УДК 343
DOI https://doi.org/10.32841/2307-1745.2022.56.23

Ковальова О. В.,
кандидат юридичних наук,
завідувач кафедри оперативно-розшукової діяльності
та інформаційної безпеки факультету № 3
Донецького державного університету внутрішніх справ

КІБЕРДОСТУПНІСТЬ ТА ЗАХИСТ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО ДОКАЗІВ ЯК ОСНОВНИЙ СТАНДАРТ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ДОСУДОВОГО РОЗСЛІДУВАННЯ ЗАРУБІЖНИХ КРАЇН

Анотація. В статті розглядається кібердоступність та захист від несанкціонованого доступу до доказів як основний стандарт інформаційного забезпечення досудового розслідування зарубіжних країн. Автор вказує, що на сьогоднішній день зарубіжні держави мають достатньо позитивний досвід у сфері інформаційного забезпечення досудового розслідування кримінальних правопорушень. Останнє пояснюється їх активним розвитком та прогресивним підходом до кримінально-правової та процесуальної політики. На сьогоднішній день зарубіжні країни мають не тільки виважену та налагоджену нормативно-правову базу, але і достатньою кількість техніки, необхідної для здійснення своєчасної пошукової та аналітичної слідчо-розшукової діяльності. Особлива увага приділяється Німеччині та США, а також вказується, що процес накопичення та використання інформації в цих країнах має бути задокументовано. Використання програмного масиву для доступу до певної інформації має бути не тільки проведене відповідно до нормативно-правових актів, але і після повідомлення осіб, у відношенні яких воно застосовується. Звертається увага на те, що правоохоронні органи США більш ретельно підходять як до збору доказової інформації, так і до захисту прав та свобод своїх громадян. Більше того, в країні враховуються не тільки інтереси кримінальних правопорушників та потерпілих, але і власне правоохоронних органів. Саме з метою спрощення роботи останніх, скорочення термінів досудового розслідування в країні ведеться плідна робота над створенням шляхів удосконалення рівня інформаційного забезпечення досудового розслідування.

Підсумовується, що в межах досліджуваного стандарту інформаційне забезпечення у зарубіжних країнах поділяється на такі види як: 1) *техніко-криміналістичне забезпечення* – технічні засоби та прилади, необхідні для здійснення судово-експертної діяльності в межах кримінального провадження з наступним створенням інформаційного масиву; 2) *інформаційно-довідкове та методичне забезпечення* – наукова література, в якій викладені особливості та алгоритми проведення досудового розслідування; 3) *інформаційно-аналітичне та загально-технічне забезпечення* – засоби та прилади, необхідні для вирішення загальних проблем та завдань досудового розслідування.

Ключові слова: досудове розслідування, кібердоступність, інформаційне забезпечення, несанкціонований доступ, кримінальне правопорушення, зарубіжні держави, програмне забезпечення.

Постановка проблеми. На сьогоднішній день зарубіжні держави мають достатньо позитивний досвід у сфері інформаційного забезпечення досудового розслідування кримінальних правопорушень. Останнє пояснюється їх активним розвитком та прогресивним підходом до кримінально-правової та процесуальної політики. На сьогоднішній день зарубіжні країни мають не тільки виважену та налагоджену нормативно-правову базу, але і достатньою кількість техніки, необхідної для здійснення своєчасної пошукової та аналітичної слідчо-розшукової діяльності. Таким чином, виходячи із вказаного, вважаємо за доцільне зупинитись на цьому питанні більш детально з метою виокремлення найбільш сучасних підходів до інформаційного забезпечення досудового розслідування суспільно небезпечних діянь з метою імплементації позитивного досвіду в українську кримінальну процесуальну діяльність.

Мета. Метою статті є розгляд кібердоступності та захисту від несанкціонованого доступу до доказів як основних стандартів інформаційного забезпечення досудового розслідування зарубіжних країн.

Аналіз наукових публікацій. Окремі аспекти особливостей інформаційного забезпечення досудового розслідування у зарубіжних країнах було розглянуто у працях І.В. Арістової, О.М. Бандурки, В.М. Брижко, В.І. Галагана, В.О. Глушкова, В.Г. Лукашевича, Є.Д. Лук'янчикова, А.М. Новицького, О.В. Олійника, Ю.В. Попова, В.М. Росоловського, О.С. Саінчина, Д.Я. Семир'янова, І.С. Стаценко-Сургучової, Л.В. Трофімової, В.С. Цимбалюка, В.Ю. Шепітька та інших вчених.

Виклад основного матеріалу. Відтак, «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]. Таким чином, законодавцем Німеччини було створено умови для застосування необмеженого кібердоступу до певного кола інформації, необхідної для доказування та досудового розслідування взагалі.

