслідок чого є створена система запобігання корупції в Україні.

На думку, Д.Г. Заброда, під державною антикорупційною політикою (державною системою запобігання корупції), розуміється передбачений законами та підзаконними нормативно-правовими актами комплекс правових, економічних, освітніх, виховних, організаційних та інших заходів, що формуються і реалізуються органами державної влади, місцевого самоврядування та громадськістю з метою виявлення, припинення фактів корупції, усунення детермінантів, що її опосередковують, відновлення порушених прав і законних інтересів фізичних, юридичних осіб та держави [3, с. 103].

Сучасний стан системи запобігання корупції в Україні є такою, що реалізується через цілеспрямовану антикорупційну політику держави. Для боротьби з корупцією в Україні створено низку спеціальних органів, серед яких є Вищий антикорупційний суд України, Національне антикорупційне бюро України, Національне агенство з питань запобігання корупції, Національна рада з питань антикорупційної політики та Спеціалізована антикорупційна прокуратура та інші органи. Також діяльність держави у сфері запобігання корупції врегульовано у багатьох нормативно-правових актах, зокрема у базовому законі з даного питання – Законі України «Про запобігання корупції».

Крім того, із прийняттям низки антикорупційних законів у жовтні 2014 року в Україні здійснено найбільш масштабне та системне реформування антикорупційного законодавства. Зміни законодавчого поля стосувалися врегулювання ключових секторів антикорупційної діяльності в державі:

1) формування та моніторинг державної антикорупційної політики;

2) превентивна антикорупційна діяльність; 3) переслідування за корупцію [1, с. 41-42].

Крім того, 28 квітня 2018 року Уряд України схвалив проект «Державної програми щодо реалізації засад державної антикорупційної політки в Україні (Антикорупційної стратегії) на 2018-2020 роки».

Таким чином, О.В. Скочиляс-Павлів вважає, що протягом останніх років представники державної влади почали робити активні кроки на шляху запобігання корупції в Україні. На сучасному етапі реалізація системи запобігання корупції в Україні має низку завдань, які нададуть можливість державним антикорупційним органам діяти у сфері запобігання корупції комплексно, системно та послідовно. Серед таких завдань виокремлює: 1) проведення аналізу та оцінки раніше здійснюваних антикорупційних заходів, визначення їх результативності та впливу на рівень корупції; 2) окреслення пріоритетних напрямків протидії корупції; 3) визначення заходів та ресурсів для досягнення пріоритетів, а також відповідальних структур і термінів їх виконання; 4) встановлення системи відслідковування реалізації антикорупційних заходів; 5) створення механізмів координації антикорупційних зусиль державних органів та інститутів; 6) вироблення критеріїв оцінки стану корупції в країні та їх вдосконалення на основі міжнародних критеріїв [5, с. 32].

Проте слід зазначити, що існує багато проблемних питань у сучасній системі запобігання корупції в Україні, оскільки не повністю вдається досягнути багатьох цілей і мети, що закріплені у нормативно-правових актах з даного питання. Таким чином потребує удосконалення система запобігання корупції в Україні.

Зокрема, І.Є. Мезенцева пропонує застосовувати такий підхід до вдосконалення запобігання корупції в Україні, який випливає з розроблюваної в Інституті держави і права ім. В.М.Корецького доктрини протидії злочинності, що виражається формулою: «соціальна культура громадян плюс кримінальна юстиція». Науковець пояснює, що так звана культурницька доктрина полягає ось у чому: якщо в Україні не буде створено умов для розвитку соціальної (тобто політичної, економічної, правової, моральної) культури громадян, то жодні конституційні, законодавчі, судові, управлінські чи інші реформи не матимуть антикримінального, зокрема й антикорупційного, ефекту, а отже, й будь-якого взагалі. Мезенцева вважає, що допомогти нашій державі можуть лише реформи на зразок «Нового курсу» Ф.Рузвельта, які мають саме антикорупційний потенціал, тобто створюють умови для розвитку політичної, економічної, правової, моральної культури громадян [4, с. 52].

Інший науковець П.І. Гаман виокремлює аж дев’ять напрямків вдосконалення системи запобігання корупції нашої країни:

1) наявність в країні сильної політичної волі щодо реалізації заходів антикорупційної політики;

2) формування на початковому етапі довіри до дій влади з боку суспільства;

3) тотальний наступ на корупцію, що передбачає впровадження замість перетворень вжиття грунтовних заходів антикорупційної політики;

4) залучення нових кадрів у сферу державного управління щодо антикорупційної політики держави;

5) обмеження ролі держави, а саме в заходах приватизації та податковій реформі;

6) прийняття нестандартних рішень, що насамперед це може стосуватися звільнення під заставу з-під варти осіб, засуджених за корупційні злочини;

7) єдність зусиль ключових політичних осіб, відповідальних за вжиття антикорупційних заходів, та тісної взаємодії між ними;

8) адаптація міжнародного досвіду до місцевих умов України з приводу антикорупційної політики нашої держави;

9) використання технологічних досягнень, що має призвести до зменшення кількості особистих контактів громадян з державними чиновниками і сприятиме підвищенню стандартів прозорості і спрощенню вирішення завдань щодо забезпечення ефективного моніторингу якості надання адміністративних послуг [2].

Таким чином, можна зробити висновок, що сучасна система запобігання корупції в Україні потребує значного вдосконалення для ефективності її застосування. Всі ці заходи вдосконалення, що запропоновані даними науковцями, що були висвітлені вище, є значними і дієвими. Проте, на нашу суб'єктивну думку ще одним важливим заходом вдосконалення системи запобігання корупції є запровадження жорсткіших покарань за корупцію. В основному це є встановлення жорсткої відповідальності за корупційні правопорушення та злочини, а саме, наприклад: заборона дозволу

випускати з під арешту корупціонерів під заставу; закріплення у законі прямої заборони займати будь-які державні посади і працювати в державних органах особам, які мають судимість за корупційні злочини та правопорушення, незалежно від того чи є вона погашена чи непогашена; закріплення чіткого механізму невідворотності покарання за корупційні правопорушення у законодавчих актах, що унеможливить корупціонерів ухилятися від відповідальності, шукаючи різні прогалини у законодавстві. Реалізація таких заходів спричинить у суспільстві страх до вчинення корупційних правопорушень, що неабияк допоможе реально зменшити корупцію в Україні до її мінімальних масштабів поширення.

Література:

1. Публічно-правова протидія корупції: навчальний посібник / В.В. Топчій, В.А. Шкелебей, Т.М. Супрун. Вінниця:ТОВ «Нілан-ЛТД», 2016. 208 с.
2. Гаман П.І. Антикорупційна державна політика: проблеми та перспективи розвитку. Державне управління:удосконалення та розвиток. 2018. №10. URL: http://www.dy.nayka.com.ua/?op=1&z=1316 (дата звернення: 03.11.2019).
3. Заброда Д.Г. Поняття державної антикорупційної політики. Право і безпека. 2012. №2(44). С. 98-104.
4. Мезенцева І.Є. Новий підхід до вдосконалення протидії корупції в Україні. Корупція як загроза національній безпеці України: попереджаємо, протидіємо, переслідуємо: матеріали між. наук.-прак. конф. Київ, 2017. С. 51-54.
5. Скочиляс-Павлів О.В. Правові аспекти удосконалення державної антикорупційної політики. Львів, 2014. С. 27-33.

Використання сучасних технологій відеоаналітики в органах Національної поліції

Русило М.О.
курсант факультету підготовки фахівців для досудового розслідування
Дніпропетровського державного університету внутрішніх справ
Мирошниченко В.О.
професор Дніпропетровського державного університету внутрішніх справ
к. т. н., доцент

На даний час системи відеоспостереження широко застосовуються для забезпечення охорони банків, торговельних центрів, розважальних закладів, промислових підприємств, інших комерційних і некомерційних організацій. Системи відеоспостереження дають змогу здійснювати швидке реагування на небезпечну ситуацію, спостереження за персоналом та відвідувачами, широке застосування та перспективи системи відеореєстрації мають в області контролю за дорожнім рухом. У практиці Національної поліції камерами зовнішнього відеоспостереження обладнуються місця масового скупчення людей і це як правило різного роду парки, сквери, площі, прилегла територія ринків і великих торгових центрів, аварійно-небезпечні ділянки доріг. Сигнали з камер відеоспостереження надходять на спеціальні передавачі, призначені для передачі в локальні комп'ютерні центри відеоконтролю. У цих центрах відбувається процес обробки, стиснення і передачі інформації через волоконно-оптичну мережу на Центральний пост відеоспостереження. Такий пост обладнується прямим каналом аудіозв'язку і режимом обміну відео інформацією з відділами поліції, а також комплектом екстреного зв'язку «тривожна кнопка» для виклику оперативної групи в разі вчинення правопорушення. Для оперативного реагування задіюються екіпажі поліції на автомашинах [1].

Сучасні системи відеоспостереження дозволяють знаходити у людському потоку підозрілих осіб, покинуті речі, які можуть становити небезпеку для оточуючих, виявляти ознаки скоєння правопорушення та слідкувати за діями безпосередньо поліцейських. За допомогою сучасних можливостей відеозйомки впізнання особи стає набагато легше та простіше. Відомо, що людина володіє індивідуальністю (неповторністю) зовнішнього вигляду і відносну стійкість ознак. Процес ідентифікації полягає в порівнянні двох (або декількох) сукупностей ознак між собою. Тому для ідентифікації необхідно виділити ці ознаки. Але традиційні камери відеоспостереження на сьогоднішній день не задовольняють потреб в оперативному реагуванні на можливі позаштатні ситуації на великих об'єктах транспортної інфраструктури. Для вирішення сучасних завдань потрібні комплексні інтелектуальні системи, в основі яких лежать складні алгоритми відеоаналітики.

Відповідно до сучасного кримінально-процесуального законодавства матеріали відеозапису можуть виступати в якості доказів у кримінальній справі, будучи додатками протоколів слідчих і судових дій, речовими доказами, а також іншими документами [2]. При описі зовнішності людини

великими елементами особи, що володіють криміналістично значущими ознаками, є: волосяний покрив голови, лоб, брови, очі, повіки, щоки, ніс, носогубний фільтр, губи, зуби, підборіддя, вушні раковини. Однак у великому елементі при поглибленому його вивченні можна виділити складові частини: при описі очей - будова очної щілини, виступання очних яблук, вид внутрішніх кутів очей; при описі носа - перенісся, спинка носа, підстава носа, крила носа. При цьому кожен елемент зовнішності може характеризуватися такими ознаками: формою, розміром, положенням, кольором. Парні елементи також мають симетрію або асиметрію. Кожна ознака має три значення вираженості (два крайніх і одне середнє). На думку фахівців, «загальне число людей, з яких може бути виділено кожну особу за сукупністю цих ознак, дорівнюватиме 950».

Як відомо, в роботі по розкриттю злочинів важливе значення має фактор часу. Більшість злочинів розкривається в результаті розшуку злочинців «по гарячих слідах». Тому, чим раніше стане відомо органам поліції про скоєний злочин, тим реальніше є можливість швидко виявити і затримати злочинця. Це пояснюється тим, що злочинці іноді протягом деякого часу після вчинення злочину знаходяться на невеликій відстані від місця скоєння злочину, можуть зберігати на собі сліди злочину і мати предмети, здобуті злочинним шляхом. Використовуючи новітні методи отримання та обробки відеоінформації, можна, здійснювати безперервний збір та передачу, інтелектуальний аналіз і архівування відеоданих від великого числа камер з можливістю оперативного відображення і доступу до відеоархіву з робочих місць операторів. Захищені від вандалів камери рекомендується встановлювати на території міста в найбільш криміногенних місцях (місцях скупчень людей, під'їздах житлових будинків, дорогах, провулках, і т.д.).

Практично будь-яке обладнання або пристрої для відеоспостереження, володіють розширеними величезними настройками для якості зйомки в денний або темний час зйомки з можливістю застосування посилення деталізації, промальовування (картинки як в HDR режимі) і іншими корисними ефектами [3].

Перспективними напрямками застосування відеоаналітики може бути запобігання заворушень у місцях масового скупчення людей, наприклад, біометричне впізнання - це превентивний захід, який дозволяє звести до мінімуму небезпеку виникнення скупченості та несподіваних конфліктів на вході, оскільки у рази підвищується пропускна можливість у зоні турнікетів.

Отже, значення віодеоаналітики у Національній поліції має величезну користь у сприйнятті та обробці інформації , яка допомагає у вирішенні та профілактиці задач щодо правопорушень.

Підсумовуючи викладене, зазначимо, що сьогодні сучасні засоби відеофіксації, канали передачі відеоінформації, засоби зберігання та обробки інформації мають досить високі технічні характеристики, що дозволяє створювати досить гнучкі і ефективні системи безпеки. Подальшим напрямком удосконалення систем відеофіксації повинні стати розробка інтелектуальних систем обробки відеоматеріалу і програмні засоби відеобіоідентіфікаціі людини.

Література:

1. Наказ 18.12.2018 № 1026 Про затвердження Інструкції із застосування органами та підрозділами поліції технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, засобів фото- і кінозйомки, відеозапису https://zakon.rada.gov.ua/laws/show/z0028-19
2. Кримінально-процесуальний кодекс України (Відомості Верховної Ради України (ВВР), 2013, № 9-10, № 11-12, № 13, ст.88) https://zakon.rada.gov.ua/laws/show/4651-17
3. Умная система видеонаблюдение – значение максимальной безопасности от злоумышленника, http://xtgamers.com/page-id-14648.html

SRS Femida – сучасна система технічної фіксації судового процесу

Шевченко О.І.
курсант 402-го взводу
Одеського державного університету внутрішніх справ
Форос Г.В.
професор кафедри кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішніх справ, к.ю.н., доцент

В розвитку сучасного демократичного суспільства велику роль відіграють інформаційні технології, які відкривають можливості до вільного доступу та обміну інформацією та гласності судового процесу та його повного фіксування технічними засобами, що є невід'ємним конституційним правом людини. Необхідно зазначити, що судовий процес повинен фіксуватися технічними засобами.

Фіксування судового процесу технічними засобами - технічний запис судового засідання за допомогою комплексу з фіксування судового процесу , що включає в себе створення аудіофонограми судового засідання. [1]

Доцільно було б розглянути таку систему технічної фіксації та протоколювання судового процесу, як «SRS Femida», яка здійснює цифрову багатоканальну аудіо- і відеозапис, що забезпечує прозорість судових процесів.

Система "SRS Femida" – є одним з базових компонентів в оснащенні залів судових засідань сучасними засобами, які автоматизують роботу судів. Система суттєво спрощує роботу секретарів у цілому та дозволяє повністю відмовитись від використання ручки та паперу для складання протоколів судових засідань. [2]

Система технічної фіксації та протоколювання судового процесу "SRS Femida" є досить інноваційним рішенням, яке розраховане для залів засідань, судових слухань, залів для переговорів. Компанія "Спеціальні Реєструючі Системи" встановила вже понад 15000 цифрових систем звукозапису на базі комп'ютерів у понад 16 країнах світу в судах, урядових та фінансових установах,, аеропортах, організаціях громадської безпеки електростанціях і т.д.

На сьогоднішній день система "SRS Femida" успішно застосовується у верховних, апеляційних, районних судах Вірменії (Проект Світового Банку), Грузії, , Казахстану (Проект Агентства США з міжнародного розвитку (USAID), Молдови (проект USAID), Гани , України (державна програма). Система технічної фіксації та протоколювання судового процесу «SRS Femida» є також комплексним рішенням, оскільки забезпечує легітимність аудіо/відеозапису, судового протоколювання та тиражування всієї документації і відповідних мультимедіа даних.

Система технічної фіксації та протоколювання судового процесу «SRS Femida» проста у використанні і значно спрощує процес підготовки протоколів судових засідань завдяки спеціальному редактору із застосуванням уніфікованих і редагованих шаблонів судових засідань. Спеціальний редактор здійснює повну фіксацію усіх процесуальних дій (журнал подій) у хронологічній послідовності та одночасну синхронізацію цих дій з відповідними фрагментами аудіо / відеозапису. Синхронізація аудіо- та відеоданих до тексту забезпечує моментальний доступ до необхідного події судового засідання, що є дуже зручно. У разі необхідності секретар створює в її первісному вигляді стенограму судового засідання у цілому або його фрагмента. При ознайомленні зі стенограмою досить тільки натиснути на будь-якому слові в тексті стенограми та автоматично починається відтворення відповідного фрагмента запису судового засідання. Це є досить вагомою перевагою системи «SRS Femida» у порівнянні з аналогічними системами аудіозаписи судових процесів.

Повнофункціональна установка системи, її технічна підтримка та обслуговування забезпечується у будь-якому регіоні тільки завдяки доступним дилерських мереж. Інсталяція, підтримка обладнання та спеціального програмного забезпечення здійснюється висококваліфікованими фахівцями, які підготовлюють комплекс до роботи, проводять його тестування, проводять тренінг для персоналу та тестове судове засідання.

Слід зазначити основні важливі функції системи «SRS Femida»:

Цифрова 2, 4 або 8-канальний аудіозапис;

Цифрова відеозапис (опціонально);

Синхронне відтворення аудіо / відеоданих з текстом;

Збереження і резервне збереження даних на жорсткий диск, CD / DVD диски, мережеві ресурси;

Сумісність з Windows 2000 / XP / Vista / 7 / 8.1 / 10;

Підтримка архітектури «Клієнт - сервер»;

Інтуїтивно зрозумілий інтерфейс;

Можливість аварійного відновлення;

Інтеграція з існуючими системами судового діловодства;

Система моніторингу працездатності системи;

Створення електронних протоколів судових засідань на основі уніфікованих і редагованих шаблонів судових засідань. [3]

Інтеграція із Системою технічної фіксації судового процесу «SRS Femida» насамперед забезпечує швидкий доступ до текстів протоколів та аудіозаписів та зберігання шаблонів протоколів судових засідань для різних категорій справ. А великою перевагою цієї системи є багатоканальний аудіо-відеозапис, Захист даних від модифікацій і фальсифікацій та синхронізація аудіо-відеозапису з текстом протоколу судового засідання. Система технічної фіксації та протоколювання судового процесу «SRS Femida» скорочує витрати, економить час, оптимізує ресурси і пропонує точне і надійне рішення для судів з метою гарантії прозорості судочинства, тому є дуже актуальною у наш час та допомагає проводити судові засідання результативніше.

