УДК 343.14

НІЗОВЦЕВ Ю.Ю., здобувач наукового ступеня кандидата наук,
Національна академія СБ України
ЛЕОНОВ Б.Д., *доктор юридичних наук, старший науковий співробітник*,
провідний науковий співробітник
Національної академії СБ України

ВИКОРИСТАННЯ КІБЕРТЕХНОЛОГІЙ У ПРОЦЕСІ РОЗСЛІДУВАННЯ ЗЛОЧИНІВ: АНАЛІЗ ЗАРУБІЖНОГО ДОСВІДУ

Анотація. *У статті розглянуто та проаналізовано досвід застосування кібертехнологій негласного стеження за комп'ютерами підозрюваних осіб з боку правоохоронних органів та спецслужб ФРН та США, а також сформульовано відповідні рекомендації для впровадження у діяльність вітчизняних правоохоронних органів.*

Ключові слова: *кіберзлочин, шкідливий програмний засіб, шпигунська програма, негласне спостереження.*

Summary. *The article examines and analyzes the experience of using cyber technologies of silent surveillance of computers of suspected persons by law enforcement agencies and special services of the Federal Republic of Germany and the USA, highlights the advantages and disadvantages, and also provides recommendations for implementation thereof in the activities of domestic law enforcement agencies.*

Keywords: *cybercrime, malware, spyware, silent surveillance.*

Аннотация. *В статье рассмотрен и проанализирован опыт применения правоохранительными органами и спецслужбами ФРГ и США кибертехнологий негласного наблюдения за компьютерами подозреваемых, а также сформулированы соответствующие рекомендации внедрения в деятельность отечественных правоохранительных органов.*

Ключевые слова: *киберпреступление, вредоносная программа, шпионская программа, негласное наблюдение.*

Постановка проблеми. Поєднання різноманітних інформаційних ресурсів глобальною мережею Інтернет дозволило людству значно прискорити обмін інформацією і, таким чином, суттєво поліпшити умови праці та підвищити її ефективність. Разом з тим, доступність комп’ютерної техніки, мережі Інтернет та “хмарних” технологій надають змогу обізнаному в інформаційних технологіях зловмиснику застосовувати свої знання для вчинення кіберзлочину з будь-якого місця планети, у будь-якому населеному пункті, здійснивши атаку на об’єкти, які можуть знаходитись за тисячі кілометрів від нього.

Розслідування такого роду злочинів не є цілковитою новацією для вітчизняних правоохоронних органів. Разом з тим, все ще залишається проблемою їх виявляти, фіксувати і вилучати криміналістично значиму інформацію при розслідуванні вказаної категорії злочинів для використання її надалі в якості доказової інформації. Причинами цього є дефіцит кваліфікованих кадрів, на достатньому рівні обізнаних в інформаційних технологіях, і відсутність належної кількості спеціального криміналістичного обладнання, а також відсутність практики розслідування таких злочинів тощо. Зважаючи на це, дуже корисним є вивчення досвіду розвинутих країн, в яких необхідність розслідування злочинів у кіберпросторі виникла значно раніше, ніж в нашій державі.

Результати аналізу наукових публікацій. Різним аспектам протидії кіберзлочинності, у тому числі, пов’язаним з використанням злочинцями шкідливих програмних засобів, присвятили свої роботи Д.С. Азаров, П.Д. Біленчук, А.С. Білоусов, В.М. Бутузов, В.О. Вітюк, О.П. Войтович, В.Д. Гавловський, Ю.В. Гаврилін, В.О. Голубєв, С.М. Гусаров, В.А. Каплун, М.В. Карчевський, Н.С. Козак, В.В. Крилов, С.А. Кузьмін, А.А. Музика, Л.П. Паламарчук, Д.В. Пашнєв, Н.А. Розенфельд, М.В. Рудик, Л.М. Соловйов, Т.Л. Тропіна, В.П. Шеломенцев та інші вчені. Разом з тим, досі не досліджувався досвід використання шкідливих програмних засобів іноземними спецслужбами та правоохоронними органами з метою негласного стеження під час розслідування злочинів, і, відповідно, не вироблялися розроблені на основі аналізу цього досвіду рекомендації для впровадження у практичну діяльність вітчизняних правоохоронних органів.

