УДК 343.92
DOI https://doi.org/10.32850/sulj.2021.4.4

ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ: ОПЕРАТИВНО-РОЗШУКОВІ ЗАХОДИ ПРОФІЛАКТИКИ DDOS ТА СПАМУ І ЗАПОБІГАННЯ НИМ

Воронов І. О.

У статті йдеться про необхідність урахування сучасних форм кіберзлочинності для здійснення ефективної профілактики й запобігання в аспекті її форм.

З урахуванням усієї суспільної небезпеки, що несуть такі кримінальні правопорушення, існує пряма необхідність удосконалення наявної системи профілактики кримінальних правопорушень та запобігання ним, а також її заходів, зокрема кримінологічних, процесуальних та оперативно-розшукових.

У межах дослідження проаналізовано сучасні заходи профілактики кримінальних правопорушень і запобігання ним.

Сучасний етап розвитку світової інформаційної спільноти характеризується інтенсивним розвитком процесів інформатизації, широким їх впровадженням у всі сфери людської діяльності. Визначальною рисою цих явищ є постійне збільшення числа суб'єктів – користувачів, залучених у ці процеси. З таких суб'єктів формуються потенційні злочинці або потенційні жертви. Ситуація в Україні за останні роки характеризується наявністю вкрай негативної і дуже стійкої тенденції до змін у структурі злочинності.

Увага фокусується на історії ботнетів, яка тісно пов'язана з появою і розвитком так званих троянських програм, які активно використовувалися для прихованого збору даних.

Взаємодія між складовими комп'ютерами мережі ботнет відбувається за допомогою мережевих протоколів, типи яких є підставою для їх класифікації.

За типом архітектури ботмережі поділяються на мережі з єдиним центром управління та децентралізовані, що використовуються для здійснення широкого спектру завдань. Керівником (адміністратором) потужних ботнетів з понад 100 тисяч фейкових облікових записів виступає одна людина. Окрім кібератак і зламування сайтів також здійснюється підбір паролів до скриньок електронної пошти на віддалених платформах.

Визначено, що замовники перебувають на закритих форумах та у чатах Telegram, а розрахунки здійснюються через електронні платіжні системи (навіть ті, які заборонені в Україні).

Ключові слова: *профілактика, запобігання, кримінальні правопорушення, процесуальні заходи, оперативно-розшукові заходи.*

Voronov I. O. Combating cybercrime: operational and investigative measures to prevent and avert DDoS and spam

The article presents the modern forms of cybercrimes for effective prevention and prediction in aspect of its forms.

Taking into account all the public danger posed by criminal offenses, there is a direct need to improve the existing system of prevention and prevention of criminal offenses, as well as its measures: criminological, criminal procedure and operational search.

Within the framework of this research, modern criminal procedure and operative-search measures of prevention and prevention of criminal offenses are analyzed.

The current stage of development of the world information community is characterized by the intensive development of informatization and their widespread implementation in all spheres of human activity. A distinctive feature of these phenomena is the constant increase in the number of actors – users involved in these processes. With such actors potential criminals or potential victims are formed. Situation in Ukraine in recent years is characterized by an extremely negative and very stable trend towards changes in the structure of crime.

Attention is focused on the history of Botnet, which has close connection with emergence and development of so called Trojans, which were actively used for covert data collection.

The interaction between the constituent computers of the Botnet is carried out using network protocols, the types of which are the basis for their classification.

According to the type of architecture, botnets are divided into networks with a single control center or decentralized, which used to perform a wide range of tasks. One person can be the manager (administrator) of powerful botnets with more than 100,000 fake accounts. In addition to cyber-attacks and hacking, passwords are also selected for e-mail accounts on remote platforms.

It is stated that clients based in closed forums and chats of Telegram, and payments are made through electronic payment systems (some of which are prohibited in Ukraine).

Key words: *prevention, prediction, criminal offenses, criminal-procedural measures, operative-search measures.*

Постановка проблеми та її актуальність. Припинити існування злочинів у сфері високих інформаційних технологій неможливо, оскільки суспільство вже не в змозі відмовитися від сучасних здобутків. Нація, яка від них відмовиться, ризикує загальмуватися у власному розвитку. Саме тому необхідно враховувати паралельність таких процесів, як розвиток суспільства й розвиток злочинності. Більш того, Україна перебуває на порозі членства до Європейського Союзу, у зв'язку з чим вирішення та врегулювання потребують питання активних форм протидії кіберзлочинності.