Література:
1. Про затвердження інструкції про порядок фіксування судового процесу технічними засобами [Електронний ресурс] : Наказ від 21.07.2005 №84. Електронні данні Режим доступа: http://zakon/rada.gov.ua/laws/show/z0868-05
2. SRS Femida файл [pdf] [Електронний ресурс] : документ. Електрон. дан. [С] & [Р], 2019. Режим доступа: http://srs.kiev.ua/wp-content/uploads/2019/08/SRS-Femida-Brochure-UA_2019.pdf. Дата звернення: 31.10.2019. Загл. з екрану.

Використання інформаційних технологій під час розслідування злочинів

Щирська В. С.
доцент кафедри кримінального права та кримінології
факультету підготовки фахівців для органів досудового розслідування
Одеського державного університету внутрішніх справ
к.ю.н., капітан поліції
Зварич Р. А.
курсант 302 взводу
Одеського державного університету внутрішніх справ
рядовий поліцій

Актуальним питанням сьогодення, що потребує розгляду, є значення та роль інформаційних технологій під час розслідування злочинів, так як стрімке впровадження в різні галузі життєдіяльності суспільства новітніх досягнень науково-технічного прогресу та заміна традиційних знарядь праці й комунікацій на комп'ютерну техніку призвели до кардинальної зміни механізму вчинення злочинів.

Інформаційні технології викликали появу нових можливостей, які використовуються злочинцями для скоєння злочинів на національному, міжнародному і транснаціональному рівнях. Злочинні об’єднання, окремі «фахівці» кримінального бізнесу повною мірою використовують новітні технології для «відмивання» грошей, здобутих злочинним шляхом, несанкціонованого доступу до інформаційних систем та інших злочинних дій. Це потребує застосування адекватних засобів протидії таким злочинним проявам шляхом впровадження досягнень науки і техніки у діяльність правоохоронних органів. [4, с. 9]

Чимало науковців займалися дослідженням цієї проблеми, зокрема П.Д. Біленчук, С.С. Чернявський, Р.А. Калюжний, М.А. Погорецький, А.І. Марущак, В.Ю. Шепітько, В.П. Бахін та інші. Саме їх внески мають вагоме значення для подальшого повного та всебічного висвітлення проблеми.

Інформаційні технології - це система методів, процесів та способів використання обчислювальної техніки і систем зв'язку для створення, збору, передачі, пошуку, оброблення та поширення інформації з метою ефективної організації діяльності людей. Тобто закономірним наслідком розвитку інформаційних технологій стає їх глобальне впровадження в усі аспекти життєдіяльності людини. [1, с. 458]

Для підвищення ефективності та оперативності розслідування злочинів нині накопичений чималий досвід застосування новітніх технологій у процесі попередження, виявлення та протидії злочинності, розшуку підозрюваного та обвинуваченого, провадження окремих слідчих (розшукових) дій, здійснення судових експертиз.

Основними напрямами використання інформаційних технологій у досудовому слідстві є створення та ведення криміналістичних обліків, побудова суб’єктивних портретів, користування базою законодавства України та іншими базами даних. У сучасних вимогах слідчим потрібні інформаційні технології для оптимізації управління процесами інформаційного забезпечення, здійснення автоматизованого пошуку відомостей щодо будь-яких об’єктів (осіб, предметів, подій), одержання формалізованих знань з усіх видів баз даних, що існують у світі, статистичного і географічного аналізу подій, пошуку окремих об’єктів, осіб тощо.

Інформаційні технології надають можливість оперативного збирання, зіставлення та аналізу відомостей з різних джерел (повідомлень, результатів оперативно-розшукових заходів, допитів, адресної бази даних тощо), установлення хронологічної послідовності подій за часом та відповідності окремих фактів, дозволяють здійснювати складання планів та схем місця події, моделювання події злочину за допомогою комп’ютерної техніки, а також забезпечують можливість отримання інформації у повному, систематизованому та зручному для користування вигляді співробітниками та підрозділами органів внутрішніх справ.

Прикладом застосування інформаційних технологій під час розслідування злочинів в Україні є стаття 232 КПКУ, що регламентує проведення допиту, впізнання у режимі відеоконференції під час досудового розслідування за допомогою інноваційних продуктів (зокрема, комунікаційної системи Skype). Також згідно зі статтею 240 КПКУ задля уточнення відомостей, які мають значення для встановлення обставин кримінального правопорушення, слідчий, прокурор має право провести слідчий експеримент під час якого можуть проводитися вимірювання, фотографування, звуко- чи відеозапис, складатися плани і схеми, виготовлятися графічні зображення, відбитки та зліпки, які додаються до протоколу.

Важливою інформаційною технологією став передбачений статтею 214 КПКУ Єдиний реєстр досудових розслідувань. Цей реєстр визначено як створену за допомогою автоматизованої системи електронну базу даних, відповідно до якої здійснюється збирання, зберігання, захист, облік, пошук, узагальнення даних, що стосуються кримінального правопорушення (дата надходження заяви про вчинення злочину, короткий виклад обставин, що можуть свідчити про вчинення кримінального правопорушення тощо).

Отже, внаслідок науково-технічного прогресу та розвитку інформаційних технологій злочин починає набувати нових, більш складних форм. Звідси виникає потреба в покращенні матеріального забезпечення та застосуванні новітніх технологій у діяльності правоохоронних органів задля протидії цим злочинам. На даному етапі в Україні створюються та успішно використовуються різноманітні інформаційно-пошукові системи, бази та банки даних, системи електронного документообігу, що сприяють ефективному виконанню різноманітних оперативно-службових завдань. Відбувається переоснащення інформаційних підрозділів сучасною потужною комп'ютерною технікою, а ефективність роботи правоохоронних органів безпосередньо залежить від їх вмінь та навичок володіння тією або іншою комп’ютерною програмою.

Література:

1. Інформаційні системи і технології на підприємствах : підручник / В.Л. Плескач, Т.Г. Затонацька. К. :Знання, 2011. 18с.
2. Криміналістика: підруч. / В.Ю. Шепітько, В.О. Коновалова, В.А. Журавель [та ін.]: за ред. В.ІО. Шепітька. 5-те вид. переробл. та допов. К.: Ін Юре, 2016. 640 с.
3. Кримінальний процесуальний кодекс України: чинне законодавство із змінами та доповненнями на 04 серпня 2017 року: Офіц. Текст. К.: Алерта, 2017. 292 с.
4. Практикум з криміналістики : навч.. посібн.. / кол.. авторів : В.Ю. Шепітько, В.О. Коновалова, В.А. Журавель та ін.. ; за ред.. В. Ю.. Шепітька.. К.. : Ін Юре, 2013.. 128 с.

Інформаційно-аналітичний документ як результат інформаційно-аналітичної діяльності

Форос Г.В.
професор кафедри кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішніх справ
к.ю.н., доцент
Кірей Д.В.
слухачка 2 курсу
Одеського державного університету внутрішніх справ

Інформаційні-аналітична діяльність є невід'ємною частиною всіх сфер суспільного життя. Вона має певні цілі та завдання, для реалізації яких існують конкретні засоби, що сприяють отриманню необхідних результатів. У нашій державі існують спеціальні інформаційно-аналітичні установи, що складають систему інформаційного забезпечення користувачів документальною інформацією універсального, галузевого, проблемно-тематичного змісту.

В процесі здійснення наукової діяльності постала гостра потреба у створенні спеціальних документів, які б допомогли користувачеві полегшити пошук документу. Проблема методичних особливостей сучасних інформаційно-аналітичних документів є важливою не тільки для працівників інформаційних структур, але й для викладачів навчальних закладів, де готують фахівців інформаційної діяльності як майбутніх створювачів інформаційної продукції. Аналіз наукових праць, присвячених цій проблематиці, дозволяє стверджувати, що теоретико-методичні засади інформаційно-аналітичної діяльності знаходяться в стадії формування.

Одним з актуальних питань є визначення поняття «інформаційно-аналітичний документ» та встановлення його особливостей. Відмінність інформаційних документів від інших документів полягає насамперед у тому, що вони є результатом опрацювання інформації, яка міститься в інших (вихідних або первинних) джерелах інформації. Отже, інформаційний документ належить до вторинно-документального рівня інформації і має властивості вторинного документа, а саме: містить інформацію з первинних документів в узагальненому вигляді; містить відомості про сам первинний документ, на основі якого його створено; обов'язково є результатом аналітико-синтетичного опрацювання вихідного документа; є результатом та засобом інформаційної діяльності, за допомогою якого здійснюються інформаційні процеси.

За рівнем згортання вихідну інформацію в інформаційно-аналітичних документах можна поділити на чотири види: бібліографічна інформація; реферативна інформація; оглядова інформація; оглядово-аналітична інформація. Але, ми вважаємо, що цільове призначення інформаційних документів з аналітичною інформацією не змінює його допоміжної функції в системі інформаційного забезпечення. З метою визначення можливостей різних інформаційно-аналітичних документів для забезпечення інформаційних потреб замовників інформації, а також, щоб навчитися створювати такі документи, слід впорядкувати їх, іншими словами, класифікувати інформаційно-аналітичні документи.

За методом викладення змістової інформації у вторинному документі вирізнимо такі інформаційно-аналітичні документи:

1) документ-екстракт. Це документ, побудований на реченнях, що містять основні положення змісту вихідного документа та екстрагуються з нього в інформаційно-аналітичний документ;

2) перефразований документ. Інформаційний документ, в якому зміст вихідного документа передається у перефразованому вигляді. Так складається більшість видів інформаційно-аналітичних документів;

3) інтерпретований документ. В такому інформаційно-аналітичному документі зміст вихідного джерела передається на основі узагальненого уявлення про нього. Таке подання змісту первинного документа найбільш характерне для документів оглядового типу.

Універсальної класифікації інформаційно-аналітичних документів на сьогоднішній день не існує, але виділяють наступні види наукових документів. Одним з найпоширеніших видів інформаційно-аналітичної діяльності є реферування. Витоки практичної реферативної діяльності, як відомо, зародилися й набули розвитку в бібліотечно-бібліографічній практиці, при цьому увагу головним чином, змісту документа, його основним даним і висновкам.

В системі наукової комунікації та інформаційно аналітичної діяльності реферат є основною інформаційно-комунікативною одиницею, що зумовлено його споживчими властивостями: серед усіх видів вторинних інформаційних документів реферат відрізняється найбільшою інформативністю в розкритті змісту першоджерела; використання реферату для пошуку поточної або ретроспективної інформації дає змогу зекономити до 90 % часу, необхідного в разі звернення до первинних документів; форма подання інформації у вигляді реферату зручніша для тривалого зберігання у фондах довідково-інформаційних служб, полегшує та прискорює підготовку інформаційних видань і створення інформаційних масивів; у деяких випадках реферат може замінити першоджерело (коли необхідна користувачеві інформація стосується не основної теми роботи, а суміжних питань, або коли первинний документ недоступний унаслідок мовного або організаційного бар'єрів).

Аналіз наукових праць, дозволив прийти до висновку, що реферат - це багатофункціональний вторинний документ. Він виконує безліч функцій: інформативну та науково-комунікативну, прогностичну, довідкову і адресну, індексування й індикативну. Відповідно до завдань реферат може надавати необхідну систематизовану фактографічну інформацію, оцінювати, узагальнювати, синтезувати її, рекомендувати найбільш нові, цінні та корисні повідомлення для конкретного користувача. Наявність у рефераті точного бібліографічного опису документа забезпечує виконання рефератом адресної функції, без чого неможливий документальний інформаційний пошук. Ще одна функція реферату - можливість індексування змісту первинних документів без використання текстів першоджерел.

Згідно з науковими розробками О. А. Гречихіна, під реферативною інформацією слід розуміти змістовний результат процесу реферування, який відображається в реферативному виданні у формі певного знакового (літературного) твору - реферату чи їх сукупності - для виявлення нової, цінної та корисної документальної інформації. Методика реферування полягає у послідовному здійсненні операцій, пов'язаних з оцінкою, відбором, аналізом і узагальненням відомостей, які містяться у первинному джерелі. Процес реферування базується на виконанні цих логічних операцій. Однією з основних специфічних особливостей, на яку необхідно зважати у ході складання реферату, є його повна

змістова та деяка формальна залежність від первинного документа. У такому розумінні реферат слід розглядати як інформаційну модель реферованого документа.

Таким чином, цінність оглядово-аналітичних документів пов'язана з можливістю швидкого «входження» з їхньою допомогою в певну проблематику, а також з тим, щоб скласти уявлення про перспективні напрями її розвитку. Між оглядовими та аналітичними документами багато спільного, тому їх часто розглядають як змішаний вид вторинних документів – оглядово-аналітичні документи.

Література

1. Про інформацію [Електронний ресурс]: закон України від 02.10.1992 № 2657-12 в редакції Закону України від 01.01.2017, підстава 1774-19. Електрон. дан. (1 файл). Режим доступу: http://zakon1.rada.gov.ua. Назва з екрана.
2. Сілкова, Г.В. Інформаційно-аналітична діяльність у структурі інформаційної діяльності // Бібліотекознавство. Документознавство. Інформологія . 2007р. - №4. 37-44.
3. Хромченко, Л.Г. Організація інформаційної діяльності (теоретичні основи): навч. Посіб. Для студентів сеціальності «Міжнародна інформація», «Міжнародні економічні відносини»/ Л. Г. Хромченко, О.С. Раковська-Башмакова, А.С. Шраєр; за ред.. Х.В. Чаковського. Х. : «МСУ Харків», 2013. 352с.

Особливості співробітництва правоохоронних органів країн ЄС у сфері протидії кібертероризму

Форноляк В.М.
доцент кафедри «Боротьба з тероризмом та захист
учасників кримінального судочинства»
Національна академія Служби безпеки України
к. п. н.

Новітній етап розвитку України, як незалежної держави, характеризується поглибленням співробітництва з іншими державами у різних сферах. Нагальної та особливої уваги потребує співробітництво у сфері протидії кібертероризму, яке зумовлене розвитком транснаціональної терористичної злочинності. У зв’язку з цим Україна співробітничає з різними країнами керуючись міжнародними договорами. Окрім того, антитерористична діяльність вітчизняних суб’єктів боротьби з тероризмом певним чином пов’язана з діяльністю такої європейської інституцій, як Європол.

Правоохоронні органи країн Євросоюзу значну увагу приділяють питанням протидії поширенню ідеології тероризму в інформаційно-телекомунікаційних мережах. Це зумовлено тим, що останнім часом організації та групи терористичної спрямованості досить широко використовувати можливості соціальних медіакомунікацій та Інтернету. Варто згадати як групи джихадистів використовуючи Інтернет організували погоджені кампанії в соціальних мережах для залучення прибічників для звеличання актів тероризму [1]. Досить часто терористичні угруповання мають свої веб-сайти, однією із задач яких є вербування нових членів. Окрім веб-сайтів вони створюють власні телевізійні канали. Правоохоронними органами зафіксовувалися епізоди цілеспрямованого вербування прихильників різних суспільних напрямів, віртуального заохочування до дій терористичної спрямованості [2, с. 239].

Для підвищення ефективності заходів щодо протидії поширенню тероризму та реалізації скоординованої діяльності антитерористичних організацій в системі Європейського контртерористичного центру Європолу (ECTC) функціонують Групи інтернет-досліджень (European Internet Referral Unit, IRU), які уповноважені співпрацювати з правоохоронними органами як держав-членів Європейського Союзу, так й інших держав та приватним сектором, ключовими задачами яких є: координація й обмін між правоохоронними органами інформацією про хід виконання завдань щодо ідентифікації терористичного й насильницько-екстремістського інтернет-контенту; виконання завдань щодо ідентифікації забороненого інтернет-контенту у співробітництві з операторами зв'язку й власниками інформаційних ресурсів; підтримка правоохоронних органів шляхом надання стратегічного й оперативного аналізу [3].

Активну роль у сфері протидії кіберзагрозам відіграють й міжнародні організації. Зокрема, з 2013 року у структурі Європолу в Гаазі (Нідерланди) функціонує Європейський центр по боротьбі з кіберзлочинністю (European Cybercrime Centre – EC3). Слід зауважити, що ця організація здійснює висококваліфіковані технічні, аналітичні й цифрові судові експертизи для забезпечення розслідувань

злочинів правоохоронними органами держав-членів ЄС і асоційованих партнерів Європолу у випадках використання віртуального простору з терористичною метою [4].

Для підвищення ефективності боротьби з кіберзлочиністю Комісією Євросоюзу розроблена погоджена політика співробітництва між державами-членами ЄС а також відповідними установами, що реалізовано у зверненні Єврокомісії до Європарламенту «Стратегії кібербезпеки Євросоюзу: відкритий, безпечний і надійний кібер-простір». В цьому документі пропонується розширити співпрацю як на рівні правоохоронних органів окремих країн, так і глобальну міжнародну співпрацю [5].

Значним кроком стало прийняття «Директиви про атаки проти інформаційних систем» [6], що сприяло покращенню міжнародного співробітництва між судовими та правоохоронними органами держав-членів Європейського Союзу і зобов'язало здійснювати збір статистичної інформації щодо кібератак і централізовано направляти її до компетентних органів.

Питання протидії кіберзлочинності перебувають також в центрі уваги органів та інституцій Організації Об'єднаних Націй, зокрема Генеральної Асамблеї, Економічної і Соціальної Ради, Комісії з попередження злочинності і кримінального правосуддя, конгресів ООН з попередження тероризму та злочинності, рішення яких потребують розробки шляхів і засобів для вирішення.

В антитерористичній діяльності правоохоронних органів країн Євросоюзу активно використовуються сучасні інформаційно-телекомунікаційні системи, впроваджені новітні форми реалізації інформаційно-правоохоронного співробітництва країн ЄС. У процесі співробітництва Європолу з іншими державними правоохоронними органами держав-членів Європейського союзу щодо протидії кібертероризму важливе значення має організація інформаційних комунікацій, які варто розглянути. Зокрема, Інформаційна система Європола (Europol Information System, далі - EIS) – це одна з основних інтегрованих баз даних агентства ЄС. Завдяки цій системі держави-члени мають можливість здійснювати інформаційний обмін щодо підозрюваних, засуджених, подій та фактів, пов'язаних з організованою злочинністю та тероризмом. EIS надає первинну інформаційну підтримку під час розслідувань, що дозволяє швидко визначити наявність відповідної інформації, здійснити пошук посилань на її джерело, з яких потім можна буде одержати інформацію за допомогою регламентного запиту через уповноважений національний підрозділ [7].