Метою статті є аналіз передового зарубіжного досвіду використання кібертехнологій при розслідуванні злочинів, виявлення позитивних та негативних тенденцій такої практики, вироблення рекомендацій для використання цього досвіду українськими правоохоронними органами.

Виклад основного матеріалу. Детальний огляд всього прогресивного досвіду застосування так званих шпигунських програм, які є різновидом шкідливих програмних засобів (далі – ШПЗ), правоохоронними органами та спеціальними службами виходить за межі даного дослідження. З огляду на вітчизняне законодавство, вважаємо за доцільне розглянути і проаналізувати два приклади застосування ШПЗ, а саме, їх застосування при розслідуванні кіберзлочинів правоохоронними органами Федеративної Республіки Німеччини та Федеральним бюро розслідувань Сполучених Штатів Америки.

У 2008 році Конституційний суд ФРН своїм рішенням дозволив проведення таємних онлайн-обшуків персональних комп’ютерів підозрюваних у разі суворого дотримання низки умов. Цей спосіб проведення розслідувань може застосовуватись лише тоді, коли є “обґрунтовані підозри в наявності загрози встановленому правопорядку”, перш за все “здоров’ю, життю і свободі людини”. Норма діє також у разі виникнення загрози основам і власності держави або основам існування людини. Проведення таємних он-лайн-обшуків допускається тільки із санкції суду. Застосовувана при цьому шпигунська програма отримала назву “бундестроянець”.

Зважаючи на ефективність цієї технології, парламент ФРН 22 червня 2017 року своїм законом дозволив використовувати “бундестроянця” для спостереження за перепискою в Інтернеті або через месенджери, наприклад WhatsApp. Оскільки повідомлення месенджерів передаються каналами зв’язку у зашифрованому вигляді, залишається єдина реальна можливість їх переглянути – на пристрої відправника та/або на пристрої отримувача, що й буде здійснювати “бундестроянець”. Крім того, розширилось коло випадків його застосування. Якщо раніше приховане кіберспостереження дозволялося застосовувати лише в справах, пов’язаних з тероризмом, то тепер Бундестаг дозволив використовувати вказані технології при розслідуванні вбивств, комп’ютерних махінацій, відмивання грошей, ухилення від сплати податків, злочинів, пов’язаних з порушенням міграційного законодавства. Як і при прослуховуванні телефонних розмов, служби, які ведуть спостереження, зобов’язані у кожному окремому випадку отримати відповідний дозвіл від прокуратури [1].

Розглянемо особливості процедури застосування кібертехнологій з метою розслідування правопорушень за законодавством ФРН. Зокрема, під час використання спеціальних технічних засобів до інформаційно-технічної системи вносяться тільки ті зміни, які потрібні для збирання даних, а після закінчення заходу вносяться всі можливі технічні зміни, що автоматично повертають систему до вихідного стану.

Скопійовані дані мають бути технічно захищені від змін, несанкціонованого використання та несанкціонованого ознайомлення.

Використання технічного засобу має бути запротокольоване із зазначенням: характеристик технічного засобу і часу його використання; технічних даних ідентифікації інформаційно-технічної системи, а також тих систем, в яких проводилися навіть незначні зміни; інформації, що дозволяє встановити місце розташування зібраних даних; відомостей про підрозділ, який проводить цей захід.

Дані протоколу можуть використовуватися з метою підтвердження для підозрюваного законності проведення заходу або для встановлення місця, де проводився цей захід.

Заходи щодо проникнення в інформаційно-технічні системи можуть бути спрямовані лише щодо особи, яка підлягає відповідальності згідно з § 17 або § 18 Закону “Про Федеральну поліцію”.

Указані заходи здійснюються за поданням керівника Федерального відомства кримінальної поліції (далі – ВКА) або його заступника на підставі судового ордеру, в якому повинно бути зазначено: прізвище та адреса особи, стосовно якої проводиться захід (в разі наявності); за можливості точна характеристика інформаційно-технічної системи, в якій має проводитися збирання даних; тип, межі та тривалість заходу із зазначенням часу його закінчення; головні причини проведення.

Під час проведення заходу правоохоронцями докладається максимум зусиль (наскільки це дозволяють технічні можливості), для того щоб відомості, які стосуються сфери особистого життя, не збиралися. Отримані дані (під наглядом уповноваженого представника суду) мають негайно переглядатись уповноваженим з питань захисту даних Федеральної кримінальної поліції та двома службовцями ВКА, один з яких має бути фахівцем із судових справ, на предмет змісту інформації, яка стосується особистого життя. Дані, що стосуються сфери особистого життя, не повинні використовуватися та мають бути негайно знищені. Процес накопичення даних та їх знищення має бути належним чином задокументовано.

