обратном шифровании информации, и асимметричных криптосистем, таких как Эль-Гамаль, Ривест-Шамир-Эйдельман, Меркл-Хеллман и Хор-Ривест, использующих один ключ в шифровании информации, способствует повышению качества услуг специалистов отрасли в защите информации.

Криптографические методы защиты информации в автоматизированных системах необходимы не только для защиты информации, обрабатываемой на компьютере или хранящейся на различных запоминающих устройствах, но и для обеспечения полноты информации, передаваемой по сетевым каналам связи. То есть применение криптографических методов позволяет передавать скрытую информацию по каналам связи и обеспечивать достоверность информации путем ее хранения в зашифрованном виде на носителях информации.

Библиографические ссылки

1. Казахстанский путь – 2050: Единая цель, единые интересы, единое будущее : Послание первого Президента Республики Казахстан Н. А. Назарбаева народу Казахстана (Астана, 17 января 2014 года).

2. Об утверждении Концепции кибербезопасности «Киберщит Казахстана» : Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407.

3. Тулбасова Б. К., Омарова С. А., Унейбаева Р. К. Информационная безопасность и защита информации : учеб.-метод. комплекс. Алматы : Нур-Принт, 2012. 115 с.

Телійчук В. Г.,
доцент кафедри
оперативно-розшукової діяльності
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук,
старший науковий співробітник, доцент

ЩОДО ПРОБЛЕМИ ОПЕРАТИВНО-РОЗШУКОВОЇ ПРОТИДІЇ НЕЗАКОННОМУ ОБІГУ ВОГНЕПАЛЬНОЇ ЗБРОЇ У МЕРЕЖІ «ІНТЕРНЕТ»

В Україні з усієї групи злочинів, пов’язаних із порушенням установлених правил поводження з загально небезпечними предметами, найбільш поширеним злочином є незаконне поводження зі зброєю, бойовими припасами або вибуховими речовинами. Неконтрольований обіг відповідних загально небезпечних предметів приховує в собі високий рівень небезпеки спричинення шкоди людям та довкіллю. Суспільна небезпека злочинів, пов’язаних із незаконним обігом зброї, зумовлена тенденцією розвитку насильницької озброєної злочинності, а ще незаконним збройним

підприємництвом [1].

Протидія незаконному обігу вогнепальної зброї у мережі «Інтернет» є складовою протидії злочинності. Протидія злочинності – це діяльність держави, яка спрямована на напрацювання стратегії реакції суспільства на злочинність (загально соціальний рівень) та профілактику злочинів, виявлення та запобігання (припинення) злочинним діям, реагування на вчинений злочин кримінально-правовими засобами (притягнення винних до кримінальної відповідальності) (спеціальний рівень). Однією зі складових спеціальної протидії незаконному обігу вогнепальної зброї у мережі «Інтернет» є оперативно-розшукова протидія. Протидія злочинності оперативно-розшуковими заходами містить у собі систему оперативно-розшукових та інших заходів і реалізується в окремих організаційно-тактичних формах.

Тенденції розвитку оперативно-розшукової діяльності у сфері використання інформаційних технологій спираються на застосування спеціальних технічних засобів контролю, фіксації та обробки інформації. Треба зазначити, що працівники органів Національної поліції (далі – НПУ) відстають від вимог часу, залишаючись технічно недостатньо озброєними в сучасному стані, від чого ефективність запобігання, виявлення та розслідування кримінальних правопорушень з використанням оперативно-розшукових заходів є низькими, і це важко приховати. Згідно із статистичними даними правоохоронних органів, приблизно 35–40 % традиційних злочинів щорічно вчиняється з використанням сучасних телекомунікаційних, комп’ютерних та інших технологій, а у майбутньому цей відсоток може суттєво збільшитись [2, с. 31]. Використання злочинцями в протиправній діяльності мережі «Інтернет», зокрема, під час незаконного розповсюдження вогнепальної зброї, бойових припасів і вибухових речовин, набуло сьогодні масштабних негативних тенденцій. Злочинцями відразу було позитивно оцінено технічні можливості використання в протиправній діяльності такого зв’язку, насамперед можливість у будь-якому місці країни та в будь-який час зв’язатися зі співучасником, при цьому зберігаючи анонімність абонентів-користувачів мережі «Інтернет». На відміну від стільникового телефонного зв’язку, комп’ютер (ноутбук) не завжди можна запеленгувати та визначити його місцезнаходження (відповідно, і користувача), оскільки для виходу в Інтернет можуть використовуватися портативні пристрої в різноманітних місцях, де є можливість підключення до мережі, що набагато спрощує вчинення протиправних діянь та впровадження в злочинну діяльність таких засобів зв’язку. Останнім часом усе частіше мережа «Інтернет» стала використовуватися злочинцями також як засіб платежу за вчинення різноманітних протиправних діянь, у тому числі для оплати під час придбання вогнепальної зброї, бойових припасів і вибухових речовин [3]. Мережа «Інтернет» являє собою просторову структуру, яка містить ієрархію різних учасників: установ реєстрації доменних імен і безлічі посередників, розподілених асиметричним способом (операторів системи та

інших). Усі вони забезпечують кінцевим користувачам можливість доступу до мережних протоколів і вебсерверів [4].