Деталізований аналіз фронтальних баз даних у сфері боротьби з тероризмом проводиться у спеціалізованому контртерористичному обліку (the Counter Terrorism Analysis Work File, далі - AWF) та самостійних фокусних групах. Облік AWF забезпечує підгрунтя для оперативної інформаційно-аналітичної підтримки у сфері протидії тероризму. В зазначеному обліку утримується та опрацьовується значний обсяг інформації з різних напрямів. Отримана інформація щодо терористичних спрямувань обробляється в рамках самостійних координаційних центрів. У цих інформаційних теренах здійснюється збір інформації, перевірка, аналіз за допомогою спеціальних груп контртерористичних аналітиків і експертів. Основним координаційним центром є аналітична група «Мандрівники» [8].

Слід зазначити, що ЕСТС здійснює комплексний підхід до обробки інформації, а її інформаційний центр забезпечений від будь-якого несанкціонованого доступу та працює в режимі он-лайн: 24 години на добу, 7 днів на тиждень. Інформація, яка знаходиться в одній інформаційній системі, автоматично звіряється з усіма іншими базами даних Європолу, щоб доповнити відсутні дані.

Фундаментом діяльності Європолу становить взаємний обмін інформацією, тому швидка та безпечна її передача має важливе значення. Інформаційний обмін між країнами Євросоюзу й Європолом здійснюється з дотриманням визначених правил конфіденційності. Для підвищення ефективності обміну інформацією правоохоронними органами країн Євросоюзу, Європолом та іншими суб'єктами, які мають угоди про оперативне співробітництво з Європолом, створений та активно використовується мережний додаток по безпечному обміну інформацією (the Secure Information Exchange Network Application, SIENA). Ця платформа забезпечує зручний та швидкий обмін стратегічною і операційною інформацією, яка доступна для: аналітиків та експертів, офіцерів зв'язку Європолу, держав-членів, третіх сторін, з якими Європол має угоду щодо співпраці. На даний час понад 90% усіх держав-членів та 46 контртерористичних органів підключені до спеціальної контртерористичної среди SIENA.

З кінця 2017 року в рамках Європолу працює цифрова антитерористична платформи SIRIUS для проведення онлайн-розслідувань. Це новітня система для вирішення поточних завдань, що стоять перед правоохоронними органами при дослідженні мережі Інтернет. SIRIUS використовується як веб-платформа для співробітників правоохоронних органів і операторів зв'язку для обміну досвідом й передовими методами в галузі розслідування злочинів, пов'язаних з використанням мережі Інтернет. SIRIUS отримує відомості від різних інтернет-сервісів і надає правоохоронним органам інструментарій

для їх аналізу з можливістю зворотного зв'язку – це дозволяє більш оперативно оформляти запити [9]. Із платформою SIRIUS співробітничають представники Facebook, Google, Microsoft, Twitter і Uber.

Таким чином, розвиток співробітництва у сфері протидії кібертероризму між Україною та ЄС є пріоритетом для нашої держави. Чинні Угоди про співробітництво між Україною та Європолом формують правову базу для використання нами можливостей цієї організації, а саме: компетентні органи України і ЄС можуть ефективно співпрацювати у розслідуванні злочинів терористичної спрямованості, розгляді питань щодо співробітництва в цілому, боротьби з тероризмом та організованими злочинними угрупованнями в сферах кіберзлочинності, торгівлі людьми, здійснювати обмін стратегічною і оперативною інформацією проводити спільні навчально-тренувальні заходи антитерористичного характеру.

Література:

1. Интернет-справочник ЕС - IRU ЕС [Електронний ресурс]. Режим доступу : https://www.europol.europa.eu/about-europol/eu-internet-referal-unit-eu-iru.
2. Мукомела І. Кібернетичний тероризм – загроза національній безпеці XXI ст. *Протидія терористичній діяльності: міжнародний досвід і його актуальність для України: мат-ли міжнар. наук.-практ. конф.* (30 вересня 2016 року). Київ: Національна академія прокуратури України, 2016. С. 238–241.
3. Europols internet referral unit combat terrorist and violent extremist propaganda. [Електронний ресурс]. Режим доступу: www.europol.europa.eu/content/europol%E2%80%99s -internet-referral-unit-combat-terrorist-and-violent-extremist-propaganda.
4. Европейский центр киберпреступности - ЕС3 [Електронний ресурс]. Режим доступу: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.
5. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace : Joint communication to the European parliament, the Council, the European economic and social committee and the Committee of the regions : JOIN(2013) 1 final : Brussels, 07.02.2013 [Електронний ресурс]. Режим доступу : http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf.
6. Рамкове рішення № 2005/222/ПВД Ради про атаки на інформаційні системи [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/994_a82/card5?lang.
7. Інформаційні системи Європолу [Електронний ресурс]. Режим доступу: https://pravo.studio/osnovyi-kriminalistiki/informatsiyni-sistemi-evropolu-75838.html.
8. The European Unions's Policies on Counter Terrorism [Електронний ресурс]. Режим доступу: http://www.europarl.europa.eu/RegData/etudes/stud/2017/583124/ipol_stu(2017)583124_en.pdf.
9. Платформа для служителей закона ЕС [Електронний ресурс]. Режим доступу: https://threatpost.ru/europol-launches-sirius/23068

Метод фактологічного аналізу як один із методів доказування

Цільмак О.М.
професор кафедри соціології та психології
Національного університету «Одеська юридична академія»
д.ю.н., професор
ORCID: 0000-0001-7348-4876

На сучасному етапі модернізації слідчої діяльності існує необхідність осучаснення методичного забезпечення досудового розслідування кіберзлочинів. Слід зазначити, що у слідчих органів досудового розслідування Національної поліції України в арсеналі є досить велика кількість методів, однак, й є досить велика кількість методів, що не винайшли теоретико-методологічного обґрунтованого опису. Серед таких методів слід виділити й метод фактологічного аналізу, який є одним із вагомих методів доказування.

Концептуальним положенням фактологічного аналізу, як загальносистемного методу правозастосовної діяльності, присвячені праці Колдіна В.Я., Александрова І.В., Крестовнікова О., Смірнової С. та ін. Однак, досі залишається фактично неопрацьованим науковий апарат його загальнотеоретичних положень та не має чіткого опису технології його застосування. Усе це істотно ускладнює і знижує ефективність застосування зазначеного методу під час досудового розслідування кримінальних правопорушень. У зв'язку з цим, досить актуальними питанням (як в теоретичному так і в практичному сенсі) є:

1) опис загальнотеоретичних положень методу фактологічного аналізу, тобто розкриття змісту його дефініції, визначення та конкретизація його мети, завдань, предмету, об'єкту, суб'єктів застосування, основних переваг та недоліків, основних принципів та правил застосування;

2) конкретизація технології його застування на підготовчому, основному та заключному етапах.

Отже, як відомо, існують такі різновиди доказів [3]:

1) фактологічні – які спираються в основному на фактичний матеріал;

2) формально-логічні – які спираються закони формальної логіки;

3) експериментальні – які побудовані на експерименті;

4) емпіричні – які спираються на осмислений і узагальнений досвід.

Для того щоби зазначені різновиди доказів були належними, допустимими та достовірними, вони повинні базуватися на низці науково обґрунтованих методів, які доведуть їх повноту та надійність. Отже, кожен з цих різновидів доказів ґрунтується на провідному методі науково-практичного пізнання. Зокрема, фактологічні докази забезпечуються методом фактологічного аналізу.

Під фактологічним аналізом слід розуміти спосіб виділення з масиву даних стосовно кримінального правопорушення фактів (або окремих елементів, сегментів, частин фактичних даних) для їх подальшого агрегування (цілісного об'єднання) та встановлення ступеню доказового значення.

Слід зазначити, що метод фактологічного аналізу є інтегральним інформаційно-пошуковим способом пізнання, який взаємопов'язаний з іншими методами пізнання, такими як:

1) загальнологічні (аналіз, синтез, індукція, дедукція, наукова абстракція, узагальнення, аналогія, моделювання, класифікація та ін.);

2) графічні (таблиці, графіки, діаграми, матриці та ін.); 3) емпіричні методи (порівняння, опис);

4) математичні (реєстрація, математичне та геометричне моделювання, ранжування (рангова оцінка), шкалювання та ін.);

5) криміналістичний моніторинг;

6) стратегічного планування;

7) програмні та апаратні методи обробки та захисту інформації, контролю достовірності інформації та ін.

Як й кожний метод, що застосовується під час досудового розслідування кримінального правопорушення, метод фактологічного аналізу має власну мету, завдання, об'єкт і предмет вивчення та потребує дотримання певних принципів, правил й умов його застосування. Отже, розглянемо зазначені загальнотеоретичні положення.

Так як, основною метою фактологічного аналізу є фактологічний доказ того, що наявна сукупність фактичних даних про факти та обставини кримінального правопорушення є: 1) належними, допустимими та достовірними доказами; 2) взаємопов'язаними та достатніми для прийняття обґрунтованого процесуального рішення; – то зазначений метод потребує ретельного розкриття через його алгоритм застосування під час досудового розслідування кіберзлочинів.

Література:

1. Колдин В.Я. Обоснование правового решения: фактологический анализ. *Учебно-практическое пособие*. М.: МГУ им. М.В. Ломоносова, 2014., 512 с. URL: http://stom.tilimen.org/v-svyazi-s-etim-predstavlyaetsya-ustarevshim-tradicionnij-vzgl.html?page=3

Колдин В.Я. Фактологический анализ в структуре правоприменительной деятельности // *Вестник Московского унивнрситета*. Серия 11. Право. 2008. № 6

2. Коротков Э.М. Исследование систем управления: учебник. Москва. Издательско-консалтинговая компания «ДеКА» 2014. URL: http://www.bibliotekar.ru/sistema-upravleniya/79.htm

СЕКЦІЯ 4
ПІДГОТОВКА ПЕРСОНАЛУ ДЛЯ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ В УКРАЇНІ

Актуальні аспекти підготовки кадрів з попередження кіберзлочинності в Україні

Моїсеєнко К.Д.
Студент групи-ПМСПз-19-1
Університету державної фіскальної служби України
Полуніна Л.В.
старший викладач кафедри фінансових розслідувань
Університету державної фіскальної служби України

Широке розповсюдження комп'ютерної злочинності вимагає розроблення якісно нових підходів до підготовки фахівців у галузі інформаційних технологій для оперативних підрозділів Національної поліції, у тому числі для підрозділів кіберполіції. Відповідна методика має передбачати не лише навчання прийомам виявлення, розслідування і припинення комп'ютерних злочинів, але й, передусім, озброєння фахівців сучасними знаннями, які дозволяють широко та ефективно застосовувати інформаційні технології на різних напрямах оперативно-розшукової, слідчої й іншої службової діяльності.

Однією з кадрових проблем Національної поліції в сучасних умовах є потреба фахівців, які здатні убезпечити особу, суспільство та державу на новому технологічному рівні. Ефективно протидіяти злочинності під силу лише правоохоронцям, які досконало володіють законодавчою базою, мають належний рівень професійної підготовки, достатній досвід боротьби з сучасними видами злочинів.

Підготовка кваліфікованих кадрів у цьому напрямі і забезпечення ними практичних підрозділів – з кожним роком все чіткіше набуває міжвідомчого характеру, оскільки сама кіберзлочинність з вузьковідомчого статусу реально виходить на рівень проблеми національної безпеки.

У зв'язку з різким переходом систем управління на ІТ-рішення відчувається нестача фахівців у сфері інформаційної безпеки. І в нашій країні така необхідність зростає набагато швидше, ніж йде підготовка відповідних кадрів.

Особливістю професійної підготовки фахівців у галузі інформаційних технологій є динамічний розвиток новітніх інформаційно-телекомунікаційних технологій і, відповідно, змісту навчання. Ця проблема має вирішуватись своєчасним оновленням змісту навчання й інтеграцією базової освіти та більш гнучкої курсової підготовки. Одне з основних питань організації спеціалізованої підготовки фахівців у галузі інформаційних технологій для оперативних підрозділів полягає у визначенні раціонального співвідношення прикладних і технічних аспектів викладання. Така побудова навчального процесу з основним нахилом на практичне відпрацювання певних умінь і навичок, разом з викладанням інших дисциплін, зокрема: «Особливості розкриття кіберзлочинів», «Інформаційно-аналітична робота в оперативно розшуковій діяльності» тощо дає можливість підготувати сучасних правоохоронців, які зможуть адекватно протидіяти кіберзлочинам [1, с. 4-6].

Підготовка фахівців у галузі інформаційних технологій повинна здійснюватися на основі переліку компетентностей, які дають можливість випускнику закладів вищої освіти МВС виконувати службові обов'язки в різних підрозділах Національної поліції, зокрема: фахові компетентності у галузі інформаційних технологій:

- здатність здійснювати оцінку оперативної обстановки і прогнозування злочинності;
- здатність використовувати теоретичний та методичний інструментарій для обґрунтування управлінських рішень;
- здатність виявляти, запобігати і припиняти правопорушення у кіберпросторі;
- здатність використовувати теоретичний та методичний інструментарій для оперативно-розшукової ідентифікації, оперативно-розшукової діагностики, оперативно-розшукового прогнозування;
- здатність до пошуку, систематизації та аналізу інформації для вирішення професійних програм і наукових завдань;
- здатність застосовувати управлінські навички у сфері інформаційних технологій;
- здатність розробляти завдання для програмування інформаційних систем у сфері протидії злочинності;

- здатність вивчати, використовувати й адаптовувати міжнародні стандарти та нормативи у професійній сфері.

Майбутні фахівці в галузі інформаційних технологій мають знати:

- методи й прийоми отримання, систематизації й аналізу оперативно-розшукової, статистичної та іншої інформації для оцінки оперативної обстановки й прогнозування злочинності;
- прийоми та методи оперативного, тактичного й стратегічного аналізу при розслідуванні кримінальних правопорушень;
- методи, прийоми й інструменти використання оперативно-службової інформації для прийняття управлінських рішень;
- методи та засоби виявлення, запобігання й припинення правопорушень у кіберпросторі;
- основні види та методи оперативно-розшукової ідентифікації, оперативно-розшукової діагностики, оперативно-розшукового прогнозування;
- методи й прийоми комп'ютерної та аналітичної розвідки;
- особливості побудови та функціонування автоматизованих інформаційних систем Національної поліції України;
- основні програмно-технічні засоби, що використовуються при обробці та захисті інформації в діяльності органів Національної поліції України;
- міжнародне законодавство, стандарти й правила використання моделі поліцейської діяльності, керованої аналітикою (Intelligence-Led Policing/ILP);
- отримувати, систематизувати й аналізувати оперативно-розшукову, статистичну та іншу інформацію для оцінки оперативної обстановки й прогнозування злочинності;
- застосовувати прийоми та методи оперативного, тактичного й стратегічного аналізу при розслідуванні кримінальних правопорушень;
- застосовувати методи й прийоми використання оперативно-службової інформації для прийняття управлінських рішень;
- виявляти, запобігати й припиняти правопорушення у кіберпросторі;
- застосовувати набуті знання при використанні автоматизованих інформаційних систем Національної поліції України;
- використовувати сучасні програмно-технічні засоби для обробки та захисту інформації в діяльності органів Національної поліції України;
- вивчати, адаптувати та використовувати міжнародне законодавство, стандарти й правила використання моделі поліцейської діяльності, керованої аналітикою (Intelligence-Led Policing/ILP) в органах Національної поліції України [2 с. 305–307].

У сучасних умовах стрімкого розвитку інформаційних технологій навчальний процес у закладах вищої освіти МВС має гнучко та своєчасно реагувати на зміни в правовому полі. Це вимагає від відомчих закладів вищої освіти удосконалення змісту та методики навчання відповідно до реальних умов і завдань протидії злочинності та розвитку новітніх інформаційно-телекомунікаційних засобів. Крім того, працівники підрозділів кіберполіції та інформаційно-аналітичних відділів оперативних підрозділів Національної поліції мають бути як оперативниками, так і фахівцями з комп'ютерної техніки. Зважаючи на транснаціональний характер кіберзлочинів і специфіку інформаційного середовища в мережі Інтернет, такі фахівці повинні вільно володіти іноземними мовами, передусім англійською [3 с. 51–68].

Боротьба з комп'ютерною злочинністю і кібертероризмом є одним з найважливіших завдань сучасності. Успішність протидії в цьому напрямі багато в чому визначається якістю підготовки фахівців з інформаційної безпеки. Удосконалення навчально-виховної роботи створює передумови для запобігання і попередження комп'ютерної злочинності, особливо, в молодіжному середовищі.

Література:

1. Коваленко В.В. Реалії та перспективи реформування відомчої освіти й науки. *Науковий вісник* Національної академії внутрішніх справ. 2010. № 6.
2. Хахановський В.Г. Проблеми підготовки кадрів з протидії кіберзлочинності. *Митна справа*. 2017. № 2 (74). Ч. 2.
3. Кудінов В.А. Вирішення проблем добору та підготовки кадрівправоохоронців щодо протидії кіберзлочинності. *Кадровий вісник*. 2011. № 1.

Актуальні питання впровадження інформаційно-комунікативних технологій у навчально-виховний процес ЗВО з особливими умовами навчання у сфері протидії кіберзлочинності

Косаревська О.В.
провідний науковий співробітник відділу організації наукової роботи
Одеського державного університету внутрішніх справ
к. п. н., доцент

Одним із викликів XXI століття є вагоме зростання злочинів у сфері комп'ютерних технологій.

За статистикою Міжнародного союзу електрозв'язку, Україна за показником розвитку інформаційно-телекомунікаційних технологій займає 79 місце, що обумовлює актуальність проблеми протидії кіберзлочинності та забезпечення інформаційної безпеки.

Одним із ключових напрямків розвитку системи МВС України є модернізація відомчої освіти та оновлення стратегії управління інформаційними ресурсами за рахунок ефективного використання інформаційно-комунікативних технологій [1].