Для здійснення прихованого проникнення може бути використано спеціальне програмне забезпечення, наприклад, Überwachungs-software (“програмне забезпечення для моніторингу”).

Важливим аспектом прихованого проникнення до інформаційно-технічної системи є те, що про здійснення цього заходу згідно з § 20w Закону “Про федеральне управління кримінальної поліції та співробітництво федерації і земель за кримінальними справами” необхідно повідомити осіб, щодо яких він проводився.

Допоміжну функцію у процесі проведення оперативно-розшукових заходів шляхом використання кіберпростору у ФРН виконують інформаційні системи спеціальних служб NADIS (Nachrichtendienstliches Informationssystem) та поліції INPOL [2].

Разом з тим, слід зазначити, що німецькі правозахисники та спеціалісти з комп’ютерної безпеки вбачають у ситуації, що склалася, певну небезпеку порушення прав і свобод [3]. Так, фахівці із Спілки комп’ютерних експертів і професіональних хакерів Chaos Computer Club (CCC) проаналізували код “бундестроянця” та виклали результати аналізу у своєму звіті [4]. Виявилось, що можливості цих програм значно ширші, ніж заявлялося офіційно. Наприклад, з’ясувалося, що “бундестроянці” можуть не просто спостерігати за поточним спілкуванням користувача та зчитувати його, але й встановлювати на комп’ютер, за яким ведеться спостереження, додаткові програмні модулі. Ці модулі дозволяють сканувати жорсткий диск, а також дистанційно керувати мікрофоном, відеокамерою та клавіатурою.

Більше того, програма дозволяє приховано інсталювати на комп’ютер підозрюваного дані, які можуть слугувати доказом його вини. Особливу увагу фахівців з ССС привернуло те, що функція встановлення додаткових модулів у коді “троянця” прихована особливо ретельно. Як вважають правозахисники, не виключено, що розробники знали про те, які можливості вона дає та що це йде всупереч закону.

Отже, як бачимо, не зважаючи на чітко прописані процедури застосування технологій кіберстеження, у німецьких правозахисників все ще залишаються обґрунтовані побоювання щодо можливості порушення гарантованих Конституцією прав і свобод при застосуванні “бундестроянця”.

З огляду на розглянутий вище досвід застосування шпигунських програм правоохоронними органами ФРН, цікавим є також досвід правоохоронних органів США (насамперед – ФБР) щодо застосування кібертехнологій при розслідуванні злочинів.

Правило 41 Федеральних правил кримінальних процедур [5] визначає процедуру отримання ФБР або іншим федеральним правоохоронним органом США дозволу на негласне отримання інформації з електронних пристроїв. Разом з тим, як повідомляє “The Wall Street Jornal” [6], ФБР офіційно не розкриває деталей своєї діяльності, але інформацію можна зібрати по уривчастих відомостях з судових рішень та з інтерв’ю колишніх і нинішніх агентів. Наприклад, в одному з судових документів згадується, що агенти ФБР просили дозволу суду на здійснення фотозйомки із зараженого комп’ютера, але суддя не дозволив, побоюючись, що в кадр потраплять люди, які не мають відношення до розслідування.

Перший відомий комп’ютерний інструмент спостереження ФБР був сніфером трафіку (від англ. to sniff – “нюхати”) під назвою Carnivore, який встановлювався на мережевих магістралях за дозволу постачальників Інтернет-послуг [7]. Починаючи з 1998 року ФБР використало його приблизно 25 разів, доки громадськість дізналася про це в 2000 році внаслідок розголосу, якого набула відмова провайдера Earthlink дозволити ФБР встановити інструмент у своїй мережі. Earthlink побоювався, що сніффер надасть ФБР необмежений доступ до всіх комунікацій з клієнтами. ФБР наполягав, що його прецизійні фільтри не дозволяють збирати щось, окрім цільових повідомлень. Але незалежний огляд Carnivore виявив, що при неправильному налаштуванні система могла збирати “зайву інформацію”, крім того, система мала дуже низький рівень захисту.