Аналіз останніх досліджень і публікацій. Науково-теоретичне підґрунтя дослідження склали праці вчених з теорії оперативно-розшукової діяльності, криміналістики та кримінального процесу, теорії інформації та управління, зокрема роботи К.В. Антонова, В.Д. Берназа, К.І. Бєлякова, В.М. Бутузова, А.Ф. Волобуєва, В.І. Галагана, Ю.М. Грошевого, Е.О. Дідоренка, О.Ф. Долженкова, В.П. Захарова, А.В. Іщенка, А.І. Марущака, С.С. Овчинського, Ю.Ю. Орлова, В.Л. Ортинського, М.А. Погорецького, Б.Г. Розовського, М.Б. Саакяна, М.В. Салтевського, М.Я. Сегая, О.П. Снігерьова, Д.С. Чернавського.

Виклад основного матеріалу. За офіційними статистичними даними Генеральної прокуратури України встановлено, що в період із 2018 по 2020 рр. відзначено високий рівень кіберправопорушень в Україні.

Стан розвитку злочинності у сфері високих інформаційних технологій свідчить про те, що теоретично кожен користувач може стати жертвою злочину. На фоні кризових явищ та посилення структурних деформацій в економіці продовжують поширюватися процеси криміналізації інформаційної сфери суспільства. Започаткувався і не припиняється процес формування злочинних угруповань, до яких втягнені різноманітні фахівці у сфері високих інформаційних технологій. Це зміцнює їх та сприяє отриманню прибутків і легалізації коштів.

Сучасний етап розвитку світової інформаційної спільноти характеризується інтенсивним розвитком процесів інформатизації, широким їх впровадженням у всі сфери людської діяльності. Визначною рисою цих явищ є постійне збільшення числа суб'єктів – користувачів, залучених у ці процеси. Фактично з таких суб'єктів формуються потенційні злочинці або потенційні жертви. Криміногенна ситуація в Україні за останні роки характеризується наявністю вкрай негативної і дуже стійкої тенденції до змін у структурі злочинності. У цьому аспекті В.Д. Берназ справедливо зауважує, що індивідуальна злочинність стрімко поступається груповій, а групова, у свою чергу, швидко переростає в організовану злочинну діяльність [1, с. 24]. Така тенденція спостерігалася також у злочинності у сфері високих інформаційних технологій, але поява та вдосконалення спеціальних програмних засобів спричиняють перерозподіл людського і програмно-технічного фактору на користь останнього.

Можливості комп'ютерів, об'єднаних у мережу, – це не просто сума можливостей кожного з елементів, а набуття нової потужності. Під час об'єднання комп'ютерів у мережу, навіть локальну, користь від такого утворення зростає експоненціально. Ефективність збільшується чи не на порядок. Таким чином, завдяки новим можливостям обсяг і структура знань змінюються і кількісно, і якісно лише за кілька років. Сенс інформаційних технологій полягає саме у їх синергізмі, ефекті об'єднаних можливостей і потенціалів. Інформатизація перш за все характеризується системністю. До речі, слід зауважити, що об'єднання комп'ютерів у мережу здійснювалося для надання широкого доступу користувачів до ресурсів та швидкого обміну даними на великі відстані. Проте це й було використано кримінальними структурами для дистанційного вчинення злочинів, внаслідок чого такі кримінальні діяння набули статусу міжнародного.

Отже, започатковується та відпрацьовується новий принцип злочинної діяльності, згідно з яким можливості одного програмно-апаратного комплексу помножуються на їх кількість. Спочатку необхідна кількість комп'ютерів досягалася за рахунок засобів, які належали членам злочинного угруповання. Виникнення та вдосконалення телекомунікаційних програмних засобів дали можливість одному користувачу встановлювати контроль над великою кількістю комп'ютерів і керувати ними особисто.

Для позначення «захопленої» мережі комп'ютерів використовується термін "botnet", який є скороченим збірним поняттям від англійських слів "robot" і "network" [2, с. 24]. Термін «ботнет» можна вважати загальним поняттям і використовувати у сполученні зі словом «мережа», аналогічно до терміна «мережа Інтернет». У загальному визначенні ботмережа – це субмережа, що виникає внаслідок загальної або часткової мобілізації ресурсів, яка проводиться відкрито або приховано для можливості використання програмно-апаратного комплексу користувачів з певною метою.