«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 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» [2, с. 109]. Варто також звернути увагу на те, що процес накопичення та використання інформації має бути задокументовано. В країні з цією метою використовується спеціальне програмне забезпечення, призначене для моніторингу. Цікавим фактом також є те, що використання програмного масиву для доступу до певної інформації має бути не тільки проведене відповідно до нормативно-правових актів, але і після повідомлення осіб, у відношенні яких воно застосовується.

«Допоміжну функцію у процесі проведення оперативно-розшукових заходів шляхом використання кіберпростору у ФРН виконують інформаційні системи спеціальних служб NADIS (Nachrichtendienstliches Informationssystem) та поліції INPOL» [3]. «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» [4]. «Так, фахівці із Спілки комп'ютерних експертів і професіональних хакерів Chaos Computer Club (CCC) проаналізували код «бундестроянця» та виклали результати аналізу у своєму звіті» [5]. «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 CCC 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, 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»» [1, с. 110]. Таким чином, можна сказати, що не дивлячись на теоретично корисну програму, котра сприяє збору та наступному використанню доказової інформації спеціально уповноваженими особами, фактично на практиці часто виникають ситуації, коли така програма може бути використана з метою посягання на доказовий електронний документообіг. Останнє свідчить про те, що на сьогоднішній день навіть у зарубіжних країнах в межах інформаційного забезпечення досудового розслідування не завжди дотримуються прав та свобод людини та громадянина.

«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» [6] «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»» [7], «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» [8]. Варто звернути увагу на те, що правоохоронні органи США більш ретельно підходять як до збору доказової інформації, так і до захисту прав та свобод своїх громадян. Більше того, в країні враховуються не тільки інтереси кримінальних правопорушників та потерпілих, але і власне правоохоронних органів. Саме з метою спрощення роботи останніх, скорочення термінів досудового розслідування в країні ведеться плідна робота над створенням шляхів удосконалення рівня інформаційного забезпечення досудового розслідування.

«Починаючи з 1998 року ФБР використало Carnivore 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» [1, с. 111]. Отже, як свідчить практика, як і у Німеччині, у США, не дивлячись на їх виваженість та принциповість, також є прогалини у роботі засобів інформаційного забезпечення, котрі можуть негативно відбитися не тільки на результатах досудового розслідування, а і на іміджі самих правоохоронних органів.

«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» [1, с. 112]. Отже, основним алгоритмом створення програм для удосконалення інформаційного забезпечення досудового розслідування у США є розробка програм, котрі фактично «ламають» комп'ютерну систему та імплементуються у роботу останньої.

«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 вебсайт, 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» [1, с. 112]. Таким чином ФБР створює програми, котрі надають можливість отримати необмежений доступ до комп'ютерів користувачів, які підозрюються у вчиненні кримінальних правопорушень або у співучасті. Варто також звернути увагу на те, що аналогічні алгоритми, закладені в базу таких програм також часто використовуються хакерами для кібератак та отримання несанційонованого доступу до персональних даних 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» [9]. «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» [10]. Що стосується пошуку та отримання інформації в контексті розслідування фактів створення сайтів із дитячою порнографією, маємо зауважити, що такого роду програми є дуже корисними, оскільки вони не тільки надають можливість отримати доступ до такого сайту, а і встановити дані, необідні для розшуку підозрюваних осіб та доказування їх причетності до цих кримінальних правопорушень.

«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» [11]. «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 обумовили майже повну відсутність публічно доступної інформації про застосовувані ними «хакерські» технології. У пресу потрапляють лише окремі витоки інформації, наприклад» [12-14], «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]. Таким чином, ми можемо стверджувати, що такого роду програми можуть не тільки сприяти отриманню інформації, необхідної для позитивного завершення досудового розслідування, а і навпаки – порушувати нормальний алгоритм останнього.

«Варто звернути увагу на те, що 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» [1, с. 110]. Отже, в українському законодавстві основна увага акцентується на першочерговому захисті прав та свобод громадян країни, особливо – захисті персональних даних, у зв'язку із чим було передбачено спеціальну процедуру отримання дозволу на вилучення певної інформації.

Висновки. Таким чином, проведене дослідження дозволило підсумувати, що в межах вказаного стандарту інформаційне забезпечення у зарубіжних країнах поділяється на такі види як: 1) *техніко-криміналістичне забезпечення* – технічні засоби та прилади, необхідні для здійснення судово-експертної діяльності в межах кримінального провадження з наступним створенням інформаційного масиву; 2) *інформаційно-довідкове та методичне забезпечення* – наукова література, в якій викладені особливості та алгоритми проведення досудового розслідування; 3) *інформаційно-аналітичне та загально-технічне забезпечення* – засоби та прилади, необхідні для вирішення загальних проблем та завдань досудового розслідування.

