форму розпорядження власним майном у випадку смерті, забезпечити відповідний захист прав і законних інтересів всіх учасників спадкових взаємовідносин. Отже, спадкування за заповітом являється одним із видів спадкування та регулюється главою 85 ЦК. Воно найбільше відображає спадкодавче волевиявлення. Заповіт являється особистим розпорядженням фізичної особи у випадку власної смерті.

1. Конституція України, затверджена на п'ятій черговій сесії ВРУ 28 червня 1996 р. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.

2. Цивільний кодекс України від 16.01.2003 р. (з наступними змінами та доповненнями станом на 17.05.2021). *Відомості Верховної Ради України*. 2003 Ст. 356.

3. Дзера О.Г. Науково-практичний коментар до Цивільного кодексу України: у 2 томах - 5-те видання, перероблене і доповнене. К.: Юрінком Інтер, 2015. Т.1. 832 с.

4. Желіховська Ю. В. Поняття та юридична природа «спадкового представлення». *Ученые записки Таврического национального университета им. В.И. Вернадского. Серия «Юридические науки».* 2013. № 2-1. С. 261-265

5. Нестерцова-Собакарь О.В. Спадкове право: навч. посібник [для студ. вищ. навч. закл.]. кол. авт. ; кер.авт. кол, канд. юрид. наук, доц. Нестерцова-Собакарь О.В. Дніпро : Дніпроп. держ. ун-т внутр.справ, 2017. 164 с.

Лазарєва Я.А., курсантка
Дніпропетровського державного
університету внутрішніх справ

Науковий керівник:
Кисельов А.О., к.ю.н, доц.,
доцент кафедри
оперативно-розшукової діяльності
Дніпропетровського державного
університету внутрішніх справ

ЗАКОРДОННИЙ ДОСВІД ЗАСТОСУВАННЯ «OSINT» У ПРОТИДІЇ КРИМІНАЛЬНИМ ПРАВОПОРУШЕННЯМ

Застосування «OSINT» дозволяє отримати відповідь на безліч питань, які виникають у особи, що приймає рішення (ОПР) питання, а також зосередити зусилля розвідувальних органів на виконання більш складних і «вузьких» завдань, які не розпорошуючи сили інших напрямків розвідки на добування того, що можна отримати з відкритих джерел.

Технологія «OSINT» є однією з важливих технологій «глибинного збору» різнорівневого формату інформації, а також формування на її базі принципово нових знань.

Поширення і використання перевіреної інформації з відкритих джерел дозволяє здійснювати обмін такою інформацією, оскільки при її отриманні не

використовуються приховані методи і секретні джерела. Одна з найбільш детальних відомостей про «OSINT» в НАТО міститься в посібниках «NATO Open Source Intelligence Handbook» (2006-2017 р.р.) та інструкціях «NATO Open Source Intelligence Reader» (2006-2017 р.р.), які містяться в передмові.

Вичерпна інформація та різні погляди на «OSINT» - інформація стосується всіх команд НАТО, оперативних груп, країн-членів, цивільно-військових комітетів та робочих груп, а також інших організацій, які можуть планувати або брати участь у спільних операціях.

Третя збірка в цій групі документів НАТО, «NATO Intelligence Explo-?tation of the Internet» (2002 р.), застаріла і була видалена, хоча доступна на інших ресурсах в «Інтернеті» [1].

США використовує інформацію, отриману за допомогою «OSINT», в більшій мірі для планування бойових дій, організації та проведення військових операцій, запобігання терористичним актам [2].

На думку аналітиків американської розвідки, на сьогодні неперевірені джерела інформації, провокаційні ресурси та недостовірна інформація є найбільшою проблемою методу «OSINT».

Для того, щоб отримати найбільш актуальну та якісну інформацію, користувачеві необхідно обробити багато інформації з різних джерел та узагальнити її відповідно до мети та завдань дослідження. США мають розгалужену мережу центрів та агентств, які надають інформацію «OSINT» та надають інформацію понад 7000 споживачам інформації.