З огляду на це актуальною проблемою, на наш погляд, постає проблема удосконалення інформаційно-технічної підготовки майбутніх фахівців правоохоронної діяльності у ЗВО з особливими умовами навчання.

Аналіз сучасних наукових досліджень вітчизняних та зарубіжних авторів стосовно стратегічних напрямків розвитку інформаційно-комунікаційних технологій (далі ІКТ) у ЗВО: В.Ю. Биков, Р.С. Гуревич, О.Д. Данілова, П. Коммерс, В.П. Поляков, О.С. Товканець, Д.В. Чистов, М.А. Федотова та інші та наукової парадигми рівного доступу до якості освіти на основі сучасних ІКТ: О.Ю. Іохов, К.Ю. Ісмайлов, О.Є. Користін, О.В. Косаревська, О.О. Косиченко, О.М. Куракін, О.В. Придатко, Є.В. Рижов, В.В. Сеник, В.В. Тулупов, Г.М. Шорохова та інші, дає підстави наголосити на окремі аспекти удосконалення професійної інформаційно-технічної підготовки здобувачів вищої освіти з протидії кіберзлочинності.

Цифрові технології у професійній підготовці здобувачів вищої освіти в сучасних умовах інтенсивного розвитку інформаційно-комунікативного середовища та зростання кіберзлочинності в Україні і всьому світі набувають особливої актуальності та потребують виконання першочергових, на наш погляд, завдань.

По-перше, слід зазначити необхідність подальшої автоматизації та інформатизації освіти за рахунок створення спеціального віртуального освітнього середовища, що передбачає:

- забезпечення в необхідних обсягах новітнього комп'ютерного обладнання;
- облаштування інформаційних осередків для проведення аудиторних занять (інтерактивних аудиторій, лабораторій електронного управління, оснащення навчальних «робочих місць оперативного працівника НПУ», тошо).
- створення умов для організації «спеціального режиму» для проведення інформаційно-технічної підготовки та узгодження обсягу, змісту інформації, яка необхідна для навчальної взаємодії між суб'єктами та об'єктами освітнього процесу [3, с. 8].

По-друге, це впровадження новітніх педагогічних технологій й алгоритмів управління освітнім процесом, за рахунок:

- насичення дидактичних матеріалів об'єктивно – орієнтованими на правоохоронну діяльність програмними засобами по отриманню, зберіганню та передачі оперативної інформації в сфері протидії кіберзлочинності;
- розвитку комунікативних здібностей по веденню «інтерактивного діалогу» (технічна мова спілкування: ключові слова, обмеженість набору символів);
- створення відкритої платформи ІКТ, поширення електронного контенту, за рахунок впровадження «хмарних» педагогічних технологій, синергетичного міждисциплінарного середовища для зацікавлених осіб, комп'ютерна візуалізація навчальної інформації [4, с. 11] .

По-третє, значну роль у формуванні творчого мислення та підвищення рівня інформаційної культури для здобувачів вищої освіти, на нашу думку, відіграє організація у ЗВО умов для проведення експертно – дослідної роботи.

Так, наприклад, це створення на громадських засадах навчально-тренувального центру моніторингу кіберпростору (ХНУВС), постійно діючої (цілодобово) моніторингової групи курсантів в рамках роботи науково-дослідної лабораторії кримінального аналізу (ОДУВС) дає можливість розробляти наукові проекти в сфері протидії кіберзлочинності.

Також суттєвим внеском проведення науково-дослідної роботи здобувачів вищої освіти в рамках діяльності наукових гуртків кафедр інформаційно-технічного спрямування ЗВО з особливими умовами навчання, результати яких обговорюватимуться під час наукових заходів з проблем протидії кіберзлочинності: (інтернет конференції, круглі столи, наукові тематичні семінари, участь у міжнародних наукових проектах тощо) [5].

По-четверте, це зміцнення кадрового потенціалу ЗВО, за рахунок введення додаткових кваліфікаційних вимог до науково-педагогічного складу з викладання інформаційно – технічної спрямованості, наприклад, як:

- «Протидія кіберзлочинності»;
- «Кримінальний аналіз»;
- «Інформаційні технології»;
- «Інформаційне забезпечення професійної діяльності» тощо.

Обумовленість вимог стосовно наявності базової технічної освіти у поєднання з отриманням юридичної освіти, обов'язкового стажування у оперативних підрозділах НПУ з протидії кіберзлочинності, на наш погляд, буде сприяти впровадженню єдиного стандарту єдиного уніфікованого управління ІКТ на всіх рівнях освітньої системи [6].

На підставі вище зазначеного, ми дійшли висновку, що вимоги сьогодення у вихованні творчо – активного резерву майбутніх фахівців правоохоронної сфери передбачає широке використання засобів новітніх інформаційних технологій для реалізації ідей розвиваючого навчання, та формування особистості правоохоронця нової формації

Література:

1. Про схвалення Стратегії розвитку органів системи Міністерства внутрішніх справ на період до 2020 року: розпорядження Кабінету Міністрів України від 15.11.2017 №1023-р.// БД «Законодавство України» / ВР України. URL: http://zakon.rada.gov.ua./laws/show/1023-2017-%D1%80
2. В.П. Поляков, Д.В. Чистов «Развитие информационных образовательных технологий и формирование информационного пространства Финансового университета» [Електронный ресурс]. Доступно : http://old.fa.ru Дата доступа:10.02.2019.
3. Р.С. Гусевич «Інформаційне суспільство як важливий чинник розвитку освітнього середовища у ВНЗ», Сучасні інформаційні технології та інноваційні методики навчання у підготовці фахівців: методологія, теорія, досвід, проблеми, Київ – Вінниця, ТОВ фірма «Планер», 2015, Вип.43, с.8.
4. В.Ю. Биков Мобільний простір і мобільно орієнтоване середовище інтернет-користувача: особливості модельного подання та освітнього застосування. *Інформаційні технології в освіті*, № 17, с.9-36, 2013.
5. Підготовка поліцейських в умовах реформування системи МВС України, Харків. Нац., ун-т внутр. справ, каф. спец. фіз., підготовки ф-ту №2. Харків: ХНУВС, 2018. 246 с.
6. Кібербезпека в Україні: правові та організаційні питання: матеріали всеукр. наук. прак. конф., м.Одеса, 17 листопада 2017 р. Одеса: ОДУВС. 2017. 204 с.

Місце аналітиків в правоохоронній системі України

Радова М.Р.
курсант 302 навчального взводу
факультету підготовки фахівців для підрозділів кримінальної поліції
Одеського державного університету внутрішніх справ
рядовий поліції
Лісніченко Д.В.
старший науковий співробітник
науково-дослідної лабораторії з проблемних питань кримінального аналізу
Одеського державного університету внутрішніх справ

Актуальність теми роботи. В сучасних умовах формування правоохоронної діяльності держави неабикого значення набуває здійснення аналітичної роботи в правоохоронних органах. Вибір теми для написання даної роботи обумовлений значенням вивчення актуальних аспектів визначення місця аналітиків в правоохоронній системі. Крім того, сучасні умови розвитку суспільства характеризуються

значним збільшенням обсягу інформації, що визначає необхідність активного розвитку сфери інформаційно-аналітичної діяльності для забезпечення правопорядку в нових умовах.

Зазначимо, що діяльність правоохоронних органів не може здійснюватися поза тих змін, які відбуваються в соціумі, незважаючи на їх активну модернізацію та розбудову. Вона не в змозі повною мірою прогнозувати виклики і загрози кримінального світу, що вимагає розробки методів і методик розслідування злочинів на основі аналітичної діяльності та сучасних інформаційних технологій.

Звичайно, інформаційно-аналітична діяльність повинна бути ефективною, тобто сприяти безпосередньому розкриттю правопорушень у будь-якій сфері суспільного життя. Найбільш важливою змістовною характеристикою процесу управління є робота з інформацією - її збір, накопичення, систематизація, оцінка та перерозподіл. Відповіло до ст. 1. Закону України «Про інформацію» інформація - будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [2].

Однак ця функція має на увазі під собою не просто «механічний» збір суб'єктом управління інформації про стан керованої ним системи і оточуючого її зовнішнього середовища. Інформацію неправильно ототожнювати з усім обсягом надходження відомостей. Дані про об'єкт стають інформацією лише тоді, коли отримують зміст і форму, придатну для використання в процесі управління.

Таким чином, інформаційно-аналітична діяльність являє тобою динамічний процес аналізу суспільних відносин і виявлення потенційних вразливостей, які можуть стати об'єктом злочинного зазіхання.

Інформаційно-аналітична робота, будучи одним із напрямів підвищення ефективності діяльності правоохоронних органів, є невід'ємною складовою частиною управлінської діяльності на всіх рівнях їх функціонування. Разом з тим, інформація представляє цінність не сама по собі, а в якості бази проведення її аналізу, від якого залежить планування діяльності правоохоронних органів. Проведення робіт з планування і прогнозування в рамках великої і складної системи правоохоронних органів вимагає великого обсягу вихідних систематизованих даних і ретельної, копіткої роботи з проведення аналізу цих даних (встановлення взаємозв'язків, угруповання даних, підвищення їх достовірності).

При цьому інформаційно-аналітичне забезпечення правоохоронних органів являє собою самостійну систему, що характеризується певними принципами організації та управління, що має властиві їй функції і чітко сформульовані цілі розвитку як на найближчий, так і на перспективний періоди і складається в свою чергу з підсистем, між якими існують стійкі структурні зв'язки. Розгляд інформаційно-аналітичного забезпечення діяльності правоохоронних органів як системи визначає обґрунтованість використання системного підходу до її аналізу. Системний підхід до організаційних систем (систем, в яких присутній елемент організації і управління) базується на розгляді їх як планово-керованих, цілеспрямованих систем.

Надаючи аналітикам можливість опрацьовувати дані про порушення закону, працівники органів правопорядку отримують можливість використовувати готовий оперативно-аналітичний продукт, а не первинну інформацію. При цьому вони отримують такі переваги: по-перше, продукт окреслює конкретно тенденції злочинності не лише за географічною ознакою, а й у часових рамках; по-друге, у зв’язку з тим, що продукт надає можливість мати більше інформації щодо місць ймовірного скоєння злочинів, більше часу та зусиль можливо витратити на попередження скоєння злочинів; по-третє, оскільки час витрачається більш продуктивно, співробітники мають більше можливостей у наданні допомоги своїм колегам у разі потреби [3, с.61].

Найважливішою особливістю інформаційно-аналітичної роботи в діяльності правоохоронних органів є її міждисциплінарний характер, так як сам цей феномен знаходиться на стику цілого ряду наукових дисциплін. До їх числа можна віднести соціологію, політологію, інформаціологію, управлінську науку та інші галузі науки.

Крім того, інформаційно-аналітична діяльність дозволяє використовувати потенціал юридичних наук в процесі формування кримінально-правової політики держави з метою забезпечення громадської безпеки на основі використання даних криміналістики, кримінології, судової психіатрії, судової медицини і так далі, що дозволяють комплексно здійснювати боротьбу зі злочинністю.

Наразі міждисциплінарний характер інформаційно-аналітичної діяльності стає об'єктивно необхідним в процесі прийняття рішень та повинен відповідати принципам поваги прав і свобод людини і громадянина, законності, гуманізму, презумпції невинуватості.

Саме на обробку інформації і спрямована аналітична робота. Її призначення полягає, по-перше, у вивченні закономірностей практично всіх процесів і явищ суспільного життя, які тією чи іншою мірою впливають на діяльність органів внутрішніх справ, по-друге, у використанні здобутих відомостей і знань для забезпечення ефективності цієї діяльності [4, с.66].

Інформаційно-аналітична діяльність дозволяє не тільки збирати і обробляти інформацію, а й здійснювати на її основі ефективне забезпечення правопорядку, боротьбу зі злочинністю. Застосування інформації також стає все більш необхідним. У стратегічному і тактичному плані дані можуть бути використані для прийняття більш точних і виправданих рішень.

Вимоги до інформаційно-аналітичної діяльності повинні відповідати тим цілям і завданням, які зобов'язана виконувати правоохоронна система в цілому. Така діяльність повинна ґрунтуватися на повному, системному аналізі різнорідної інформації, яка має безпосереднє значення для оперативно-розшукової діяльності (ОРД) і дозволяє виявити напрямки розвитку кримінальних тенденцій у суспільстві. Розвиток інформаційних технологій дозволяє використовувати накопичену інформацію для виявлення взаємозв'язків між різними даними, що відносяться до конкретного виду злочину або злочинів. В результаті з'являється можливість більш точного аналізу криміногенної обстановки в певному територіальному сегменті та боротьби зі злочинністю в ньому [5, с.112].

В рамках вітчизняної правової системи розвиток інформаційно-аналітичної діяльності перебуває на недостатньо високому рівні, що пов'язано з відсутністю централізованого, структурованого підходу до її організації. Довгий час ця діяльність ґрунтувалася на теорії та методології криміналістики, але в даний час набуває все більш міждисциплінарного характеру. Важливість розвитку інформаційно-аналітичної діяльності правоохоронних органів полягає не тільки в підвищенні якості правоохоронної діяльності, а й підтримці стабільності в суспільстві, створення законних умов для його всебічного розвитку.

Отже, інформаційно-аналітичне забезпечення організаційно входить до системи управління системою правоохоронних органів, забезпечуючи у своїй діяльності досягнення завдань і цілей створення останньої. Аналітична робота є невід'ємною і найважливішою складовою частиною управлінської діяльності і виступає не якимось епізодичним, короткочасним актом, що виконує спеціально призначений працівник, а функцією усіх ланок системи, здійснюється постійно.

Аналітична робота – це безперервний процес вивчення управлінської та іншої інформації. Аналітична робота служить засобом виявлення і оцінки значущості виникаючих перед конкретною системою проблем, формулювання її цілей, визначення об'єктивно необхідних функцій, обґрунтування структури та підвищення ефективності діяльності по виконанню поставлених завдань. Навіть, якщо цілі органу визначені вищестоящою системою управління, то і в цьому разі аналітична робота забезпечує: виявлення часткових проблемних ситуацій; висунення та з'ясування конкретних проміжних цілей управління; вибір основних напрямів діяльності; визначення та оцінку окремих дій по досягненню намічених цілей.

Література

1. Конституція України, прийнята на п'ятій сесії Верховної Ради України 28.12.1996. Відомості Верховної Ради України. 1996. № 30. С. 141.
2. Про інформацію: Закон України від 2 жовтня 1992 року. Відомості Верховної Ради України. 1992. № 48. Ст. 650.
3. Заєць О.М. Імплементація методів аналітичної діяльності в діяльність органів правопорядку України в умовах інтегрування до Європейського співтовариства. О.М. Заєць. Інформаційно-аналітичне забезпечення діяльності підрозділів кримінальної поліції : збірник наукових статей за матеріалами доповідей Всеукраїнської науково-практичного семінару 23 березня 2018 року. Львів: ЛьвДУВС, 2018. С. 60-64.
4. Моргунов О.А. Сутність та особливості інформаційно-аналітичної роботи в органах внутрішніх справ. О.А. Моргунов. Науковий вісник Ужгородського національного університету, 2014. Серія ПРАВО. Випуск 27. Том 2. С. 65-68.
5. Судові та правоохоронні органи України: навч. посіб. М.В. Ковалів, С.С. Єсімов, Ю.С. Назар, М.Т. Гаврильців, Г.Ю. Лук'янова; Львів. держ. ун-т внутр. справ. Львів: ЛьвДУВС, 2016. 386 с.

Психологічні особливості осіб, які вчиняють злочини у сфері високих технологій

Форос Г.В.
професор кафедри кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішніх справ, к.ю.н., доцент

На сьогодні кіберзлочинність – це реальна глобальна загроза, яка може походити з будь-якої країни світу і виходити за межі конкретної юрисдикції на відміну від багатьох інших традиційних злочинів. Обумовлено це тим, що інформаційно-телекомунікаційні системи все більше впливають на

сучасне суспільство. І такі терміни як: «хакери», «комп'ютерні віруси», «кіберзлочинність» все частіше зустрічаються не тільки в повсякденному, але й в роботі юриста. Окремі аспекти проблеми протидії кіберзлочинності, вже розглядаються в правовому та організаційному аспектах, але лише окремі її питання висвітлювались у монографіях, наукових збірниках, навчально-методичних посібниках як вітчизняних, так і зарубіжних науковців, наприклад в роботах Д.П. Біленчука, В.В. Вертузаєва, В.Б. Вєхова, О.Г. Волеводза, В.Д. Гавловського, В.М. Гуцалюка, В.В. Голубєва, А.М. Жодзишського, К.Ю. Ісмайлова, Р.А. Калюжного, В.В. Крилова, Б.А. Кормича, М.І. Панова, В.В. Пивоварова, Л.К. Терещенка та багатьох інших.

Проблема організації попередження кіберзлочинів пов'язана з певними соціальними групами, індивідами, особистостями та життєвими ситуаціями, до яких вони потрапляють. Характеризуючи особу злочинця, кримінологи традиційно класифікують чотири групи ознак: соціально-демографічні; кримінально-правові; статусно-рольові; морально-психологічні.

Для розгляду соціально-демографічної характеристики можна звернутися до статистики:

Кримінологічні дослідження, проведені Іванченком О.Ю., показують, що переважно кіберзлочини вчиняють чоловіки (близько 87,5%). Це зумовлено тим, що на чоловіків припадає більша кількість технічних спеціальностей, ніж на жінок. Проте в наш час питома вага жінок-кіберзлочинців зростає, що обґрунтовується підвищенням інтересу жінок до сучасних інформаційних технологій [1, с. 174].

Кримінологами виділяються такі вікові групи кіберзлочинців: від 16 до 17 років, від 18 до 28, від 29 до 39, від 40 до 54, та особи віком від 55 і старше. За статистикою Генеральної прокуратури України в 2017 році всього було виявлено 472 особи, які вчинили кіберзлочини. 187 з них віком від 16 до 17 років було 8 осіб (менше 2 %), віком 18-39 років - 184 особи (39 %), 29-39 років - 185 осіб (39,2 %), 44-54 роки — 93 особи (19,7 %), 55 років і старше - 8 осіб (менше 2%) [2].