Слід зазначити, що, перехоплюючи мережевий трафік, Carnivore не мав змоги прочитати зашифровані повідомлення. Отже, для розшифровки ФБР було вимушене застосовувати додаткові інструменти, наприклад, так звані “клавіатурні шпигуни” або “кейлоггери” (англ. – keylogger) для перехоплення паролів. У 1999 році під час розслідування діяльності організованого злочинного угруповання необхідно було перехопити Інтернет-листування одного з ватажків цього угруповання, Нікодемо Сальваторе Сарво (Nicodemo Salvatore Scarfo), який використовував шифрування для захисту своїх повідомлень. Щоб прочитати ці повідомлення, ФБР встановило на його комп'ютері кейлоггер. Причому на відміну від сучасних систем, які можна встановлювати віддалено, агентам ФБР довелося двічі фізично проникнути до офісу Сарво: для встановлення кейлоггеру та для отримання перехопленої ним інформації. Слід зазначити, що отримання віддаленого контролю за комп’ютером Сарво на той час було неможливо внаслідок декількох причин, однією з яких було те, що Сарво для доступу до мережі Інтернет використовував комутоване з’єднання.

У 2001 році стало відомо про новий інструмент ФБР для перехоплення паролів – Magic Lantern, який можна було встановлювати віддалено та який, окрім натиснення

клавіш, фіксував історію веб-перегляду, усі відкриті на комп’ютері порти, а також імена користувачів та збережені паролі. Вважається, що Magic Lantern вперше був використаний в операції Trail Mix під час розслідування у відношенні групи з прав тварин у 2002 та 2003 роках.

У 2009 році стало відомо про ще один інструмент спостереження – CIPAV (від Computer and Internet Protocol Address Verifier – верифікатор комп’ютера та адреси Інтернет-протоколу), призначений для збирання IP-адреси та MAC-адреси комп'ютера, інвентаризації всіх відкритих портів та програмного забезпечення, встановленого на комп’ютері, а також інформацію з системного реєстру, ім’я користувача та останню URL-адресу, відвідану з даного комп’ютера. Всі ці дані відправлялися до ФБР через мережу Інтернет. Тим не менш, CIPAV не мав функціоналу кейлоггера і не перехоплював інформацію з каналів зв’язку.

Цей інструмент у 2004 році допоміг ідентифікувати вимагача, який пошкоджував телефонні та Інтернет-кабелі, і щоб припинити цю протиправну діяльність, вимагав грошей від телекомунікаційних операторів. У 2007 році CIPAV був використаний для ідентифікації підлітка, який надіслав електронною поштою повідомлення про замінування середньої школи штату Вашингтон. Щоб заразити комп’ютер підозрюваного підлітка, ФБР змусило його завантажити спеціальний програмний засіб, розмістивши посилання (файл формату “pdf”) в приватній кімнаті чату облікового запису MySpace. Посилання було для фальшивої статті Associated Press, яка мала на меті повідомити про загрозу бомби. Згодом цей же інструмент був використаний у різних інших випадках розслідувань, починаючи від хакерських атак до проявів тероризму та шпигунства, для основної мети – ідентифікувати IP-адресу комп’ютерів зловмисників, які використовували різні способи анонімізації своїх дій в Інтернеті для того, щоб приховати свою особу та місцезнаходження.

У 2012 році ФБР починає використовувати новий спосіб атак, відомий під назвою “водопій” (англ. – watering hole attack). Ця атака передбачає впровадження шпигунських програм на веб-сайт, де збираються підозрювані у вчиненні злочину, внаслідок чого заражаються комп’ютери всіх відвідувачів сайту. Федеральні агенти часто та успішно використовували зазначену атаку для викриття відвідувачів веб-сайтів з дитячою порнографією. Зазвичай ці сайти розміщуються в анонімній мережі Tor, доступ до якої можна отримати лише за допомогою його спеціалізованого браузера, який приховує реальну IP-адресу користувачів. Першим відомим випадком застосування атаки “водопій” є операція “Торпедо”, спрямована на розкриття анонімних відвідувачів трьох дитячих порнографічних сайтів, розміщених на серверах штату Небраска у 2012 році. А в 2013 році ця тактика була застосована у відношенні постачальника послуг анонімного веб-хостингу Freedom Hosting, на серверах якого розміщувалися серед інших і сайти з дитячою порнографією. У серпні 2013 року, після того як ФБР захопило контроль над серверами Freedom Hosting, всі розміщені на них сайти відображали сторінку “Down for Maintenance” з вбудованим в неї прихованим кодом Javascript. Код використовував одну з вразливостей Firefox, щоб примусити заражені комп'ютери виявити свою реальну IP-адресу для ФБР. Тим не менш, була одна проблема з тактикою. Хостинг Freedom – це не лише розміщення дитячих порнографічних сайтів, на ньому також розміщувалися ресурси непричетних до злочинної діяльності організацій та осіб, які також могли бути ураженими “федеральним” ШПЗ.