В основу створення ботнетів був покладений принцип мережевого адміністрування. Як адміністратор керує певною корпоративною мережею, так і злочинець заради досягнення мети використовує віддалений доступ для керування комп'ютерами, підключеними до неї.

Історія сучасних ботнетів тісно пов'язана з появою і розвитком «троянських» програм, які активно використовувалися для прихованого збору таких даних, як номери кредитних карток, стан грошового рахунку, коди ліцензійного програмного забезпечення, коди доступу до різних послуг [3, с. 55].

Взаємодія між складовими комп'ютерами мережі ботнет відбувається за допомогою мережевих протоколів, типи яких є підставою для їх класифікації. За типом протоколів, що використовуються, мережі ботнет поділяються на такі групи, як IRC-, IM- та web-орієнтовані.

IRC-орієнтовані мережі належать до найперших видів ботнетів, де керування ботами здійснювалося на основі IRC (Internet Relay Chat) – сервісу Інтернет, який дає користувачам можливість спілкування шляхом надсилання текстових повідомлень багатьом кореспондентам з усього світу одночасно (у режимі реального часу). Кожен комп'ютер з'єднувався із зазначеним у тілі програми-бота IRC-сервером, заходив на певний канал і чекав команди від свого хазяїна.

IM-орієнтовані є не дуже популярним видом ботнетів. Вони відрізняються від своїх IRC-орієнтованих аналогів тільки тим, що для передачі даних використовують певні канали IM-служб (Instant Messaging – системи миттєвої передачі повідомлень) (наприклад, AOL, MSN, ICQ). Невисока популярність таких ботнетів зумовлена складнощами, що виникають під час створення окремого акаунта, тобто облікового запису в комп'ютерній системі, як сукупності засобів та прав користувача IM-служби для кожного бота. Річ у тім, що боти повинні виходити в мережу й постійно бути присутніми в онлайн-режимі. Оскільки більшість IM-служб не дає змогу входити до системи з різних комп'ютерів, використовуючи той самий акаунт, кожен бот повинен мати свій номер IM-служби. При цьому власники IM-служб усіляко перешкоджають будь-якій автоматичній реєстрації акаунтів. У результаті цього адміністратори IM-орієнтованих ботнетів значно обмежені в числі наявних зареєстрованих акаунтів, відповідно, й у числі ботів, одночасно присутніх у мережі. Звичайно, боти можуть використати той самий акаунт, виходити в онлайн один раз у певний проміжок часу, відсилати дані на номер хазяїна й протягом короткого проміжку часу очікувати відповіді. Однак це породжувало проблему швидкого реагування на відповідні команди.

Web-орієнтовані – це відносно новий тип ботнетів, що швидко розвиваються завдяки відносній легкості розроблення, великої кількості web-серверів в Інтернеті й простоті керування. Для керування web-орієнтованих ботнетів використовується CGI (від англ. "Common Gateway Interface", що означає загальний інтерфейс шлюзу, який використовується для зв'язку зовнішньої програми з web-сервером).

Вибравши найкращий тип протоколу обміну, створювачі ботнетів швидко переключилися на дослідження можливих варіантів їх архітектури. Виявилось, що ботмережа з єдиним центром керування вельми вразлива. Єдиний центр керування був класичним технологічним рішенням для управління, але одночасно виступав критичним вузлом, оскільки його виявлення й відключення обов'язково приводило до припинення існування ботмережі. Це надало поштовх до створення ботнетів з іншою архітектурою. За типом архітектури ботмережі поділяються на мережі з єдиним центром управління та децентралізовані. У мережі ботнет з єдиним центром управління всі комп'ютери з'єднуються з важливим фрагментом, що позначається як C&C (Command & Control Centre – командно-управлінський центр). Він виступає ключовою ланкою у функціонуванні такої мережі, оскільки перебуває в режимі постійного очікування підключення комп'ютерів, яких реєструє у своїй базі даних. За допомогою центру здійснюються також подальше спостереження за роботою підключених комп'ютерів та розсилка необхідних команд. Для керування централізованою мережею особі, яка її створила, достатньо мати безпосередній або віддалений доступ. Останній має низку переваг. Мережі з єдиним центром управління є найпоширенішим типом з огляду на те, що їх легше створювати та керувати ними. Проте й нейтралізація побудованих за таким принципом мереж можлива шляхом виявлення їхнього центру.