Характерною особливістю таких протиправних операцій є їх міжрегіональний характер: особа, яка замовляє вогнепальну зброю, бойові припаси й вибухові речовини, може перебувати в одному районі (міста чи регіону), особа, яка робить закладку вогнепальної зброї, бойових припасів і вибухових речовин – у другому районі (міста чи регіону), а процес легалізації отриманих від незаконного обігу цих засобів коштів – у третьому. Отже, злочинці розуміють, що, перебуваючи в різних регіонах країни, вони ускладнюють викриття своєї протиправної діяльності, оскільки в більшості випадків їх особа не відома покупцям вогнепальної зброї, бойових припасів і вибухових речовин. Зазначене унеможливлює фіксацію таких фактів злочинної діяльності оперативними підрозділами Національної поліції України.

До способів використання комп'ютерних технологій у сфері незаконного обігу вогнепальної зброї, бойових припасів і вибухових речовин належать такі: 1) приховування інформації щодо поставок партій вогнепальної зброї, бойових припасів і вибухових речовин шляхом криптографічного кодування електронних посилань; 2) шифрування інформації щодо номерів банківських рахунків, баз даних фінансових активів, способів зв'язку зі спільниками, даних обліку торговельних операцій; 3) шляхом використання неконтрольованих засобів електронного зв'язку для передачі інформації, безпосередньо пов'язаної з проведенням незаконних операцій, у тому числі за допомогою чат-кімнат в Інтернеті з обмеженим доступом; 4) «відмивання» доходів від незаконного обігу вогнепальної зброї, бойових припасів і вибухових речовин за допомогою електронних платежів [3].

Інтернет має три специфічні властивості, які можуть сприяти відмиванню грошей: вільний доступ, анонімність відносин між клієнтом та фінансовою установою, висока швидкість здійснення електронних угод.

Майже вся аудіо-, відео- та текстова інформація, яка є на сторінках сайтів в мережі «Інтернет», а так само й імена конкретних інтернет-сайтів розшукується його користувачами шляхом формування відповідних пошукових запитів у спеціальних пошукових сервісах. За своєю внутрішньою будовою пошукові сервіси можна поділити на такі складові частини: відкриту для користувача, та закриту від користувача.

Відкриту для користувача частину умовно можна поділити на такі, зокрема, складові частини:

– одне чи декілька доменних імен інтернет-сайту, через які здійснюється доступ до самого пошукового сервісу; графічна оболонка пошукового сервісу;

– інструменти для формування пошукових запитів та роботи з ними; блок відображення результатів пошуку інформації за сформованими пошуковими запитами.

Закриту від користувача частину можна умовно поділити на такі

складові частини:

– пошуковий індекс – перелік доменних імен інтернет-сайтів та конкретної інформації, яка розміщена в мережі «Інтернет», що може вивести пошуковий сервіс у блоці відображення результатів пошуку інформації за сформованими пошуковими запитами; пошукові роботи – це спеціальні програми, які сканують інформаційний простір мережі «Інтернет», та відносять чи виключають ту чи іншу інформацію до бази даних пошукового сервісу; внутрішні правила, за якими пошукові роботи відносять ту чи іншу інформацію до пошукового індексу пошукової системи; база даних, в якій зберігається аудіо-, відео- та текстова інформація, яку було включено до пошукового індексу пошукового сервісу.

Необхідно зазначити, що різні пошукові сервіси використовують різні внутрішні правила та різних пошукових роботів, через що їх пошукові індекси та бази даних можуть суттєво відрізнятись одна від одної. Саме тому під час пошуку інформації, що становить тактичний чи оперативний інтерес, необхідно користуватись різними пошуковими сервісами. Під час розробки оперативних заходів необхідно враховувати і технічні аспекти. Новітні технології дозволяють зловмисникам уникнути відстеження місця, де вони перебувають. Найбільш поширений спосіб уникнути інтернет-спостереження – використовувати комп'ютери із загальним доступом в інтернет-кафе, бібліотеках тощо. На сьогодні найбільш поширеним способом уникнути встановлення місцеперебування є використання анонімайзерів і TOR-мережі. У разі використання web-proxy через доступ провайдера до серверів, на яких знаходяться вебресурси, «сліди запитів» залишаються на ISP-сервері і дозволяють відстежити місцеперебування комп'ютера користувача.

У разі використання Інтернету в протиправній діяльності здебільшого затримати злочинців можна тільки за допомогою оперативних заходів. Під час використання TOR-мереж визначити місцеперебування кінцевого комп'ютера доволі складно, тому з метою профілактики можна розміщувати сайти-пастки для встановлення осіб, які цікавляться придбанням вогнепальної зброї, а також робити контрольні закупівлі [4].

Бібліографічні посилання

1. Шинкаренко І. І. Виявлення та встановлення зброї, бойових припасів або вибухових речовин, що перебувають у незаконному поводженні. *Право і Безпека*. 2014. № 3. С. 170–174. URL: http://nbuv.gov.ua/UJRN/Pib_2014_3_36
2. Максимус Д. О., Юхно О. О. Використання сучасних інформаційних технологій працівниками органів внутрішніх справ при проведенні негласних слідчих (розшукових) дій : навч. посіб. Харків : Ніка Нова, 2013. 102 с.
3. Кириченко О. В. Мережа Інтернет як засіб незаконного розповсюдження вогнепальної зброї, бойових припасів та речовин. URL: https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/6905/1/%D0%9C%D0%95%D0%A0%D0%95%D0%96%\
4. Телійчук В. Г. Оперативно-розшукова протидія наркозлочинності в мережі Інтернет як стратегія протидії наркозлочинності в Україні. *Вісник ДДУВС*. URL: http://visnik.dduvs.in.ua/wp-content/uploads/2019/02/NV_spec_1_2018.pdf