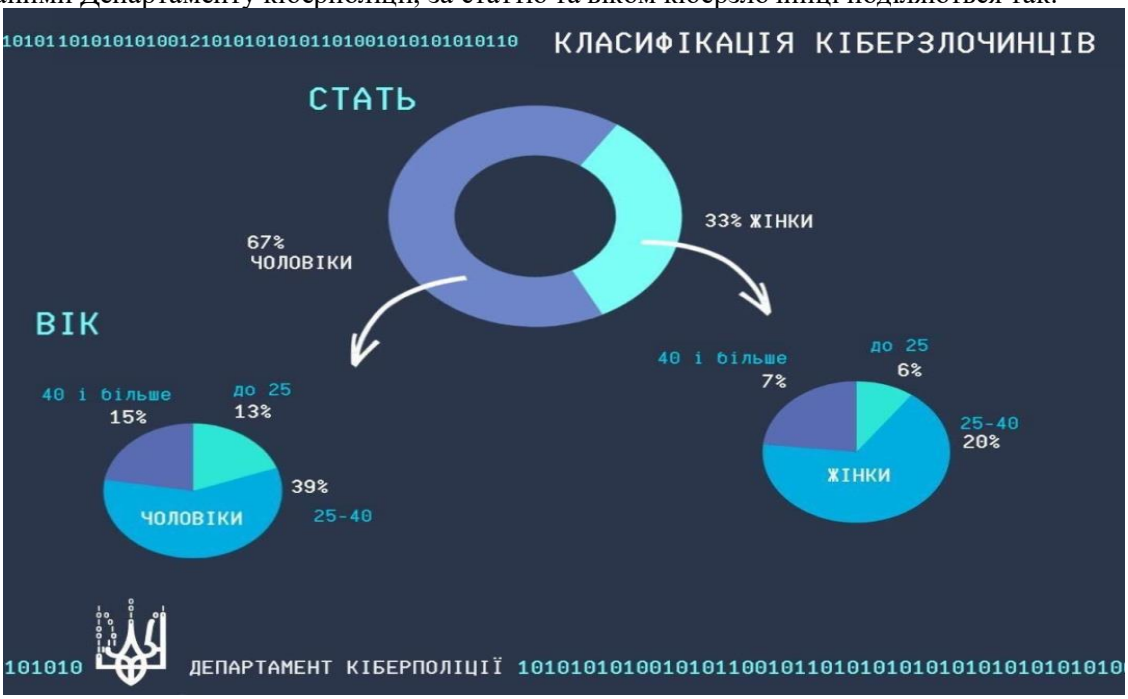
Щодо сімейного стану злочинців, то 58% кіберзлочинців були неодруженими, 16 % - розлучені, 26 % - одружені. Такі дані зумовлені тим, що більшість кіберзлочинців є особами молодого віку, які ще не створили сім'ї.

Переважна більшість кіберзлочинців, мають повну вищу освіту - 65,3 % (308 осіб), професійно-технічну освіту - 10,3 % (49 осіб), повну загальну середню освіту - 24,4 % (115 осіб). Наявність повної вищої освіти та професійно-технічної освіти в кіберзлочинця пояснюється специфікою використання комп'ютерної техніки [2].

За ознакою зайнятості кіберзлочини вчиняють працездатні особи - 55 % (259 осіб), ті, хто ніде не працює і не навчається - 36,6% (173 особи), та безробітні - 8,4 % (40 осіб) [2].

Однак, зазначені статистичні дані стосуються лише виявлених злочинів, оскільки цей вид злочинності характеризується високим рівнем латентності, ми не можемо стверджувати, що ці дані відображують реальні масштаби проблеми.

За даними Департаменту кіберполіції, за статтю та віком кіберзлочинці поділяються так:



З ознак, що складають кримінально-правову характеристику розглянемо дані про судимість, види злочинів, що як правило, вчиняються разом із кіберзлочинністю та утворюють сукупність.

За даними Державної судової адміністрації України, серед осіб, засуджених за вчинення кіберзлочинів 5,1% раніше вчиняли злочини. Однак, кримінально-правовий рецидив не утворювався, оскільки особи були звільнені від кримінальної відповідальності(0,5%), визнані такими, що не мають судимості були 1,9%, судимість була погашена або знята у 2,7% випадків. Водночас 5,8% осіб засуджених мають не зняту і не погашену судимість.

За статистичними даними майже кожен п'ятий злочин у сфері високих технологій було вчинено у сукупності з іншими злочинами, а саме: проти власності – 22%; у сфері службової діяльності та професійної діяльності, пов'язаної з наданням публічних послуг – 8%; проти авторитету органів державної влади, органів місцевого самоврядування та об'єднань громадян – 6%; у сфері господарської діяльності – 5,3%; проти виборчих, трудових та інших особистих прав і свобод людини і громадянина – 3,3%; проти громадського порядку та моральності – 0,6%.

Можна виділити відмінні психологічні риси особистості злочинця:

- Незадоволеність, не комфортність
- Інше, чим у законослухняних громадян відношення до суспільних цінностей, вони вирішують виникаючі перед ними життєві завдання іншими способами
- Ослаблена емоційність у відношенні до навколишніх, звужене коло стимулів, що мають значення для інших осіб
- Украй перекручене уявлення про суспільство проектуючи на навколишніх свої почуття й спонукання, злочинці вважають себе незрозумілими, відчуженими
- Тенденції до ризик, сильним відчуттям, прагненням до реалізації своїх потреб
- Імпульсивні, агресивні, погано контрольовані, не враховують свої помилки, не бояться покарань
- Зневажають морально-етичними, правовими нормами, звичаями, установленими правилами
- Завищена самооцінка викликана почуттям несправедливості

Отже, судово-психологічна класифікація розрізняє три типи злочинців: асоціальний (менше злісний); антисоціальний (злісний) і тип особистості злочинця, що характеризується дефектами психічної саморегуляції (випадковий). У всіх злочинах у сфері використання електронно-обчислюваних машин(комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку суб'єктивна сторона характеризується умислом, отже третій тип не може характеризувати осіб, які вчиняють злочини у сфері високих технологій. Тобто за ступенем соціальної дезадаптації, а саме за таким критерієм щойно були поділено злочинців, злочинці в сфері високих технологій можуть мати асоціальний тип(найчастіше це особи, які вперше вчинили злочин на основі загальної асоціальної спрямованості) та антисоціальний тип(особи, які неодноразово вчиняли злочини на основі стійкої антисоціальної спрямованості).

Література:

1. Іванченко О.Ю. Кримінологічна характеристика кіберзлочинності, запобігання кіберзлочинності на національному рівні *Актуальні проблеми вітчизняної юриспруденції,* — К.: № 2016. — С. 172-177
2. Статистичні дані Генеральної прокуратури України / / Офіційний сайт Генеральної прокуратури України [Електронний ресурс]. — Режим доступу: https://www.gp.gov.ua/ua/stst2011
3. Статистичні дані Державної судової адміністрації України / / Офіційний сайт Державної судової адміністрації України [Електронний ресурс]. — Режим доступу: https://dsa.court.gov.ua/dsa/
4. В Україні зростає кількість кіберзлочинів https://www.epravda.com.ua/news/2016/03/28/587044/
5. Кримінологія: підручник / В. В. Голіна, Б. М. Головкін, М. Ю. Валуйська та ін.; за ред. В. В. Голіни, Б. М. Головкіна. — Х.: Право, 2014. — 440 с.
6. Кіберзлочинність: реальна боротьба у віртуальному світі [Електронний ресурс]. – Режим доступу : http://www.imzak.org.ua/articles/article/id/853.

СЕКЦІЯ 5
ІНФОРМАЦІЙНО-АНАЛІТИЧНА ДІЯЛЬНІСТЬ ПРАВООХОРОННИХ ОРГАНІВ У БОРОТЬБІ ЗІ ЗЛОЧИННІСТЮ

Деякі проблеми взаємодії слідчого з оперативними та інформаційно-аналітичними підрозділами Національної поліції України

Мельнікова О.О.
викладач кафедри кібербезпеки
та інформаційного забезпечення ОДУВС
кандидат юридичних наук
Шаран А.А.
курсант 4 курсу факультету
підготовки фахівців для органів
досудового розслідування

Розкриття і ефективне розслідування злочинів в повній мірі залежать від узгодженості дій різних служб і підрозділів поліції. Це проявляється в першу чергу у взаємодії слідчого з підрозділами, які проводять оперативно-розшукову діяльність. Для ефективного розслідування злочинних посягань у сфері кібербезпеки необхідна чітка співпраця всіх суб'єктів, причетних до досудового розслідування.

Слідчий під час розслідування злочину не в силах самостійно виконати всі завдання, необхідні для повного і всебічного розгляду справи, тому йому об'єктивно доводиться звертатися за допомогою до інших органів, які в силу своїх повноважень надають слідчому допомогу в розкритті та розслідуванні злочинів або виступають в якості самостійних суб'єктів пізнання події злочину, які координують свої дії зі слідчим.

Організація досудового розслідування означає: своєчасне розроблення узгодженого плану заходів; налагодження належної взаємодії в процесі розслідування між слідчим, співробітниками оперативних підрозділів, спеціалістами; забезпечення кваліфікованого керівництва слідчо-оперативною групою; проведення регулярних нарад; налагодження систематичного обміну інформацією та звітністю групи тощо

Важливого значення взаємодія між слідчим та оперативними працівниками та працівниками інформаційно-аналітичного забезпечення набуває у разі розкриття злочинів в сфері інформаційних технологій.

Майже всі департаменти кримінального блоку Національної поліції України у своїй структурі мають аналітичні відділи, або працівників, які виконують завдання у сфері аналізу. Водночас жоден з аналітичних підрозділів не створює аналітичні продукти відповідно до європейських стандартів. Крім того, відсутня належна взаємодія між департаментами щодо обміну аналітичною інформацією.

У системі Національної поліції існує багато джерел розрізненої інформації, яка аналізується співробітниками різних служб автономно. Наприклад, у Департаменті протидії наркозлочинності аналізується інформація, пов'язана з наркозлочинами, у Департаменті карного розшуку – інформація щодо загальнокримінальної злочинності тощо. Крім того, кожний оперативний працівник накопичує і зберігає власну оперативну інформацію, яка після його звільнення або переміщення по службі стає практично недоступною для інших оперативних працівників.

Держава витрачає кошти на отримання інформації, а в результаті ця інформація втрачається. При цьому порушується європейський принцип про те, що інформація не належить конкретному поліцейському, інформація належить державі як один із продуктів діяльності поліції. Тому постає задача консолідації всієї оперативної інформації, її подальшого аналізу, що має сприяти розкриттю насамперед тяжких та особливо тяжких злочинів. Більшість департаментів в оперативно-службовій діяльності використовує такі джерела інформації, як Інтегровану інформаційно-пошукову систему Національної поліції та статистичну інформацію, надану Департаментом інформаційно-аналітичної підтримки.

З метою профілактики і оперативного реагування на злочини аналітики Управління кримінального аналізу запроваджують географічну прив'язку до кожного житлового будинку, з можливістю нанесення інформації на карту. Це дасть можливість здійснювати якісний аналіз скоєних правопорушень, визначати зони вчинення злочинів, скеровувати в такі місця додаткові наряди патрульної поліції та ставити завдання дільничному офіцеру поліції щодо повторного відпрацювання місць проживання осіб, які перебувають під адміністративним наглядом.

В Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні, затвердженої Наказом МВС України від 07.07.2017 р. № 575, до організаційної форми взаємодії зараховано:

1) організація взаємодії при надходженні до органу, підрозділу поліції заяв і повідомлень про кримінальні правопорушення та реагуванні на них;

2) організація взаємодії при направленні оперативним підрозділом матеріалів за результатами оперативно-розшукової діяльності до органу досудового розслідування;

3) створення та організація роботи слідчо-оперативних груп під час досудового розслідування кримінальних правопорушень;

4) виконання працівниками оперативного підрозділу органу, підрозділу поліції доручень слідчих про проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій;

5) організація взаємодії під час проведення окремих слідчих (розшукових) дій та виконання заходів забезпечення кримінального провадження;

6) забезпечення взаємодії при зупиненні досудового розслідування [1].

З урахуванням викладеного, доцільно зупинися більш детально на особливостях взаємодії слідчого з оперативними працівниками під час проведення негласних слідчих (розшукових) дій.

Взаємодія слідчого та співробітника оперативного підрозділу при проведенні НСРД сьогодні регламентується положеннями КПК України (ч. 6 ст. 246 КПК України) [2] та іншими підзаконними актами.

Відповідно до норм КПК України негласні слідчі (розшукові) дії має право проводити слідчий, який здійснює досудове розслідування злочину, або за його дорученням – уповноважені оперативні підрозділи Національної поліції, органів безпеки, Національного антикорупційного бюро України, Державного бюро розслідувань, органів, що здійснюють контроль за додержанням податкового і митного законодавства, органів Державної кримінально-виконавчої служби України, органів Державної прикордонної служби України (ч. 6 ст. 246 КПК України). Своєю чергою, під час виконання доручень слідчого, прокурора співробітник оперативного підрозділу користується повноваженнями слідчого та не має права здійснювати процесуальні дії у кримінальному провадженні за власною ініціативою або звертатися з клопотаннями до слідчого судді чи прокурора (ч. 2, 3 ст. 41) [3]. За цих умов, наприклад, керівник органу досудового розслідування, вважаючи, що по конкретному кримінальному провадженні доцільно провести НСРД, надає письмову вказівку слідчому щодо прийняття рішення про її проведення та доручення співробітнику оперативного підрозділу, який зобов'язаний її виконати. При цьому, дієвим засобом є надання вказівки слідчому на проведення НСРД та співробітнику оперативного підрозділу здійснювати одночасне забезпечення їх виконання.

При виїзді на місце події співробітник оперативного підрозділу негайно інформує слідчого про одержані дані щодо обставин вчинення кримінального правопорушення та осіб, які його вчинили, для їх подальшої фіксації шляхом проведення слідчих або негласних слідчих (розшукових) дій [1]. Поряд з цим, на жаль, законодавець (у т.ч це питання не врегульовано у відомчих нормативних актах) не визначив яким чином у такому випадку можуть невідкладно проводитися НСРД, а також слідчі (розшукові) дії. Адже окрім, огляду місця події до відкриття кримінального провадження заборонено проводити будь-які процесуальні дії. Поміж тим, співробітник оперативного підрозділу має право в межах ОРД здобути первинні оперативні дані, які в подальшому можуть бути використані при прийнятті рішень про проведення НСРД;

Працівники оперативного підрозділу, включені до складу СОГ, самостійно надають слідчому обґрунтовані пропозиції щодо необхідності проведення конкретних негласних слідчих (розшукових) дій. Дана умова, в обов'язковому порядку, передбачає щомісячне за участі керівника органу досудового розслідування заслуховування членів СОГ про результати роботи з розкриття і розслідування конкретних кримінальних правопорушень, виконання плану слідчих і негласних слідчих (розшукових) дій, а також надання практичної допомоги в їх проведенні [1]. При цьому, передбачена спрощена процедура взаємодії слідчого та співробітника оперативного підрозділу за якої здійснюється спільне планування НСРД, а також співробітник оперативного підрозділу уповноважений інформувати безпосередньо слідчого про доцільність проведення окремих НСРД.

Важливе значення має, з точки зору створення дієвого механізму реалізації слідчим права на проведення НСРД, можливість надання ним доручення уповноваженим оперативним підрозділам. Так, під час досудового розслідування кримінальних правопорушень слідчий має право надавати уповноваженим оперативним підрозділам письмові доручення про проведення негласних слідчих (розшукових) дій. У разі створення СОГ слідчий дає доручення про проведення НСРД працівникам оперативного підрозділу, включеним до її складу [4]. На жаль, керівник ОДР не має права надавати

вказівки чи доручення оперативному підрозділу, натомість ним здійснюється контроль за своєчасністю виконання доручень співробітником оперативного підрозділу.

Отже, з урахуванням вищенаведеного, керівник органу досудового розслідування при організації проведення НСРД організовує роботу слідчого під час прийняття рішення, проведення НСРД; сприяє налагодженню взаємодії слідчого з іншими уповноваженими суб'єктами щодо даного напряму діяльності, але для організації керівником органу досудового розслідування ефективної взаємодії слідчого та співробітника оперативного підрозділу необхідно надати повноваження керівнику щодо прийняття рішення про проведення НСРД та залучення до їх проведення уповноваженого оперативного підрозділу.

Таким чином, розслідування злочинів, що вчиняються у сфері використання електронно-обчислюваних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'зку, ставить перед слідчим різнорівневі завдання, для вирішення яких недостатньо виконання окремих слідчих дій. Це насамперед пов'язано із значним обсягом роботи, наявністю спеціальних знань у сфері інформаційних електронних технологій, специфічністю умов розслідування, які передбачають залучення широкого кола спеціалістів та проведенням великого обсягу судових експертиз і комплексів слідчих (розшукових) дій. Найбільшої ефективності в цьому можна досягти тільки за умови об'єднання зусиль слідчих та оперативних підрозділів, використання досвіду і допомоги правоохоронних органів інших країн.

Література:

1. Інструкція з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні затвердженої Наказом МВС України від 07.07.2017 р. № 575. URL:http://zaNon3.rada.gov.ua/laws/show/z0937-17
2. Кримінальний процесуальний кодекс України : від 13.04.2012 № 4651–VI. URL: http://zakon0.rada.gov.ua/laws/show/4651-17.
3. Кримінальний процесуальний кодекс України: наук.-практ. коментар / за заг. ред. професорів В.Г. Гончаренка, В.Т. Нора, М.Є. Шумила. К.: Юстініан, 2012. 1224 с.
4. Сало О. М. Організація взаємодії слідчого та оперативного підрозділу при проведенні негласних слідчих (розшукових) дій. Південноукраїнський часопис Одеського Державного університету внутрішніх справ. 2013. С. 67–72.

Звуколокація безпілотних літальних апаратів в задачах попередження терористичних погроз

Орлов В. В.
доцент провідних наук.
Військова академія (м. Одеса), к.т.н.

Стрімкий розвиток безпілотних літальних апаратів (БПЛА) створює загрози для об'єктів особливої важливості від неконтрольованого застосування рухливих робототехнічних систем. Несвоєчасне виявлення терористичних загроз від БПЛА, наприклад в Сирії і Саудівської Аравії, призводить до великих втрат людських життів і катастрофічних збитків нафтових компаній.