У мережі ботнет із децентралізованим управлінням P2P комп'ютери з'єднуються з певним комп'ютером, що вже є її складовим елементом. Кожен комп'ютер такої мережі має список своїх «сусідів», щоби під час отримання команди передавати її іншому. Таким чином, керування цією мережею можливе за наявності доступу, знову ж таки безпосередньому або віддаленому до хоча б одного з цієї системи комп'ютерів.

Для швидкого зростання кількості «захоплених» комп'ютерів, як правило, здійснюється підпорядкування не тільки, а може, й не стільки комп'ютерів окремих користувачів у мережі, скільки серверів локальних мереж. Підпорядковані комп'ютери можуть стати засобами приєднання цілих корпоративних мереж. За такою схемою відбувається швидка побудова злочинної технічної «піраміди». Після встановлення контролю над окремим комп'ютером або цілою локальною чи корпоративною мережею останні підключаються до командного центру для отримання подальших інструкцій.

Для створення ботмереж використовується багато методів, зокрема методів соціальної інженерії, що дають змогу за короткий проміжок часу швидко збільшувати кількість залучених комп'ютерів. Упровадження кодів спеціальних програм здійснюється за допомогою web-сайтів, у тому числі спеціально створених, електронної пошти, пристроїв уводу-виводу.

Технічна спадкоємність також відіграла не останню роль, оскільки завдяки ній ботнети з єдиним центром управління швидко перебудовувалися або приєднувалися до необхідних фрагментів мережі. Для постійного активного залучення ресурсів комп'ютера як найменшої структурної одиниці ботмережі провокаційно поширюються привабливі посилання, наприклад, на останню версію ліцензійного програмного забезпечення або нові розважальні програми, популярні фільми, ігри. Для здійснення підключення використовується масова або сфокусована розсилка поштових листів, відкриття яких запускає необхідну програму для встановлення контролю над ресурсами комп'ютера. Не останню роль відіграють у широкому залученні нових комп'ютерів як складових ботмереж сайти з порнографією, які, на жаль, мають численну кількість відвідувачів. Фактично для встановлення контролю над ресурсами комп'ютера необхідно, щоб користувач погодився з посиланням або відкрив отримане поштове повідомлення.

Для забезпечення самого процесу будови бот-мережі разом із власними дослідженнями можливих технологій створення активно використовується перевірений та усталений метод – купівля заздалегідь зарезервованих уразливих місць програмного забезпечення масового використання. Вартість невідомої вразливості в операційній системі або популярному браузері може становити десятки тисяч доларів.

Практично в будь-якому елементі програмного забезпечення, особливо великого об'єму, є свої секрети, знайти які непросто, оскільки програмний код замасковано під реально наявний алгоритм або його частину.

Серед масштабних ботмереж із потужними можливостями відомими є такі, як StormWorm, Mayday, Rustock, Maazben, Kido, Cutwail, ZeuS, Kneber, Mozi.

Узагальнення уривчастих відомостей дає змогу відтворити значну частину «технокримінальної» картини. Відправною точкою технологічного циклу побудови кримінального адміністрування є знайдена вразливість програмного забезпечення. Вона може існувати внаслідок недосконалості, помилки або завдяки спеціальному резервуванню. Таким чином, уразливості поділяються на природні та штучно створені. Виявлення невідомої уразливості або її купівля відкриває можливість написання спеціальної програми, її продажу у «чистому» вигляді, тобто без змін. Створена спеціальна програма може використовуватися безпосередньо для побудови бот-мережі або керування нею чи бути проданою. У дусі кращих традицій поширення програмного забезпечення купівля таких програм супроводжується таким сервісом, як оновлення та подальше вдосконалення продукту.

Коло суб'єктів, які можуть взяти опосередковану або безпосередню участь у такій багатоваріантній схемі, можна поділити на такі категорії, як створювачі ліцензійних програмних продуктів, дослідники, створювачі нелегального програмного забезпечення, поширювачі, орендодавці та орендатори, тобто кінцеві користувачі. Якщо йдеться про суто кримінальне використання, то усіх таких осіб, які належать до однієї або декількох категорій одночасно, поєднує єдина мета, що полягає у створенні бізнесу на основі вразливості програмного забезпечення. Ботнети використовуються для збору інформації, а це фактично безвідходна діяльність, адже збирається все, що може бути продане.