У 2015 році ФБР та його міжнародні партнери використовували аналогічну тактику, щоб виявити більше 4000 машин, що належали членам і майбутнім членам дитячого порнографічного сайту Playpen. Як і в попередніх випадках, агенти ФБР

перехопили управління над серверами й продовжили підтримувати роботу сайту на протязі приблизно двох тижнів. Правоохоронці розмістили на Playpen певний програмний засіб, завдяки якому стало можливим встановити реальні IP-адреси відвідувачів [8]. Таким чином, не дивлячись на захист анонімності в мережі Tor, агенти ФБР змогли виявити реальні IP-адреси приблизно 1300 користувачів даного ресурсу, що призвело до понад 200 кримінальних переслідувань [9]. Зрештою, приблизно 137 особам було пред’явлено звинувачення у злочинах. Однак під час судових слухань адвокати одного з затриманих Джея Мічо (Jay Michaud) зажадали від сторони обвинувачення розкрити спосіб, за допомогою якого був встановлений їх підзахисний. Але ФБР відмовилось надавати цю інформацію, посилаючись на таємність технології (у справі ця технологія фігурує під загальною назвою “мережева слідча техніка”, англ. – network investigative technique, скорочено NIT). Як наслідок, Міністерство юстиції США відмовилося від обвинувачень. Ще декілька обвинувачених успішно опротестували свій арешт на підставі того, що вони жили за межами території, зазначеної в ордері на негласне отримання інформації. До речі, останнє стало одним з приводів для внесення змін до Правила 41 у 2016 році, розширюючи права суддів на дачу ордера на всю територію США [10].

На відміну від ФБР, інші американські спецслужби, ЦРУ, АНБ та кіберпідрозділи армії США, а так само британська MI5, не виконують правоохоронних функцій, а отже, добута ними інформація, як правило, не використовується в якості доказової бази під час судових процесів. Саме це, а також інші особливості специфіки їх роботи, на нашу думку, обумовили майже повну відсутність публічно доступної інформації про застосовувані ними “хакерські” технології. У пресу потрапляють лише окремі витоки інформації, наприклад [11 – 14], які, як правило, недостатні для проведення об’єктивного дослідження. Разом з тим, інформація про окремі випадки застосування ШПЗ західними спецслужбами свідчить про можливості використання цих програм не лише для отримання інформації (тобто, для розвідувальних цілей), але й для застосування їх в якості “кіберзброї” для проведення кібердиверсій чи кібертерактів [15].

У вітчизняному кримінально-процесуальному законодавстві така негласна слідча (розшукова) дія регламентується статтею 264 КПК України: “Зняття інформації з електронних інформаційних систем” [16]. Відповідно до положень цієї статті пошук, виявлення і фіксація відомостей, що містяться в електронній інформаційній системі або їх частин, доступ до електронної інформаційної системи або її частини, а також отримання таких відомостей без відома її власника, володільця або утримувача може здійснюватися на підставі ухвали слідчого судді, якщо є відомості про наявність інформації в електронній інформаційній системі або її частині, що має значення для певного досудового розслідування. Не потребує дозволу слідчого судді здобуття відомостей з електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володільцем або утримувачем або не пов’язаний з подоланням системи логічного захисту. В ухвалі слідчого судді про дозвіл на втручання у приватне спілкування в цьому випадку додатково повинні бути зазначені ідентифікаційні ознаки електронної інформаційної системи, в якій може здійснюватися втручання у приватне спілкування.

Відповідно до ст. 256 КПК України результати зняття інформації з електронних інформаційних систем можуть використовуватися для надання доказів на тих самих підставах, що і результати проведення інших слідчих (розшукових) дій під час досудового розслідування.