Для забезпечення кібербезпеки об'єктів застосовується комплексування інформаційних технічних систем, заснованих на різних фізичних принципах: радіолокації, гидролокациі, сейсмолокациі, охоронної сигналізації, контролю і управління доступом; телевізійного спостереження; охоронного освітлення в різних спектральних діапазонах; зв'язку та оповіщення. При цьому має місце низька ефективність виявлення малих БПЛА. Вони невидимі для радарів, внаслідок малої поверхні, що відбиває і низьку висоту польоту. Відеозасоби моніторингу також малоефективні внаслідок апріорної невизначеності щодо направлення і часу появи БПЛА. Перспективним напрямком є застосування пасивних систем звуколокациі, захищених від засобів радіоелектронної боротьби.

В даний час детально вивчені записи акустичних сигналів, визначені спектральні характеристики ряду БПЛА, дронів і літаків, які показали принципові можливості локації і розпізнавання літальних апаратів. Розроблено програмне забезпечення призначене для вибору конфігурації системи в залежності від вимог, що пред'являються до розміру зони контролю і точності визначення координат. Встановлено, що для контрольованої зони 500 метрів помилка визначення координат швидкісних цілей може досягати до 10 метрів, а малорухомих цілей - приблизно в 2 рази менше. Цього достатньо для подальшого супроводу БПЛА засобами відеомоніторингу.

Одеський державний університет внутрішніх справ
«Кібербезпека в Україні: правові та організаційні питання»

Кібербезпека – важливий напрям діяльності органів державної влади щодо захисту суспільства

Котко А.О.
курсант 3 курсу 302 навчального взводу
Херсонського факультету
Одеського державного університету внутрішніх справ
рядовий поліції
Кузьменко Ю.В.
професор кафедри адміністративного права
та адміністративного процесу
Херсонського факультету
Одеського державного університету внутрішніх справ
д.п.н., доцент

Актуальність проблеми кібербезпеки в нашому суспільстві підтверджується широким колом правопорушень в системі використання обладнання, комп'ютерних програм, інформаційно-комунікаційних технологій особливо в банківській сфері, сфері захисту інтелектуальних прав, економічної безпеки, національної безпеки тощо. Політика України спрямована на вирішення даних проблем в суспільстві. Зокрема важливим кроком є розробка законопроекту № 2163-VIII від 05.10.2017 р. «Про основні засади забезпечення кібербезпеки України». Проте, варто відмітити, що заходи з протидії викликам і загрозам у зазначеній сфері перебувають на початковому етапі та не мають комплексного характеру. Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки [1].

Мета статті – висвітлити кібербезпеку як сучасний і важливий напрям діяльності органів державної влади у сфері захисту суспільства.

Кібербезпека – це процес застосування заходів безпеки з метою забезпечення конфіденційності, цілісності та доступності даних. Кібербезпека забезпечує захист ресурсів (інформація, комп'ютери, сервери, підприємства, приватні особи). Кібербезпека покликана захистити дані на етапі їх обміну та збереження. До таких заходів безпеки входять контроль доступу, навчання, аудит та оцінка ризиків, тестування, управління та безпека авторизації.

Спеціаліст з кібербезпеки займається розробкою охоронних систем для різних комунікаційних мереж і електронних баз даних, тестує і вдосконалює власні та сторонні розробки для уникнення ризиків витоку відомостей, що становлять державну або комерційну таємницю, конфіденційну інформацію. Дана професія є порівняно молодою й отримала широке розповсюдження у зв'язку із впровадженням комп'ютерних та мережевих технологій практично в усіх організаціях – від невеликих комерційних фірм до органів держбезпеки.

Створення безпечних комп'ютерних систем і додатків є метою діяльності мережевих інженерів і програмістів, а також предметом теоретичного дослідження як у галузі телекомунікацій та інформатики, так і економіки. У зв'язку із складністю і трудомісткістю більшості процесів і методів захисту цифрового обладнання, інформації та комп'ютерних систем від ненавмисного чи несанкціонованого доступу вразливості комп'ютерних систем становлять значну проблему для їхніх користувачів.

Кібербезпека – це безпека IT систем (обладнання та програм). О. Манжай вважає, що «кіберпростір – це інформаційний простір, який існує за допомогою комп'ютерних систем при взаємодії людей між собою, взаємодії комп'ютерних систем та управлінні людьми цими комп'ютерними системами» [3, с. 145].

Аналіз наукового дискурсу вітчизняних вчених щодо визначення поняття «кібербезпека» дає підстави стверджувати про те, що остаточного поняття не вироблено. Тому наведемо приклади таких визначень, які на нашу думку найбільш повно висвітлюють це поняття.

О. Баранов дає визначення: «кібербезпека – це такий стан захищеності життєво важливих інтересів особистості, суспільства і держави в умовах використання комп'ютерних систем та/або телекомунікаційних мереж, за якого мінімізується завдання їм шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки

функціонування інформаційних технологій; несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації [4].

В. Фурашев визначає кібербезпеку як стан здібності людини, суспільства і держави щодо запобігання та уникнення спрямованого, в перше чергу – несвідомого, негативного впливу інформації [5].

З урахуванням того, що проблема кібезпезпеки носить глобальний характер, цікавою видається позиція міжнародних організацій. Так, International Telecommunication Union (Міжнародний телекомунікаційний союз) у своїй Рекомендації дає таке визначення: кібербезпека – це набір засобів, стратегії, принципи забезпечення безпеки, гарантії безпеки, підходи до управління ризиками, дії, професійна підготовка, практичний досвід, страхування та технології, які можуть бути використання для захисту кіберсередовища, ресурсів організації та користувача [2].

Все більше науковців зосереджують увагу на питанні кібермогутності держави як здатності втілювати її волю та забезпечувати національні інтереси в кіберпросторі.

В даний час для України питання кібербезпеки, нарощування потенціалу кібермогутності стоять на порядку денному. Україні необхідно самостійно шукати шляхи і механізми забезпечення кібербезпеки від сучасних загроз, які постають перед нею. Слушно врахувати думку Д. Дубова, який вважає, що кіберзагрози Українській державі та суспільству умовно можна розділити на два ключових рівні. Перший – «класичні» кіберзлочини – як абсолютно оригінальні, так і вже звичні для нас, для своєї реалізації вони потребують лише сучасних інформаційних технологій. Другий – злочини, характерні для геополітичної боротьби: кібершпигунство та кібердиверсії [6, с. 210].

Звертаючись до закону України «Про основні засади забезпечення кібербезпеки України» відмітимо, що цей закон спрямовано на формування загальної державної політики кібербезпеки, а також розподіл функцій між різними відомствами. Зокрема, він дає повноваження спецслужбам для здійснення кіберзахисту країни. За законом, координувати дії в сфері кібербезпеки буде Президент через Раду національної безпеки та оборони (РНБО). Також передбачено створення Національної системи кібербезпеки, яка об'єднає низку міністерств та відомств. До неї увійдуть Держслужба спеціального зв'язку та захисту інформації, Національна поліція, Служба безпеки України, Міністерство оборони і Генеральний штаб, Національний банк, а також розвідувальні органи. Закон чітко визначає, яке відомство і за що буде відповідати в сфері кіберзахисту. Координація та здійснення державної політики стають відповідальністю Держспецзв'язку. Нацполіція повинна буде забезпечувати захист громадян, суспільства і держави в кіберпросторі, а також вживати заходів для запобігання кіберзлочинності. Серед завдань СБУ – розслідування кіберінцидентів та кібератак, здійснених проти державних інфосистем. При цьому Міноборони і Генштаб мають готувати державу «до відбиття військової агресії в кіберпросторі». Нацбанк є відповідальним за кібербезпеку в банківській сфері, зокрема, шляхом створення центру кіберзахисту НБУ. До того ж, в Україні буде створено Національну телекомунікаційну мережу, до якої увійдуть інформаційні системи бюджетної сфери (органи державної влади та держпідприємства). Порядок її формування покладено на уряд. За захищений доступ держорганів, антивірусний захист і аудит інформаційної безпеки відповідатиме Державний центр кіберзахисту [1].

Слід, розглянути більш детально функції та повноваження органів державної влади у сфері кіберзахисту:

– Державна служба спеціального зв'язку та захисту інформації України забезпечуватиме кіберзахист об'єктів критичної інформаційної інфраструктури; координуватиме діяльність інших суб'єктів кібербезпеки; забезпечуватиме створення та функціонування національної телекомунікаційної мережі; запобігатиме, виявлятиме та реагуватиме на кіберінциденти і кібератаки та усуватиме їх наслідки; інформуватиме про кіберзагрози та методи захисту від них; забезпечуватиме аудит інформаційної безпеки на об'єктах критичної інфраструктури, встановлюватиме вимоги до аудиторів інформаційної безпеки, визначатиме порядок їх атестації та переатестації. За Держспецзв'язку залишається контроль дотримання законодавства у сфері захисту інформації, проведення державної інспекції в цій сфері відповідно до Закону про захист інформації в інформаційно-телекомунікаційних системах, який діє на сьогодні. Вказаний законопроект також передбачає створення Державного центру кіберзахисту.

– підпорядкована Держспецзв'язку Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA здійснюватиме аналіз даних про кіберінциденти та вестиме їх реєстр; допомагатиме запобігати, виявляти та усувати наслідки кіберінцидентів; організовуватиме та проводитиме семінари з кіберзахисту; готуватиме та розміщуватиме на своєму веб-сайті рекомендації щодо протидії кібератакам та кіберзагрозам; опрацьовуватиме інформацію про кіберінциденти; сприятиме державним органам, органам місцевого самоврядування, військовим формуванням, підприємствам, установам та

організаціям, незалежно від форми власності, а також громадянам України у вирішенні питань кіберзахисту та протидії кіберзагрозам. Для цих цілей, як планує законодавець, CERT-UA взаємодіятиме з правоохоронними органами, своєчасно інформуючи їх про кібератаки; з іноземними та міжнародними організаціями з питань реагування на кіберінциденти; з українськими командами реагування на комп'ютерні надзвичайні події, а також іншими суб'єктами, незалежно від форми власності, які здійснюють діяльність із забезпечення безпеки кіберпростору.

– на Національну поліцію України буде покладено відповідальність за запобігання, виявлення, припинення та розкриття кіберзлочинів.

– Міністерство оборони України та Генеральний штаб Збройних Сил України забезпечуватимуть кібероборону військових об'єктів, кіберзахист об'єктів критичної інфраструктури під час війни та надзвичайного стану, а також відбиватимуть воєнну агресію в кіберпросторі.

– Служба безпеки України в межах своїх повноважень запобігатиме, виявлятиме, припинятиме та розкриватиме злочини проти миру та безпеки людства у кіберпросторі, боротиметься з кібертероризмом і кібершпигунством. Також СБУ буде надано повноваження проводити таємні перевірки об'єктів критичної інфраструктури.

– Національний банк України визначається законопроектом як регулятор з кібербезпеки в банківській сфері. Для цього він матиме право на встановлення в цій сфері власних стандартів та організацію перевірки їх дотримання.

У висновку слід зазначити, що нині питання забезпечення кібербезпеки є вкрай важливим для України. У сьогоднішній ситуації наша держава є об’єктом кіберагресії. Україні необхідно розбудовувати не тільки оборонні спроможності у кіберпросторі, а й наступальні.

Підводячи підсумок, відмітимо, що загалом, не зважаючи на певну роздробленість, законодавство у сфері кібербезпеки України в останні роки було переглянуто і трансформовано відповідно до нових викликів та загроз. Це дає підстави вважати, що законодавча база у поєднанні із реструктуризацією системи національної безпеки дозволять створити потужний механізм стримування зовнішньої кіберагресії. На нашу думку кібербезпека – це захищеність від наявних та потенційно небезпечних проявів інформаційних загроз для нормального функціонування інформаційних систем, а також комплекс заходів та засобів, що спрямовані на захист комп’ютерів, обчислювальних мереж від несанкціонованого доступу та інших дій, пов’язаних з крадіжкою, блокуванням, пошкодженням, руйнуванням та знищенням як випадкового, так і цілеспрямованого впливу.

Література:

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/card/2163-19
2. Рекомендація МСЕ-Т X.1205. Огляд кібербезпеки. Женева: МСЕ, 2009. 55 с.
3. Манжай О.В. Використання кіберпростору в оперативно-розшуковій діяльності. *Право і безпека*. 2009. №4. С. 142–149.
4. Баранов О. Про тлумачення та визначення поняття «кібербезпека». *Інформація і право*. 2014. № 2 (42). С. 54–62.
5. Фурашев В.М. Кібезпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. *Інформація і право*. 2012. № 2. С. 162–169.
6. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва: монографія. Київ: НІСД, 2014. 328 с.

Інформаційне суспільство в Україні

Ігнатушко Ю.І.
старший викладач кафедри інформаційних
технологій та кібербезпеки
Національної академії внутрішніх справ
к. ю. н.

У сучасному світі знання та інформація породжують нові знання, їхні обсяги мають суттєвий вплив на продуктивний розвиток суспільства в цілому. Це у свою чергу потребує від людства нових способів та засобів поширення і використання глобальних знань з метою подальшого прогресу, що і є головною властивістю суспільства знань і інформації.

Однією з загальносвітових тенденцій є розвиток інформаційного суспільства та суспільства знань. Динаміка цього процесу, його результати для громадян, суспільства та держави значною мірою залежать від обґрунтованості відповідної державної політки та управління, які повинні формуватись на

основі достовірної, точної, своєчасної та повної інформації про стан, тенденції та фактори впливу на розвиток, в тому числі з урахуванням прогнозних оцінок наслідків прийнятих рішень тощо.

У сучасних умовах демократизації суспільства, зміни структури й змісту освіти, її гуманізації й гуманітаризації особливого значення набуває питання підготовки людини до повноцінного життя в інформаційному суспільстві. Суть переходу від індустріального суспільства до інформаційного полягає в тому, що інформація в різних видах і формах, і насамперед у формі знання, стає важливим стратегічним ресурсом, а технічні можливості інформаційно-комунікаційних технологій, систем і мереж – головним каталізатором швидкого розвитку й упровадження науковомістких, екологічно безпечних, енергозберігаючих і ресурсозберігаючих технологій у більшості галузей діяльності людини. Інформаційно-комунікаційні технології відіграють визначальну роль у забезпеченні інформаційної взаємодії між людьми, в підготовці й поширенні масової інформації, в процесі інтелектуалізації суспільства – розвитку культури, освіти, науки. Головний аспект цього процесу – поява якісно нових можливостей розв'язання глобальних економічних і соціальних проблем, у тому числі проблем культури, освіти, екології. Інформатизація є стратегічним напрямом переходу до інформаційного суспільства [1].

Водночас питання вирішення актуальних проблем інформатизації в Україні досліджено недостатньо і залишаються не розв'язаними. Це на нашу думку пов'язано, насамперед з тим, що нормотворча діяльність та теоретичні дослідження не завжди встигають за швидким виникненням та розвитком принципово нових суспільних відносин.

Сьогодні важко собі уявити інформаційну діяльність без використання сучасних інформаційних технологій, автоматизованих інформаційних систем, їх мереж, баз та банків даних, засобів обчислювальної техніки, зв'язку і телекомунікацій. впровадження інформаційних технологій, новітніх технічних засобів в життєдіяльність людства сприяло формуванню в забезпечувальній частині інформаційної сфери двох областей: області створення і застосування інформаційних технологій та області створення і застосування засобів та механізмів інформаційної безпеки.

Область створення і застосування інформаційних технологій пов'язана з вирішенням питань забезпечення сучасного технічного рівня обігу інформації у суспільстві. У свою чергу, сучасні системи зв'язку і телекомунікацій створили проблеми безпеки інформаційної сфери. Основним призначенням інформаційної безпеки вважається виявлення погроз і захист інформації від несанкціонованого доступу; інформаційних прав і свобод особи, суспільства, держави від впливу хибної, шкідливої інформації, дезінформації.

Область створення і застосування інформаційних технологій виникла і розвивається у зв'язку з потребами всіх інших областей. В той же час жодна з основних областей не може повноцінно функціонувати без використання сучасних програмно-технічних і телекомунікаційних засобів.

Розподіл інформаційної сфери на області умовний, оскільки всі вони тісно пов'язані між собою, впливають одна на одну. Вихідна інформація створюється під впливом оточуючого середовища, а також на основі інформації з інформаційних ресурсів. У свою чергу, інформаційні ресурси створюються на основі як вихідної інформації, так і відомостей з інших інформаційних ресурсів, які виступають як накопичувачі ретроспективної інформації (інформації, яка була створена у різні часи).

В результаті споживання інформації створюється нова інформація, формуються чи доповнюються інформаційні ресурси [2] .

На сьогодні розвиток інформаційного суспільства, поширення інформаційних технологій (ІТ) в усі сфери життєдіяльності людини та суспільства стали нормою подальшої еволюції цивілізації. Продовжується перехід до інформаційної сервісно-технологічної економіки, де значна частина ВВП забезпечується діяльністю з виробництва, обробки та поширення інформації та знань. Практично всіма фахівцями, економістами, політиками усвідомлено, що розвиток ІТ створює засади сучасної економіки та добробуту людини.

Інформаційне суспільство створює нові суспільно-політичні відносини, надаючи принципово нові можливості для комунікації, бізнесу, управління.

Більш того, інформатизація викликає принципово нові проблеми, що потребують правового регулювання. Юридичні питання електронного документообігу та мережі Інтернет, застосування криптографічних засобів і цифрової готівки, забезпечення секретності електронного листування та охорони авторських прав на програмне забезпечення, боротьби з кіберзлочинністю та ін. зумовили появу того, що називають «інформаційне право», «комп'ютерне право» або «право з інформаційних технологій», «телекомунікаційне право».

Врахування особливостей комплексу різнобічних факторів впливу поширення інформаційних технологій, а також особливостей стану країни потребує єдиної скоординованої державної політики з розвитку інформаційного суспільства та суспільства знань, що вимагає об'єднання зусиль держави,

бізнесу, громадських та міжнародних організацій, запровадження нових принципів їх взаємодії: партнерства, рівності, відкритості та прозорості.