Специфіка мережі ботнет полягає також у тому, що вона може використовуватися для самозахисту. Управлінський програмний код сучасних ботмереж має швидкий цикл оновлення: приблизно один раз на годину. Така динамічна конспірація не просто вражає, але й примушує замислитися щодо визначення швидкості технології протидії. Технічно мережа ботнет складається з певних кількісних груп комп'ютерів, щоб у разі можливого виявлення обмежитися втра-

тою лише частини окремого сегменту, а не всієї мережі. Під час виявлення деструктивних заходів впливу ресурси мережі ботнет можуть використовуватися для самозахисту. У такому разі фіксується інтернет-адреса, збирається необхідна службова інформація щодо потужностей супротивника й залежно від його «вагової» категорії виділяється частина або всі ресурси мережі ботнет для інформаційного блокування. Також бот-програма може блокувати доступ користувача до ресурсів Інтернету, оскільки він може бути використаний для пошуку заходу протидії шляхом ознайомлення з консультаційними форумами, завантаження відповідного програмного забезпечення для блокування функціонування бот-програми.

Сутність DDoS-атаки полягає в тому, що за певний час на зазначену мережеву адресу постійно відправляється велика кількість пакетів даних. Стандартне звертання до сторінки ресурсу – це норма, на яку розрахована його діяльність. Сервери можуть обробляти певний обсяг трафіку в одиницю часу залежно від характеристики самого обладнання, що також впливає на здатність пропускати відповідний обсяг даних. Якщо ця межа перевищується, новий запит буде відкинутий. Таким чином, усі ресурси системи будуть повністю задіяні, внаслідок чого доступ інших користувачів стане технічно неможливим.

Історія суперництва правоохоронної і злочинної систем свідчить про обопільний науковий підхід до своєї діяльності. У першому випадку це наукові та практичні конференції. Відповідні злочинні семінари та симпозіуми з обміну досвідом мають цільову спрямованість та практичну необхідність, організовуються виключно за принципом інформативності, конкретності.

Принцип конспірації чи маскування також є неодмінним атрибутом будь-якої злочинної діяльності. Поширюється він на підготовку та вчинення злочинів у сфері інформаційних технологій, передбачаючи приховування справжніх намірів і цілей дій, надання здійснюваним операціям вигляду законних, забезпечення умов приховування виконуваних дій, маскування поведінки тощо. Відмінність полягає в тому, що цей принцип забезпечується як природними властивостями приховуваного характеру високотехнологічних процесів, так і спеціальними технічними та програмними засобами захисту.

Принцип корпоративної єдності, взаємодопомоги по праву вважається стрижнем у характеристиці злочинної діяльності, оскільки відображає в соціальній сутності злочинного середовища головне – її протистояння суспільству.

Принцип спеціалізації у структурі злочинної діяльності має такі два зрізи: у рамках різних видів злочинів і спеціалізація всередині злочинної групи. Злочинні угруповання комплектуються за видами злочинів, які вони вчиняють.

Злочинні групи базуються на диференціації ролей співучасників групи: організовують діяльність злочинної групи; ведуть розвідку та контрозвідку; забезпечують дисципліну; безпосередньо виконують злочинні діяння; здійснюють збут матеріальних цінностей. Цей принцип також має два боки. З одного боку, спеціалізація приводить до ефективнішої протиправної діяльності, а з іншого боку, вона приводить до протиріч.

Принципи злочинної діяльності переважно не змінюються, але змінюється їх зміст. Він трансформується відповідно до сучасних процесів у соціальній, економічній, інформаційній сферах, а також протистояння злочинності правоохоронної діяльності. Це зумовлює необхідність вивчення з боку останньої для своєчасного розроблення адекватних засобів та методів попередження, виявлення, розкриття та розслідування сучасних злочинів.

Злочинність у сфері високих інформаційних технологій, яка є породженням перехідного періоду розвитку, за своїми якісними та кількісними ознаками відрізняється від злочинності минулих років. Можна умовно сказати, що вона більш латентна, масштабна, професійна, організована, міжнародна, технічно оснащена [4, с. 49].

Розвиток багатьох країн світу, зокрема України, свідчить про співіснування усталених і нових форм злочинної діяльності, що охоплюють перш за все слабко контрольовані чи не контрольовані державою сфери, втручаються в економіку, політику, ідеологію та соціальні відносини. Це проявляється, зокрема, у вчиненні злочинів у сфері високих інформаційних технологій або використання їх можливостей під час здійснення тероризму, торгівлі людьми та поширення порнографії.

Спостерігається тенденція до компрометації мережевої адреси іншого користувача внаслідок власної протиправної діяльності. Аналіз інформації на спеціальних форумах мережі Інтернет свідчить про обмін знаннями щодо логічного приховання власних IP та MAC-адрес або «підставляння» даних інших користувачів.