На перший погляд здається, що процедура досить детально прописана, її проведення та використання результатів не повинно викликати труднощів. Разом з тим, під час даної процедури в окремих випадках може бути застосоване програмне забезпечення, яке за усіма ознаками відноситься до шкідливого, оскільки фактично призначене для несанкціонованого користувачем (підозрюваним) втручання в роботу його електронно-обчислювальної машини (комп’ютера). З одного боку, німецький та американський досвід вказує на ефективність застосування такого програмного забезпечення при розслідуванні як кіберзлочинів, так і інших протиправних діянь. З іншого боку, застосування такого шкідливого програмного забезпечення у правоохоронних цілях на даний час вітчизняним законодавством не врегульовано. Отже, законність застосування компетентними органами зазначеного програмного забезпечення можна піддати сумніву.

Другою проблемою є те, що цифрова інформація може бути відносно легко сфальсифікована, не залишаючи при цьому слідів фальсифікації. Останній момент є дуже суттєвим в рамках захисту прав і свобод людини, особливо якщо цифрова доказова інформація здобувається негласно. Це обумовлено, тим, що особа, відносно якої проводяться такі негласні (розшукові) дії, має значно обмежені можливості вжити законних заходів захисту. Зокрема, відповідне письмове повідомлення про факт і результати негласної слідчої (розшукової) дії повинне бути здійснене протягом дванадцяти місяців з дня припинення таких дій, але не пізніше звернення до суду з обвинувальним актом. Крім того, сторона захисту може піддати сумніву об’єктивність даних, добутих за допомогою ШПЗ та висунути вимогу дослідити це ШПЗ із залученням сторонніх (для об’єктивності) експертів. Разом з тим, ШПЗ, що застосовуються правоохоронними органами та/чи спецслужбами, як правило, мають гриф обмеження доступу. Отже, може скластися ситуація, подібна до описаної вище, коли ФБР вимушене було зняти обвинувачення проти Джея Мічо.

Як бачимо, як у ФРН, так і в США основні побоювання правозахисників пов’язані з можливістю зловживань з боку правоохоронців. Актуальною ця проблема є і для України. Співробітники правоохоронних органів, користуючись прихованістю кіберстеження, матимуть можливість отримувати відносно підозрюваного інформацію, яка не стосується розслідуваного злочину чи правопорушень взагалі (наприклад, якась особиста інформація, у тому числі, інтимного характеру). Або під час стеження за одним суб'єктом може бути отримана інформація щодо приватного життя інших, сторонніх осіб, непричетних до вчинення злочину. Або (це, мабуть, один з найгірших варіантів) правоохоронці можуть “підкинути” на комп’ютер підозрюваного докази його “вини”, тим самим звинувативши невинну особу. В цілому варіантів зловживань багато, а контроль над діями правоохоронців значно ускладнений прихованістю зазначених негласних заходів.

Висновки.

У зв’язку з викладеним, на наш погляд, дуже важливою є фіксація процесу негласного отримання інформації з електронних інформаційних систем, а також відповідне закріплення (реєстрація) отриманих відомостей. Це питання врегульоване статтею 252 КПК України “Фіксація ходу і результатів негласних слідчих (розшукових) дій”.

Проте, по-перше, весь процес пошуку, виявлення та вилучення доказової інформації повинен фіксуватися засобами об’єктивного контролю (наприклад, за допомогою відеозапису екрану комп’ютера співробітника правоохоронного органу, який керує ШПЗ, впровадженим на комп’ютер підозрюваного). Крім того, весь процес роботи програмного забезпечення, що керує зазначеним ШПЗ, та самого ШПЗ повинен ретельно логіюватися.

По-друге, задля підтвердження дійсності здобутої за допомогою ШПЗ інформації доцільно, на наш погляд, використовувати можливості електронного цифрового підпису (далі – ЕЦП). Причому захисту за допомогою ЕЦП повинна підлягати як сама вилучена доказова інформація, так і інформація об’єктивного контролю. Це дозволить запобігти змінам цифрової доказової інформації та унеможливить фальсифікацію інформації засобів об’єктивного контролю, дозволить ідентифікувати посадову особу, яка зафіксувала та вилучила отриману негласним шляхом інформацію і підписала її, а також час підписання.