Література:

1. Дмитришин В.С., Березанська В.П. Інтелектуальна власність на програмне забезпечення в Україні. К. : Вірлен, 2005. 312 с.
2. Ігнатушко Ю. І. Сучасний стан та проблеми використання комп'ютерного програмного забезпечення в органах внутрішніх справ України. *Наук.-практ. семінар 04 грудня 2009. Львівський державний університет внутрішніх справ*. С. 57–58.

Актуальні проблеми проведення судових експертиз під час розслідування воєнних злочинів

Матвєєвський О.В.
старший викладач кафедри
цивільного та трудового права
Національного університету «Одеська національна морська академія»

За всю історію більшість осіб, які вчинили військові злочини і злочини проти людяності, не було покарано. Незважаючи на військові трибунали, засновані після другої світової війни, і два недавніх міжнародних кримінальних трибуналу по колишній Югославії та Руанді, це ж справедливо й у відношенні 21 століття. З урахуванням цього розумно припустити, що більшість осіб, що здійснювали звірства, вважали, що вони не будуть покарані за злочини. Ефективне стримування є головною метою тих, хто виступає за заснування міжнародного кримінального суду. Як тільки стане ясно, що міжнародне співтовариство більше не буде миритися з такими жахливими діяннями і буде залучати до відповідальності і виносити відповідні покарання главам держав і військовим керівникам, а також рядовим військовослужбовцям або ополченцям, ті, хто підбурює до геноциду, здійснює кампанії етнічних чисток, вбивства, зґвалтування та звірства щодо цивільних осіб під час збройного конфлікту або використовує дітей у варварських медичних експериментах, вже не зможуть легко знаходити собі спільників.

Разом з тим процес доказування міжнародних злочинів є найскладнішим, тому що склад цих злочинів багато-об'єктовий, кількість епізодів велика, самі злочини досить різноманітні та фактично всі вони тяжкі.

Більшу частину серед них можливо характеризувати, як військові злочини. Розкриття і розслідування військових злочинів, а потім судовий розгляд справ – це головним чином процес доказування, який має постійно удосконалюватись на основі більш глибокого проникнення в сутність речей. Доказування в судочинстві спрямоване на встановлення фактів з відомостей які потрапляють слідчому у вигляді слідової інформації, яка потребує дослідження і тлумачення.

При розслідування військових злочинів кількість слідової інформації неймовірна. Це в першу чергу сліди біологічного походження, поранені та загиблі особи, залишки вибухових об'єктів та вибухової речовини, балістичні об'єкти різних форм (зброя, набої, сліди пострілу та інше), деталі військової техніки та озброєння та інше. Окремим напрямком для розгляду та вивчення є інформація стосовно тактики та техніки військових дій, стратегій проведення військових операцій.

Таким чином експертне забезпечення військових злочинів умовно необхідно поділити на три великих групи. По-перше це судово-медичні та військово-лікарські експертизи, далі йде великий пласт традиційних судових експертиз, і по-третє важливе значення мають спеціалізовані військово-технічні та військово-тактичні експертизи.

При розслідуванні воєнних злочинів суттєві для справи факти встановлюються за допомогою дослідження їх властивостей з використанням спеціальних знань. Спеціальні знання є професійними знаннями, які набуваються в наслідок освіти за фахом, навички при практичній діяльності в різних галузях науки, техніки, людської діяльності. Під спеціальними знаннями розуміються не лише наукові, технічні знання, а й знання в будь якої сфері людського життя. Фактично це життєвий досвід.

Становлення та залучення цих знань у судочинство здійснюється головним чином через судову експертизу. Використовуючи спеціальні знання у формі судової експертизи експерт проводить процесуальні дію, яка виконується за дорученням будь якої з сторін кримінального провадження і полягає в дослідженні на основі спеціальних знань матеріальних об'єктів, явищ та процесів, що містять інформацію про обставини справи. Саме процесуальні вимоги до проведення експертизи в українському судочинстві дуже звужують можливості дослідження.

По-перше, отримання об'єктів для проведення експертизи повинно проходити за спеціальною процесуальною процедурою, що дуже звужує кількість і якість досліджуваних об'єктів особливо при їх отриманні в час військових дій.

По-друге, в українському законодавстві процесуальні вимоги до експерта зовсім не гнучкі. В той час коли в законодавстві Німеччини судовим експертом може бути фахівець приведений судом до присяги, в Україні це людина яка ще й повинна отримати відповідну кваліфікацію і статус судового експерта.

Стан військової злочинності останнім часом все частіше перетинає міжнародні кордони, досягає безпрецедентних масштабів і становить реальну загрозу безпеці держав і всього людства. Розуміння цієї загрози сприяло створенню міжнародних механізмів попередження, припинення, виявлення злочинів і притягнення винних до юридичної відповідальності. Взаємодія й співпраця держав у сфері кримінального судочинства регулюється як нормами національного законодавства, так і міжнародними договорами та угодами. Це стосується й судової експертизи як однієї з форм застосування спеціальних знань у кримінальному судочинстві

Література:

1. Кримінальний процесуальний кодекс України від 13.04.2012 р. № 4651- VI // Відомості Верховної Ради України . 2013. № 9-10, № 11-12, № 13, ст.88.
2. Шестак В.А. Криминологические аспекты деятельности органов военного управления по предупреждению преступлений. *Lex Russica*. 2006. Т. LXV. № 5. С. 930–935..
3. Щедринов К. С. Взаимодействие военных следственных органов с другими правоохранительными органами при расследовании преступлений в районах вооруженного конфликта : [монография]. М. : Изд-ль Воробьев А. В., 2010. 228 с.
4. Zayas A. M. The Wehrmacht War Crimes Bureau, 1939–1945. Lincoln : Nebraska University Press, 1989. 364 p.2003. №4.

Інформаційно-аналітичне забезпечення та особливості здійснення пошуку осіб, які становлять оперативний інтерес у злочинах, пов'язаних з торгівлею людьми

Мельнікова О.О.
викладач кафедри кібербезпеки
та інформаційного забезпечення ОДУВС
к. ю. н.

Ісмайлов К.Ю.
завідувач кафедри кібербезпеки
та інформаційного забезпечення ОДУВС
к. ю. н.

Торгівля людьми має певні криміналістичні особливості тому, що ці злочини, головним чином, вчиняються організованими групами та злочинними організаціями. Організація оперативно-розшукових заходів щодо отримання цих відомостей здійснюється за участю всіх сил, засобів і заходів, які мають у своєму розпорядженні оперативні підрозділи БЗПТЛ. Указані ознаки можуть бути виявлені в процесі проведення: оперативного обслуговування територій та об'єктів; оперативного пошуку осіб і фактів, що становлять оперативний інтерес; використання негласного апарату; проведення оперативно-розшукових заходів у межах оперативно-розшукових справ; за матеріалами розслідування, які знаходяться у провадженні органів досудового слідства; вивчення загальних і спеціальних інформаційно-пошукових систем; повідомлення інших державних правоохоронних органів; повідомлення ЗМІ та громадян.

Дослідники А. Є. Чечетін і В. К. Якунін [195, с. 49] зазначають, що закономірності виникнення пошукової інформації виявляються в процесі: формування злочинної групи, коли особи з антигромадською установкою налагоджують між собою постійний контакт; залучення до групи нових осіб; попередньої підготовки до вчинення злочинів.

Ефективність оперативного пошуку фактів підготовки або вчинення торгівлі людьми визначається своєчасністю, повнотою та об'єктивністю інформації, що надходить до оперативних підрозділів з відкритих та негласних джерел, зручністю і можливостями обробки, зберігання та подальшого використання такої інформації. В епоху активного розвитку технічних новацій, що

дозволяють накопичувати та відтворювати значні масиви різноманітних даних, оптимально налагоджена система *інформаційно-аналітичного забезпечення* створює для оперативних співробітників реальні можливості встановлювати злочинців та запобігати злочинам «не виходячи з кабінету».

Згідно з визначенням В.Л. Регульського, інформаційно-аналітичне забезпечення, являє собою циклічний процес пошуку, збирання, опрацювання, переосмислення, зберігання, видачі інформації та її використання для прийняття оперативно-тактичних та інших рішень. Також можна визначити три методи інформаційно-аналітичного забезпечення в ОРД: інформаційно-аналітичний метод оцінки оперативної обстановки; інформаційно-аналітичний метод отримання і обробки відомостей про осіб, факти і події, що становлять оперативний інтерес; метод пошуку й використання відомостей, що містяться в інформаційно-пошукових системах [163, с. 15].

Інформаційно-аналітичне забезпечення оперативно-розшукової діяльності має на меті: підвищення ефективності протидії злочинності; створення умов для оперативної обізнаності працівників, які безпосередньо займаються профілактикою та виявленням злочинів; формалізацію необхідної взаємодії між службами та підрозділами органів внутрішніх справ; своєчасне реагування та вжиття попереджувальних заходів, спрямованих на недопущення вчинення кримінальних правопорушень певним колом осіб; отримання відомостей для оперативного реагування на заяви та повідомлення про вчинені кримінальні правопорушення, інші події, у яких убачаються їх ознаки; профілактичну роботу з криміногенною категорією громадян та особами, які перебувають на обліках Національної поліції України; контроль за оперативно-службовою діяльністю служб і підрозділів Національної поліції України.

Аналіз практики роботи свідчить, що на сучасному етапі до головних завдань інформаційно-аналітичної роботи підрозділів БЗПТЛ належать: надання можливості оперативного одержання інформації в повному, систематизованому і зручному для використання вигляді для розкриття, розслідування, попередження злочинів та розшуку злочинців; збирання, опрацювання, узагальнення та аналіз оперативної, оперативно-розшукової, оперативно-довідкової, аналітичної, статистичної і контрольної інформації для оцінки ситуації і прийняття обґрунтованих оптимальних рішень на всіх рівнях управління Національної поліції України; інтеграція і систематизація оперативних обліків Національної поліції України на всіх рівнях; створення умов для ефективного функціонування оперативних обліків, забезпечення їхньої повноти, вірогідності та актуальності; забезпечення комплексного захисту інформації та розмежування доступу до інформації.

У системі інформаційно-аналітичного забезпечення оперативних підрозділів за ознаками новизни і періодичності надходження необхідно розрізняти два види оперативно-розшукової інформації: первинні дані, тобто раніше невідома інформація, що становить оперативний інтерес; інформація, що перевірена, накопичена, врахована внаслідок здійснення оперативно-розшукових заходів і пристосована для використання в боротьбі зі злочинністю [39, с. 49; 101, с. 154].

Для систематизації матеріалів, одержаних за результатами оперативного пошуку, у т.ч. ознак торгівлі людьми, створюються відповідні оперативні обліки. Оперативні обліки – це система реєстрації, накопичення, класифікації, зберігання та використання даних про осіб, предмети, події за їх прикметами та ознаками, призначена для ефективного забезпечення негласної роботи та оперативно-розшукової діяльності оперативних підрозділів кримінальної та спеціальної поліції, яка складається з автоматизованих інформаційно-пошукових систем, картотек, оперативно-розшукових справ, справ контрольно-наглядового провадження та інших документів оперативно-розшукового та довідкового призначення. До оперативних обліків належать оперативно-розшукові, оперативно-профілактичні та оперативно-довідкові. Ведення та супроводження баз (банків) даних, що формуються в процесі здійснення оперативно-розшукової діяльності органів і підрозділів поліції, крім підрозділів Департаменту внутрішньої безпеки, здійснюється виключно ДІПКП «102» Національної поліції України, УІЗ територіальних органів НП України.

Для систематизації та аналізу матеріалів, одержаних у результаті оперативно-розшукової діяльності, в ДІПКП «102» та УІЗ територіальних органів Національної поліції України функціонує автоматизована інформаційна система оперативного призначення АІС «ОРІОН». АІС «ОРІОН» побудована за дворівневою ієрархічною структурою:

- перший рівень - центральний вузол АІС «ОРІОН» – розташовано в спеціально виділених службових приміщеннях ДІПКП «102» Національної поліції України, де накопичується інформація територіальних, міжрегіональних органів (підрозділів) Національної поліції України, оперативних підрозділів апарату Національної поліції України, і та що надходить з її відокремлених (структурних) територіальних, міжрегіональних органів (підрозділів) Національної поліції України;

- другий рівень - регіональні (обласні) вузли АІС «ОРІОН» – розташовано в спеціально виділених службових приміщеннях УІЗ територіальних органів Національної поліції України, де здійснюється збір, оброблення, зберігання інформації та її використання для інформаційно-аналітичного

забезпечення роботи оперативних підрозділів територіальних, міжрегіональних органів (підрозділів) Національної поліції України.

Використання реальних (діючих) інформаційних ресурсів АІС «ОРІОН» у навчальних цілях – забороняється. Обліку в АІС «ОРІОН» підлягає:

- відомості про осіб, які розробляються за ОРС на підставі інформаційної картки на особу ІК-Т;
- відомості, що отримані від осіб, яких готують або які вже залучені до негласного співробітництва;
- інформація, отримана в ході проведення негласної роботи та оперативно-розшукової діяльності, якщо в ній містяться відомості про: осіб, причетних до вчинення кримінальних правопорушень; злочинів, учинених у складі організованих груп чи злочинних організацій; пов'язаних з використанням вогнепальної, холодної зброї, боєприпасів, радіоактивних та психотропних речовин; з нелегальною міграцією, торгівлею людьми, кіберзлочинністю; учинених на пріоритетних напрямах економіки, на підприємствах, що мають стратегічне значення;
- відомості щодо проведених ОРЗ в рамках ОРС.

З метою отримання інформації, необхідної для негласної роботи та оперативно-розшукової діяльності, використовується інтегрована інформаційно-пошукова система (ІПС), що функціонує в системі Національної поліції України.

Таким чином, інформаційно-аналітичному забезпеченню відводиться провідна роль у справі виявлення торгівлі людьми, оскільки є реальні можливості встановлювати злочинців та запобігати злочинам за допомогою інформаційно-пошукових систем.

Література:

1. Кримінальний процесуальний кодекс України [Електронний ресурс] : закон України від 13.04.2012 р. № 4651-VI : за станом на 16. 03. 2018 р. № 2147а-19. URL: http://zakon3.rada.gov.ua. (дата звернення: 16. 08. 2018).
2. Душейко Г. О. Організаційно-тактичні основи реалізації оперативно-розшукової інформації на стадії порушення кримінальної справи : дис. … канд. юрид. наук : спец. 21.07.04. Харків, 2001. 268 с.
3. Мякота Є.В. Критерії оцінювання інформації, здобутої під час оперативного пошуку легалізації (відмивання) доходів, одержаних злочинним шляхом. Південноукраїнський правничий часопис. 2014. № 2 т. С. 152-159.
4. Регульський В.Л. Оперативно-розшукова діяльність органів внутрішніх справ : правові та організаційні основи : автореф. дис. ... канд. юрид. наук : 21.00.06. / НАВСУ. К., 1997. 20 с.
5. Чечетин А.Е., Якунин В.К. Некоторые особенности выявления организованных групп. Межвузовский сборник научных трудов. Омск : ВШМ МВД СССР, 1988. С. 48-65.

Проблемні питання захисту персональних даних при використанні інформаційних систем та технологій в боротьбі зі злочинністю

Мудрецька Г. В.
доцент кафедри кримінального процесу
Одеський державний університет внутрішні справ
к.ю.н.

Відповідно до статті 2 Закону України «Про захист персональних даних» персональними даними є відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

Відповідно до ч. 5 ст. 6 Закону, обробка персональних даних здійснюється виключно на підставі згоди особи або закону. Дане положення конкретизується статтею 11 Закону та статтею 7 Директиви 95/46/ЄС Європейського Парламенту та Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 року та статтею 6 Регламенту про захист персональних даних, який набрав чинності 24 травня 2016 року. Так, стаття 11 Закону встановлює вичерпний перелік випадків та умов, за яких може здійснюватися обробка персональних даних суб'єкта. Ця стаття є першим «фільтром» на шляху до законної обробки. Якщо обробка виходить за межі передбачених статтею 11 Закону випадків, вона автоматично розглядається як незаконна.

Положення частини першої цієї статті не застосовується, якщо обробка персональних даних:

- здійснюється за умови надання суб'єктом персональних даних однозначної згоди на обробку таких даних *;*
- необхідна для здійснення прав та виконання обов'язків володільця у сфері трудових правовідносин відповідно до закону із забезпеченням відповідного захисту;
- необхідна для захисту життєво важливих інтересів суб'єкта персональних даних або іншої особи у разі недієздатності або обмеження цивільної дієздатності суб'єкта персональних даних;
- здійснюється із забезпеченням відповідного захисту релігійною організацією, громадською організацією світоглядної спрямованості, політичною партією або професійною спілкою, що створені відповідно до закону, за умови, що обробка стосується виключно персональних даних членів цих об'єднань або осіб, які підтримують постійні контакти з ними у зв'язку з характером їх діяльності, та персональні дані не передаються третій особі без згоди суб'єктів персональних даних;
- необхідна для обґрунтування, задоволення або захисту правової;
- необхідна в цілях охорони здоров'я, встановлення медичного діагнозу, для забезпечення піклування чи лікування або надання медичних послуг за умови, що такі дані обробляються медичним працівником або іншою особою закладу охорони здоров'я, на якого покладено обов'язки щодо забезпечення захисту персональних даних та на якого поширюється законодавство про лікарську таємницю;
- стосується вироків суду, виконання завдань оперативно-розшукової чи контррозвідувальної діяльності, боротьби з тероризмом та здійснюється державним органом в межах його повноважень, визначених законом;
- стосується даних, які були явно оприлюднені суб'єктом персональних даних.

До найпоширеніших порушень відносять несанкціонований доступ до персональних даних державними та приватними установами, включаючи правоохоронні органи, за відсутності законної підстави та обґрунтованої мети такого доступу; незаконна обробка чутливої категорії персональних даних шляхом надання необмеженого до них доступу та розкриття для широкого загалу, а також збір надмірного обсягу даних щодо цілей, для яких вони обробляються в подальшому; недотримання прав суб'єктів на інформування й доступ до інформації про операції з обробки персональних даних, які їх стосуються; недотримання режиму конфіденційності та безпеки обробки персональних даних у випадках незаконної передачі баз персональних даних між володільцями даних, зокрема, з метою особистих інтересів; обробка персональних даних з метою, несумісною з тією, з якою їх було зібрано спочатку; відсутність належної політики безпеки персональних даних, затвердженої володільцем таких даних; відсутність відповідальних осіб з питань захисту даних в установах, організаціях, які є володільцями баз даних; передача даних через незахищені канали, у тому числі приватні поштові скриньки в мережі Інтернет [1].