І це не що інше, як результат скоординованих дій законодавчої та виконавчої влади, спрямованих на цілеспрямовану політику у сфері національної безпеки.

Подібні структури існують на всіх рівнях [3]. Також Ізраїль використовує «OSINT» насамперед для аналізу військових можливостей ворога.

У структурі служби військової розвідки є окремий спеціальний підрозділ для аналізу відкритих джерел інформації «Hatsaf», який збирає інформацію лише для військових цілей.

У Великобританії цивільні журналісти зі служби спостереження «BBC Monitoring» проводять перший збір інформації за допомогою «OSINT», який потім надходить до спецслужб для використання в певних областях дослідження [4, с. 380].

З метою оптимізації та удосконалення роботи з джерелами відкритої інформації в розвідувальних цілях у 2004 році Президент США Дж. Буш підписав закон «Про реформування розвідки та протидії терористичним загрозам», згідно з яким розвідка з відкритих джерел стала повноцінним і рівноправним видом діяльності розвідувального співтовариства, а в структурі Директора національної розвідки США створений Центр аналізу інформації з відкритих джерел («Open Source Center») [5, с.35].

Минько О. В. у своєму дослідженні зазначає, що якщо говорити про сучасне застосування та використання технологій «OSINT» в Україні, то варто

зазначити, що вони активно використовуються під час російсько–української війни в окремих районах Донецької та Луганської областей. Наприклад, одним із джерел інформації про ефективність артилерійського вогню терористів у Донецькій області є обговорення мешканцями міста цих подій в Інтернеті, а фотографії військової техніки, зроблені місцевими жителями, часом набагато ефективніші, ніж спостереження ОБСЄ [6, с.83].

Отже, сьогодні «OSINT» активно та успішно використовується інформаційно – аналітичними відділами провідних країн світу. Дані про відсоток продуктивності відкритих джерел інформації підтверджують необхідність та актуальність використання досвіду США та Європи для досягнення оперативних, тактичних та стратегічних цілей правоохоронних органів.

На сьогоднішній день більшість провідних країн світу активно використовують сучасні технології, що дозволяють співробітникам відповідних служб отримувати необхідну інформацію та використовують лише доступ до глобальної мережі, що концентрує велику кількість даних, необхідних для оцінки ситуації як вважатиметься необхідним, слідкувати за ситуацією та задовольняти потреби державних установ за даними, необхідними для прийняття обґрунтованих та правильних рішень.

1. Г. Додонов, Д. В. Ландэ, В. В. Цыганок, О. В. Андрейчук,С. В. Каденко, А. Н. Грайворонская/ Распознавание информационных операций/А. Г. Додонов, Д. В. Ландэ, В. В. Цыганок, О. В. Андрейчук,С. В. Каденко, А. Н. Грайворонская// Киев: ООО «Инжиниринг», 2017. 282 с.

2. Разведка с использованием открытых источников информации в США. U-U-

-

L:http://pentagonus.ru/publ/razvedka_s_ispolzovaniem_otkrytykh_istochnikov_informacii_v_ssha/80-1-0-1614 (дата звернення: 09.04.2021).

3. Разведка на основе открытых источников. URL: http://www.in4sec.com.ua/razvedka-na-osnove-otkry-ty-h-istochnikov-open-source-intelligence-osint/ (дата звернення: 09.04.2021).

4. А.В. Серватовський, Ю.М. Онищенко, П.В. Макаренко. Міжнародний досвід використання OSINT/ А.В. Серватовський, Ю.М. Онищенко, П.В. Макаренко// Актуальні питання протидії кіберзлочинності та торгівлі людьми. Харків, 2018.

5. Кондратьев А. В. Разведка в сухопутных войсках США на основе анализа открытых источников информации / А. В. Кондратьев // Зарубеж-ное военное обозрение, 2009, №5, С. 32-38.

6. Минько О. В. Використання технологій OSINT для отримання розвідувальної інформації / О. В. Минько, О. Ю. Іохов, В. Т. Оленченко, К. В. Власов // Системи управління, навігації та зв'язку. 2016. Вип. 4. С. 8.