Для приховування даних щодо IP-адрес використовуються сайти-анонімайзери, а для зміни

MAC-адреси задля цього використовуються спеціальні програмні засоби. У мережі Інтернет відзначається значна кількість сайтів, які надають анонімні послуги користувачам. Використання таких сайтів дає змогу приховувати власний IP-адрес або імітувати своє фізичне розташування на території іншої держави.

Специфіка та можливості сфери високих інформаційних технологій дають змогу кримінальним структурам і окремим злочинцям відпрацьовувати технологію вчинення відповідних кримінальних діянь, тобто сфера високих інформаційних технологій виступає полігоном, який повністю відповідає реальним умовам вчинення злочинів. Аналіз інформації, що передається каналами мережі Інтернет, свідчить про такі види технологічних тренувань, як подолання систем захисту, отримання необхідних даних (реквізитів платіжних систем), установлення контролю над окремим комп'ютером або мережею, відпрацювання швидкості мобілізації створеного ботнету й виконання поставленого завдання з подальшим його розформуванням, а також протидія іншим ботнетам.

Сучасний стан злочинів у сфері високих інформаційних технологій характеризується тим, що їх кількість не має тенденції до зменшення – навпаки, спостерігаються постійне зростання та розширення наявних меж. Цілком очевидно, що гострота проблем у цій сфері боротьби стає потенційною небезпекою для держави та вимагає прийняття неординарних рішень, кардинальних змін стереотипних підходів до її розв'язання, розроблення нових форм боротьби зі злочинністю, проте врахування пріоритетності інтересів людини та громадянина.

З огляду на динаміку високих інформаційних технологій управління подіями в дійсності подібно спробам керувати минулим. Таке управління дає миттєві результати, але рано чи пізно оплачується ще тяжчими наслідками. Управління сьогоденням породжує необхідність моніторингу вимірів параметрів порядку в комунікативних системах. При цьому можливості оперативного управління комунікативними процесами в режимі синхронії не дають необхідного результату. Вважаємо, що найефективнішим є управління подіями в реальності, оскільки це дає можливість управляти майбутнім.

Висновки. Таким чином, вважаємо, що для створення стратегічної моделі протидії великого значення набуває аналіз тенденцій у розвитку та трансформації злочинності у сфері високих інформаційних технологій. Можливості одного програмно-апаратного комплексу помножуються на їх кількість. Виникнення та вдосконалення телекомунікаційних програмних засобів дали можливість одному користувачу встановлювати контроль над великою кількістю комп'ютерів і керувати ними особисто. Аналіз зарубіжних джерел свідчить про те, що для позначення «захопленої» мережі комп'ютерів використовується термін "botnet", який є скороченим збірним поняттям від англійських слів "robot" і "network". У загальному визначенні ботмережа – це субмережа, що виникає внаслідок загальної або часткової мобілізації ресурсів, яка проводиться відкрито або приховано для можливості використання програмно-апаратного комплексу користувачів з певною метою.

За типом архітектури ботмережі поділяються на мережі з єдиним центром управління та децентралізовані, що використовуються для здійснення широкого спектру завдань. Керівником (адміністратором) потужних ботнетів з понад 100 тисяч фейкових облікових записів виступає одна людина. Окрім кібератак і зламування сайтів, здійснюється підбор паролів до скриньок електронної пошти на віддалених платформах. Як правило, замовники знаходяться на закритих форумах та у чатах Telegram, а розрахунки здійснюються через електронні платіжні системи (навіть ті, які заборонені в Україні і на які поширюється дія санкцій РНБО).

Література

1. Берназ В.Д. Норми та принципи діяльності кримінальних угруповань як джерела інформації при розслідування злочинів. *Вісник Одеського інституту внутрішніх справ*. 2005. № 2. С. 24–28.

2. Wenke L. Botnet Detection. 2008. 168 p.

3. Dunham K., Melnick J. Malicious Bots: An Inside Look into the Cyber-Criminal Underground of the Internet. 2008. 168 p.

4. Долженков О.Ф., Гусак Н.О. Організаційно-правове забезпечення боротьби з економічною злочинністю в Україні: проблеми та шляхи розв'язання. *Вісник Одеського інституту внутрішніх справ*. 2005. № 3. С. 48–50.

Воронов І. О.
доктор юридичних наук,
старший науковий співробітник, адвокат