Українське законодавство про захист персональних даних складається з більше ніж 20 нормативно-правових актів, які не мають чіткого та скорельованого з європейським законодавством визначення персональних даних. Зокрема, в ньому відсутнє право людини на інформаційне самовизначення як повноваження кожного самостійно приймати рішення про розголошення та використання своїх персональних даних [2].

Для усунення таких порушень, необхідно закріпити на законодавчому рівні та впровадити в практику певні гарантії захисту прав людини. Захист персональних даних є сукупністю правових, організаційних і технічних заходів, спрямованих на недопущення неправомірних дій з персональними даними, забезпечення їх конфіденційності, а також можливості доступу суб'єктів персональних даних до інформації про дії з їхніми персональними даними [3, с. 203]. Водночас безумовними перевагами єдиного інформаційного простору правоохоронних органів можна назвати підвищення міжнародного співробітництва в інформаційній сфері та протидію і запобігання правопорушенням.

Література:

1. Боротьба з несанкціонованим доступом і незаконними операціями з обробки персональних даних. URL: http://police-access.info/2015/04/borotba-znesanktsionovanym-dostupom-i-nezakonnymyoperatsiyamy-z-obrobky-personalnyh-danyh
2. Валентин Головченко. Правові основи захисту персональних даних. Юридична газета. URL: http://yur-gazeta.com/publications/practice/inshe/pravovi-osnovi-zahistu-personalnih-danih.html
3. Єсімов С.С. Захист персональних даних у контексті розвитку динамічних інформаційних систем. Науковий вісник Львівського державного університету внутрішніх справ. 2013. № 3. С. 198–208.

Одеський державний університет внутрішніх справ
«Кібербезпека в Україні: правові та організаційні питання»

Прикладні аспекти фахової підготовки працівників кіберполіції

Пекарський С. П.
доцент кафедри спеціальних дисциплін
та професійної підготовки факультету № 2,
(*Донецький юридичний інститут МВС України*)
к. ю. н.

Ефективна протидія будь-якому виду злочинів вимагає якісної теоретичної та практичної підготовки. Підготовка фахівців для підрозділів Національної поліції здійснюється в закладах вищої освіти зі специфічними умовами навчання, які відносяться до сфери управління МВС України. Беззаперечним є те, що в умовах військової протидії проросійським збройним формуванням на Сході України загострилося питання і кібербезпеки нашої держави.

Отже, міжрегіональним територіальним органом Національної поліції України, який входить до структури кримінальної поліції Національної поліції та відповідно до законодавства України забезпечує реалізацію державної політики у сфері боротьби з кіберзлочинністю, організовує та здійснює відповідно до законодавства оперативно-розшукову діяльність є Департамент кіберполіції Національної поліції України [1]. Зазначаємо, що на сучасному етапі розвитку правоохоронних системи ми стали свідками перетворення колишньої моделі підрозділів боротьби з кіберзлочинністю у новітній орган правозахисного призначення, який за своїми технічними та професійними можливостями має змогу миттєво реагувати на кіберзагрози, а також, у відповідності до кращих європейських та світових стандартів проводить міжнародну співпрацю по знешкодженню транснаціональних злочинних угрупувань у даній сфері. Саме тому висуваємо гіпотезу, що якісна протидія кіберзлочинам вимагає відповідної теоретичної та практичної підготовки працівників підрозділів Департаменту кіберполіції.

На нашу думку, провідну роль у процесі підготовки фахівців для підрозділів кіберполіції повинні відігравати заклади вищої освіти зі специфічними умовами навчання, які входять до сфери управління МВС України. Саме тому вважаємо, що навчальний план підготовки фахівців для підрозділів кіберполіції ступеня бакалавра за спеціальністю «Право» повинен мати термін навчання 4 роки та передбачати здобуття особою теоретичних знань, практичних умінь та навичок, достатніх для якісного виконання обов'язків з протидії злочинності за відповідною оперативно-розшуковою спеціалізацією кримінальної поліції. Також навчальна програма повинна передбачати опанування ряду специфічних дисциплін, вивчення яких є обов'язковим для подальшої професійної діяльності співробітника кіберполіції. Навчальний план для кіберполіції повинен включати загальні юридичні і спеціальні технічні дисципліни. Безпосередньо майбутні кіберполіцейські повинні оволодіти знаннями, виробити уміння та навички щодо протидії:

- злочинам проти інформаційної безпеки;
- on-line шахрайству і фінансовим злочинам;
- протиправному контенту;
- злочинам, які вчиняються з використанням інформаційних технологій та мережі Інтернет.

Тобто виявляти ознаки даних злочинних дій, осіб, які їх готують, вчинюють, надавати вірну юридичну кваліфікацію, документувати злочинну діяльність як гласно так і не гласно, здійснюючи комплекс оперативно-розшукових заходів чи негласних слідчих (розшукових) дій за допомогою технічних навиків та умінь роботи з електронно-обчислювальними машинами (комп'ютерами), телекомунікаційними та комп'ютерними Інтернет-мережами і системами.

Саме тому підготовка повинна мати специфіку, яка дозволить якісно виявляти та фіксувати цифрові джерела інформації, онлайн-джерела інформації - так звані «Електронні докази». Так ми погоджуємося з твердженням, що цифровими джерелами інформації є електронні пристрої: комп'ютери та периферійні пристрої, комп'ютерні мережі, мобільні телефони, цифрові камери і інші портативні пристрої, в тому числі пристрої для зберігання інформації, а також мереже Інтернет. Інформація з цих джерел не має відокремленої фізичної форми [2, ст. 26]. Своєю чергою у статті 96 Закону України від 3 жовтня 2017 року № 2147-VIII «Про внесення змін до Господарського процесуального кодексу України, Цивільного процесуального кодексу України, Кодексу адміністративного судочинства України та інших законодавчих актів» надано визначення поняттю «електронний доказ» [3]. Тому під електронним доказом слід розуміти інформацію в електронній (цифровій) формі, яка містить дані про обставини, що мають значення для справи, зокрема, електронні документи (в тому числі текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи тощо), веб-сайти (сторінки), текстові, мультимедійні та голосові повідомлення, метадані, бази даних й інші дані в електронній формі. Такі дані можуть зберігатися, зокрема на портативних пристроях (картах пам'яті, мобільних телефонах

тощо), серверах, системах резервного копіювання, інших місцях збереження даних в електронній формі (в тому числі в мережі Інтернет). [3, ст. 96].

Враховуючи те, що електронні дані не мають матеріального втілення і тому їх набагато легше змінити або підробити, ніж традиційні форми доказів [2, ст. 26] це ставить перед правоохоронцями завдання щодо якісного їх виявлення, фіксації, вилучення, та використання в кримінальному провадженні. Особливістю також є те, що знайти і оцінити, чи належать певні дані до події кіберзлочину без застосування програмно-технічних засобів не можливо [2, ст. 27].

Окрім того, слід погодитися з висновком про те, що нові технології з'являються і розвиваються з неймовірною швидкістю, тому методи і процедури роботи з доказами із цифрових джерел інформації потрібно постійно переглядати та оновлювати [2, ст. 28]. Даний висновок на нашу думку повністю відноситься і до планування теоретичної та практичної підготовки фахівців для підрозділів кіберполіції.

Саме тому, з точки зору прикладної підготовки, під час освітнього процесу необхідно звертати увагу на: аспекти аналітичної роботи правоохоронних органів, загальний порядок пошуку інформації про об'єкти в мережі, загальні особливості роботи з доказами, одержаними в результаті негласних слідчих (розшукових) дій тощо. Окремо потрібно приділяти увагу вивченню інформаційних технологій, які використовуються для вчинення кіберзлочинів. Як приклад інформаційні технології, які використовуються при торгівлі людьми, зокрема: для вербування, контролю та експлуатації жертв – спеціально створені веб-сайти, комп'ютерні соціальні мережі, мережеві сховища тощо. Потребують уваги і інформаційні технології, які використовуються для комунікації, незаконного одержання та відмивання коштів: електронна пошта, мультимедійні засоби спілкування, технології забезпечення анонімності та безпечної передачі інформації в мережі тощо.

Також виробка практичних навичок при проведенні слідчих (розшукових) дій в тому числі і негласних, а також оперативно-розшукових заходів при документуванні кіберзлочинів потребує уваги. Як приклад: огляд місця події злочину, вчиненого з застосуванням інформаційних технологій, огляд засобів комп'ютерної техніки чи огляд мобільних засобів мають свою специфіку і вимагають відповідних технічних знань та умінь, а також і залучення відповідних спеціалістів.

Підводячи підсумок зазначаємо, що нами розглянута деякі прикладні питання підготовки фахівців для підрозділів кіберполіції. Загальним є те, що система даної підготовки повинна відповідати вимогам Законів України: «Про вищу освіту», «Про Національну поліцію», «Про оперативно-розшукову діяльність», іншим нормативно-правовим актам МОН та МВС України щодо організації освітнього процесу у закладах вищої освіти зі специфічними умовами навчання, які входять до сфери управління МВС України. Сподіваємося, що під час конференції дане питання викличе жваву наукову дискусію.

Література:

1. Кіберполіція України, офіційний сайт [Електронний ресурс]. Режим доступу https://cyberpolice.gov.ua/contacts/;
2. Виявлення, попередження та розслідування злочинів торгівлі людьми, вчинених із застосуванням інформаційних технологій: навчальний курс / [А. Вінаков, В. Гузій, Д. Девіс, В. Дубина, М. Каліжевський, О. Манжай, В. Марков, В. Носов, О. Соловйов]. К., 2017. 148 с.
3. Про внесення змін до Господарського процесуального кодексу України, Цивільного процесуального кодексу України, Кодексу адміністративного судочинства України та інших законодавчих актів: Закон України від 3 жовтня 2017 року № 2147-VIII [Електронний ресурс]. Режим доступу https://zakon.rada.gov.ua/laws/show/2147%D0%B0-19#n2.

Криміналістичний моніторинг як метод боротьби з кіберзлочинністю

Теслюк І.О.
т.в.о. завідувача докторантури та аспірантури
Одеського державного університету внутрішніх справ
к. ю. н.

Розвиток України, як демократичної правової держави, неможливий без розробки механізму боротьби зі злочинністю. Сучасні методи боротьби з кримінальними правопорушеннями, які обумовлені впливом модифікованих інформаційних технологій, потребують наукового дослідження та обґрунтування. Очевидно, що проблема боротьби з кіберзлочинністю поширена у всіх країнах світу, у тому числі й в Україні. Щоденний пошук новітніх методів щодо попередження, запобігання та протидії злочинів з використанням інформаційно-комунікаційних технологій, направлений на зниження рівня прояву правопорушень, які останнім часом вчиняються все частіше.

Як зазначає Карчевська Г.Р. [1], з врахуванням наявних проблем діяльності судових та правоохоронних органів у сфері боротьби з кіберзлочинністю, вирішення чи подолання цих проблем має бути насамперед спрямоване на:

• по-перше, гармонізацію міжнародного та вітчизняного та законодавства у сфері кіберзлочинності, внесенням відповідних змін у кримінальне процесуальне законодавство України, зокрема щодо врахування особливостей оцінки судом електронних доказів, як таких, що найчастіше фігурують у кримінальних провадженнях з розслідування кіберзлочинів;

• по-друге, подальшу розробку окремих криміналістичних методик розслідування кіберзлочинів, з врахуванням останніх тенденцій щодо типових способів вчинення даного виду злочинів;

• по-третє, забезпечення належної фахової підготовки правоохоронців та суддів, до обов'язків яких належить розслідування кіберзлочинів та розгляд судових справ щодо них [1].

Цілком погоджуємося з вищезазначеним. Що стосується розробки окремих криміналістичних методик розслідування кіберзлочинів, то вважаємо, що для ефективної боротьби з кіберзлочинністю вкрай важливим є застосування методу криміналістичного моніторингу.

Основним завданням криміналістичного моніторингу у процесі боротьби з кіберзлочинністю та й зі злочинністю загалом, є постійний контроль динаміки показників, які відображають рівень злочинності (по типу, способу та ін.) за певний проміжок часу, у певному регіоні.

Криміналістичний моніторинг у боротьбі з кіберзлочинністю призначений для:

відстеження кіберзлочинних проявів державного та міжнародного значення;

виявлення осередку (першоджерело) вчинення кіберзлочинів;

оцінку способів та масштабів вчинення кіберзлочинів;

своєчасне реагування на злочини, які готуються у кіберпросторі;

планування подальших дій та стратегій по боротьбі з кіберзлочинністю.

Предметом криміналістичного моніторингу у боротьбі з кіберзлочинністю є протиправні злочинні дії (або бездіяльність) у кіберпросторі.

Суб'єктами криміналістичного моніторингу у боротьбі з кіберзлочинністю є слідчий, начальник слідчого відділення, оперуповноважений (за дорученням слідчого), прокурор, суддя (у ході судового розгляду).

Об'єктом криміналістичного моніторингу у боротьбі з кіберзлочинністю є кримінальні правопорушення у сфері інформаційних технологій, за допомогою комп'ютерної техніки, мереж зв'язку, мобільних засобів комунікації.

Боротьба з кіберзлочинністю неможлива без глибокого аналізу, узагальнення, перевірки та систематизації даних. Криміналістичний моніторинг у боротьбі з кіберзлочинністю є комплексною системою:

а) збору оперативної інформації щодо кіберзлочинних проявів;

б) аналізу та оцінки інформації в напрямі реальних загроз в інформаційних системах;

в) узагальнення даних щодо кіберзлочинних атак та протиправних дій в сфері інформаційних технологій;

г) порівняння інформації щодо специфіки вчинених кіберзлочинів на рівні регіону (області), держави чи міжнародному рівні;

д) систематизації криміналістично важливої інформації щодо окремих способів вчинення кіберзлочинів;

е) класифікації даних про кіберзлочинність, отриманих протягом місяця, декади, року;

є) перевірки достовірності та співвідношення отриманої інформації про вчинені кіберзлочини або злочини, які готуються в сфері інформаційних технологій;

ж) використання інформації для боротьби з кіберзлочинністю в цілому.

Перспективою застосування методу криміналістичного моніторингу органами досудового розслідування у боротьбі з кіберзлочинністю є оперативні зведення, наукові прогнози та рекомендації, спрямовані на вжиття превентивних заходів щодо зниження рівня кримінальних правопорушень у сфері інформаційних технологій.

Невідповідність діючого законодавства та відсутність нормативно-правового забезпечення, яке б регулювало суспільні відносини у сфері боротьби з кіберзлочинністю, створює сприятливі умови для підвищення рівня злочинності у сфері інформаційних технологій (комп'ютерних мереж, засобів зв'язку та ін..), а також появи нових способів їх вчинення.

Література:

1. Карчевська Г.Р. Правове регулювання інформаційних технологій в Україні: проблеми та перспективи сучасності. Збірник кращих студентських робіт. [Електронний ресурс]: Режим доступу https://ukrainepravo.com/legal_publications/essay-on-it-law/it_law_ karachevska_cybercrime/

СЕКЦІЯ 1
ПРАВОВЕ РЕГУЛЮВАННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

СЕКЦІЯ 2
АДМІНІСТРАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

СЕКЦІЯ 3
ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ В БОРОТЬБІ З КІБЕРЗЛОЧИННІСТЮ

СЕКЦІЯ 4
ПІДГОТОВКА ПЕРСОНАЛУ ДЛЯ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ В УКРАЇНІ

СЕКЦІЯ 5
ІНФОРМАЦІЙНО-АНАЛІТИЧНА ДІЯЛЬНІСТЬ ПРАВООХОРОННИХ ОРГАНІВ У БОРОТЬБІ ЗІ ЗЛОЧИННІСТЮ

Міжнародна науково-практична конференція
Кібербезпека в Україні: правові та організаційні питання
15 листопада 2020 року
м. Одеса, Україна

ЗАПРОШЕННЯ

Інформуємо Вас, що **15 листопада 2020 року** в м. Одеса відбудеться Міжнародна науково-практична конференція «Кібербезпека в Україні: правові та організаційні питання».

Для участі в конференції запрошуються вчені, співробітники науково-дослідних установ, аспіранти, курсанти, студенти.

Робочі мови конференції: українська, англійська, російська.

ПОДАННЯ ДОКУМЕНТІВ:

Для участі в конференції представити наступні документи:

1. Заявку у відповідності з формою;
2. Тези доповіді на одній із робочих мов, оформлені у відповідності із запропонованим зразком;

ПУБЛІКАЦІЯ ПРАЦЬ КОНФЕРЕНЦІЇ

Тези доповідей, отримані Організаційним комітетом та прийняті до друку, будуть видані до початку конференції у збірнику праць конференції та вислані безкоштовно на електронні адреса учасників конференції.

АДРЕСА ОРГКОМІТЕТУ:

Кафедра кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішніх справ

Адреса: вул. Успенська, 1, м. Одеса, 65000, Україна
Сайт: http://oduvs.sem-dev.co.ua/kafedra-kiberbezpeki-ta-informatsijnogo-zabezpechennya/
E-mail: 0997060070@ukr.net
facebook: https://www.facebook.com/kiberoduvs

Контактні особи:

Ісмайлов Карен Юрійович +38 (099) 70-600-70;
+38 (097) 70-600-90;
0997060070@ukr.net

Одеський державний університет внутрішніх справ
«Кібербезпека в Україні: правові та організаційні питання»
Наукове видання

КІБЕРБЕЗПЕКА В УКРАЇНІ: ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ ПИТАННЯ

Матеріали
Міжнародної науково-практичної конференції

22 листопада 2019 року

Підписано до друку 12.12.2019.Формат 60х90/8. Папір офсетний.
Гарн. «Times New Roman» Друк цифровий. Ум. друк арк. 26,1.
Наклад 500 прим.
Видавництво ОДУВС
м. Одеса, вул. Успенська, 1
Свідоцтво суб'єкта видавничої справи ДК № 3507 від 25.06.2009 р.
тел. 0487024884; 0949547884 email – *ndrvv1@gmail.com*