Література:

1. Бундестаг принял спорный закон о наблюдении за мессенджерами / Deutsche Welle. URL: http://www.dw.com/ru/бундестаг-принял-спорный-закон-о-наблюдении-за-мес сенджерами/a-39384123
2. Нізовцев Ю.Ю., Леонов Б.Д. Використання кібертехнологій у процесі розслідування злочинів: аналіз зарубіжного досвіду. *Інформація і право*. 2017. № 3. С. 108–116.
3. Манжай О.В. Досвід Великобританії, ФРН та КНР. (Навчально-тренувальний центр боротьби з кіберзлочинністю та моніторингу кіберпростору на громадських засадах). URL: http://cybercop.in.ua/index.php/naukovi-statti/80-naukovi-statti/201-dosvid-velikobritanijifrn-ta-knr
4. Спецслужба в смартфоне : в ФРГ резко критикуют новый закон о слежке. *Deutsche Welle*. URL: http://www.dw.com/ru/спецслужба-в-смартфоне-в-фрг-резко-критикуют-новый-закон-о-слежке/a-39389583
5. Фатальный «бундестроянец», или как немецкие власти подорвали к себе доверие. *Deutsche Welle*. URL: http://www.dw.com/ru/фатальный-бундестроянец-или-какнемецкие-власти-подорвали-к-себе-доверие/a-15449570
6. Federal Rules of Criminal Procedure. URL: https://www.federalrulesofcrim inalprocedure.org
7. FBI Taps Hacker Tactics to Spy on Suspects. *The Wall Street Jornal.* URL: https://www.wsj.com/articles/SB10001424127887323997004578641993388259674
8. Everything we know about how the fbi hacks people. *WIRED*. URL: https://www.wired.com/2016/05/history-fbis-hacking
9. ФБР сняло обвинения с педофила, чтобы не раскрывать исходники своей малвари. *Хакер.* URL: https://xakep.ru/2017/03/07/michaud-case-dropped

10. Child porn case dropped to prevent FBI disclosure. *BBC*. URL: http://www.bbc.com/news/technology-39180204
11. FBI's New Hacking Powers Take Effect This Week. *FORTUNE*. URL: http://fortune.com/2016/11/30/rule-41
12. C.I.A. Developed Tools to Spy on Mac Computers, WikiLeaks Disclosure Shows. *The New York Times*. URL: https://www.nytimes.com/2017/03/23/technology/cia-spying-maccomputers-wikileaks.html
13. How the NSA'S firmware hacking works and why it's so unsettling. *WIRED*. URL: 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*. URL: http://www.telegraph.co.uk/news/2017/03/07/wikileaksclaims-mi5-cia-developed-spyware-turn-samsung-tvs
15. Кибератаки : вирус-диверсант Stuxnet в ядерной энергетической программе Ирана. Часть 1. Наука и техника. URL: http://naukatehnika.com/kiberataki-virus-diversantstuxnet-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.

Kovalova O. Cyber accessibility and protection against unauthorized access to evidence as the basic standard of information support for pre-trial investigation in foreign countries

Summary. The article considers cyber availability and protection against unauthorized access to evidence as the main standard of information support of pre-trial investigation of foreign countries. The author points out that today foreign countries have quite positive experience in the field of information support of pre-trial investigation of criminal offenses. The latter is explained by their active development and progressive approach to criminal law and procedural policy. Today, foreign countries have not only a balanced and well-established regulatory framework, but also a sufficient amount of equipment needed for timely search and analytical investigative activities. Special attention is paid to Germany and the United States, and it is pointed out that the process of collecting and using information in these countries should be documented. The use of software to access certain information should not only be carried out in accordance with regulations, but also after notifying the persons to whom it applies. Attention is drawn to the fact that US law enforcement agencies are more careful both in gathering evidence and in protecting the rights and freedoms of their citizens. Moreover, the country takes into account not only the interests of criminal offenders and victims, but also the law enforcement agencies themselves. It is in order to simplify the work of the latter, to reduce the time of pre-trial investigation in the country is fruitful work to create ways to improve the level of information support of pre-trial investigation. It is concluded that within the studied standard information support in foreign countries is divided into such types as: 1) technical and forensic support – technical means and devices necessary for forensic activities in criminal proceedings with the subsequent creation of an information array; 2) information and methodological support and methodological support – scientific literature, which sets out the features and algorithms of pre-trial investigation; 3) information-analytical and general-technical support – means and devices necessary for solving general problems and tasks of pre-trial investigation.

Key words: pre-trial investigation, cyber-availability, information support, unauthorized access, criminal offense, foreign countries, software.