Зауважимо, що з технічної точки зору реалізувати об’єктивний контроль процесу негласного застосування ШПЗ та захист матеріалів за допомогою ЕЦП цілком можливо. Такі технології в Україні існують, їх потрібно лише адаптувати для потреб оперативних підрозділів. Що стосується юридичних аспектів, то і в цьому плані практика застосування електронного цифрового підпису не нова для українського законодавства (це, перш за все, Закони України “Про електронний цифровий підпис” та “Про електронні документи та електронний документообіг”).

Разом з тим, можливість застосування ЕЦП у кримінальному процесі досі не регламентована, як не регламентована й можливість застосування засобів об’єктивного контролю дій оперативних працівників.

Слід наголосити, що, на наш погляд, застосування ЕЦП у кримінальному процесі буде корисним не лише у розглянутому випадку негласного кіберспостереження, а у всіх випадках, коли у справі фігурують цифрові докази.

Використана література

1. Бундестаг принял спорный закон о наблюдении за мессенджерами / Deutsche Welle. – Режим доступу : http://www.dw.com/ru/бундестаг-принял-спорный-закон-о-наблюдении-за-мессенджерами/a-39384123

2. Манжай О.В. Досвід Великобританії, ФРН та КНР. – (Навчально-тренувальний центр боротьби з кіберзлочинністю та моніторингу кіберпростору на громадських засадах). – Режим доступу : http://cybercop.in.ua/index.php/naukovi-statti/80-naukovi-statti/201-dosvid-velikobritaniji-frn-ta-knr

3. Спецслужба в смартфоне : в ФРГ резко критикуют новый закон о слежке / Deutsche Welle. – Режим доступу : http://www.dw.com/ru/спецслужба-в-смартфоне-в-фрг-резко-критикуют-новый-закон-о-слежке/a-39389583

4. Фатальный “бундестроянец”, или как немецкие власти подорвали к себе доверие / Deutsche Welle. – Режим доступу : http://www.dw.com/ru/фатальный-бундестроянец-или-как-немецкие-власти-подорвали-к-себе-доверие/a-15449570

5. Federal Rules of Criminal Procedure. – Режим доступу : https://www.federalrulesofcriminalprocedure.org

6. FBI Taps Hacker Tactics to Spy on Suspects / The Wall Street Jornal. – Режим доступу : https://www.wsj.com/articles/SB10001424127887323997004578641993388259674

7. Everything we know about how the fbi hacks people / WIRED. Режим доступу : https://www.wired.com/2016/05/history-fbis-hacking

8. ФБР сняло обвинения с педофила, чтобы не раскрывать исходники своей малвари / Хакер. – Режим доступу : https://xakep.ru/2017/03/07/michaud-case-dropped

9. Child porn case dropped to prevent FBI disclosure / BBC. – Режим доступу : http://www.bbc.com/news/technology-39180204

10. FBI’s New Hacking Powers Take Effect This Week / FORTUNE. – Режим доступу : http://fortune.com/2016/11/30/rule-41

11. WikiLeaks Reveals 'Athena' CIA Spying Program Targeting All Versions of Windows / The Hacker News. – Режим доступу : http://thehackernews.com/2017/05/athena-cia-windows-hacking.html

12. C.I.A. Developed Tools to Spy on Mac Computers, WikiLeaks Disclosure Shows / The New York Times. – Режим доступу : https://www.nytimes.com/2017/03/23/technology/cia-spying-mac-computers-wikileaks.html

13. HOW THE NSA'S FIRMWARE HACKING WORKS AND WHY IT'S SO UNSETTLING / WIRED. – Режим доступу: https://www.wired.com/2015/02/nsa-firmware-hacking

14. Wikileaks claims MI5 and CIA developed spyware to turn televisions and smart phones into bugs / The Telegraph. – Режим доступу : http://www.telegraph.co.uk/news/2017/03/07/wikileaks-claims-mi5-cia-developed-spyware-turn-samsung-tvs

15. Кибератаки : вирус-диверсант Stuxnet в ядерной энергетической программе Ирана. – Часть 1 / Наука и техника. – Режим доступу : http://naukatehnika.com/kiberataki-virus-diversant-stuxnet-v-yadernoj-energeticheskoj-programme-irana-chast1.html

16. Кримінальний процесуальний кодекс України : Закон України від 13.04.12 р. // Відомості Верховної Ради України (ВВР). – 2013. – № 9-10, № 11-12, № 13. – Ст. 88.

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~