Войцеховська Дар'я Миколаївна
курсант 204 навчальної групи ННІ № 3 НАВС, капрал поліції

Науковий керівник:
Яровий Кирило Васильович
кандидат юридичних наук, старший викладач кафедри інформаційних технологій та кібербезпеки ННІ № 1 НАВС, капітан поліції

СТАН ДОСЛІДЖЕННЯ ПИТАННЯ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Зростання злочинності та вдосконалення методів їх вчинення ускладнюють роботу правоохоронних органів. У відповідь на це Національна поліція України (далі – НПУ) активно впроваджує нові інформаційні технології та системи, які допомагають їй ефективніше розкривати злочини, забезпечувати громадський порядок та безпеку громадян.

Проблематика інформаційного забезпечення правоохоронних органів вивчалися різними фахівцями з різних наукових галузей. Зазначене свідчить про комплексний підхід до розвитку наукової думки в цьому напрямку. Наприклад, І.Р. Бондар [1] розробив алгоритм управління програмою безперервності функціонування системи інформаційної безпеки держави. О. Панченко [2] дослідив питання державного управління у сфері забезпечення інформаційної безпеки в контексті різних дестабілізуючих факторів. Б.В. Паш [3] розглянув сутність та структуру інформаційної безпеки в умовах глобалізації. Є.В. Кобко дослідив місце інформаційної безпеки в структурі національної безпеки через аналіз сучасного стану та перспектив правового регулювання відповідних суспільних відносин [4]. М.Т. Гаврильців зосередився на дослідженні сутності інформаційного захисту як складової національної безпеки України в умовах гібридної війни [5].

На нашу думку, для вирішення проблеми інформаційного забезпечення правоохоронних органів необхідно посилити розвиток програмного забезпечення та співпрацю з науково-дослідними установами, щоб забезпечити постійне оновлення та підвищення кваліфікації персоналу у сфері кібербезпеки.

Підрозділи інформаційно-аналітичної підтримки в Національній поліції керують використанням сучасних інформаційних технологій, забезпечуючи функціонування ІПНП в рамках ЄІС МВС та оперуючи інформаційними ресурсами. Серед їхніх завдань – створення та супровід автоматизованих систем,

забезпечення доступу до інформації, створення підсистем ЄІС МВС та формування баз даних різного характеру.

Основні завдання цих підрозділів включають:

- забезпечення роботи комплексної інтегрованої системи, яка підтримує функціонування суб'єктів системи, надає їм інформаційну підтримку та обслуговує їх діяльність. Зазначене включає розробку та підтримку програмного забезпечення, технічні засоби зв'язку, обробку та захист інформації;
- створення та підтримка інформаційних ресурсів, які представляють собою групи взаємозв'язаних даних, об'єднаних в системах МВС за певними критеріями, включаючи пріоритетні інформаційні ресурси;
- забезпечення доступу до інформаційних ресурсів інших органів державної влади, включаючи пріоритетні ресурси МВС;
- розробка та підтримка підсистем Єдиного інформаційного простору МВС, зокрема Інформаційного порталу Національної поліції України та його компонентів;
- виконання інших завдань інформаційного, інформаційно-аналітичного, технічного та технологічного характеру [6, с. 278].

Враховуючи вищевикладене слід зазначити, що для удосконалення роботи підрозділів НПУ, які відповідають за використання сучасних інформаційних технологій та реалізацію функцій ІПНП в рамках ЄІС МВС, можна розглянути наступні шляхи удосконалення:

1) оптимізація інтегрованої системи (вдосконалення програмного забезпечення та технічні засоби зв'язку, щоб забезпечити ефективне функціонування системи);

2) розвиток інформаційних ресурсів (розширення та покращення існуючих інформаційні ресурси, забезпечуючи їх відповідність потребам і вимогам поліцейської діяльності);

3) підвищення доступності інформаційних ресурсів (забезпечення зручного та безпечного доступу до інформації для інших органів державної влади та внутрішніх користувачів, зокрема через розробку спеціалізованих інтерфейсів та засобів авторизації);

4) оновлення та підтримка підсистем (забезпечення постійної підтримки та оновлення існуючих підсистем ЄІС МВС, включаючи ІПНП, з метою забезпечення їхньої ефективної роботи та відповідності сучасним вимогам);

5) регулярне навчання та підвищення кваліфікації персоналу (забезпечення ефективного використання інформаційних технологій, персонал повинен постійно підвищувати свою кваліфікацію та навчатися використовувати нові інструменти та методи аналізу даних).

На нашу думку зазначені шляхи вдосконалення інформаційного забезпечення НПУ можуть сприяти покращенню роботи та підвищенню їхньої ефективності під час розслідування та розкриття злочинів правоохоронними органами.

Список використаних джерел:

1. Боднар І. Р. Інформаційна безпека як основа національної безпеки. Механізм регулювання економіки. 2014. № 1. С. 68–75.
2. Панченко О. Інформаційна складова національної безпеки. Вісник Національної академії Державної прикордонної служби України. 2019. Випуск 3. URL: https://www.rdc.org.ua/download/stati/Informational-warehouse.pdf (дата звернення: 15.04.2024).
3. Паш Б. В. Складові інформаційної безпеки держави: постановка питання. Закарпатські правові читання. 2017. Том 1. С. 509–512.
4. Кобко Є. В. Інформаційна безпека в системі національної безпеки: сучасність і перспективи. National law journal: teory and practice. 2019. March. С. 46–50.
5. Гаврильців М. Т. Інформаційна безпека держави в системі національної безпеки України. Юридичний науковий електронний журнал. 2020. № 2. С. 200–203.
6. Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС і навчальному процесі : збірник наукових статей за матеріалами доповідей Всеукраїнської науково-практичної конференції 23 грудня 2016 року / упорядник Т. В. Магеровська /. Львів : ЛьвДУВС, 2017. 313 с.

Haborets Olha Andriivna
PhD, Associate Professor of the Department of Operational-search Activities and Information Security of Donetsk State University of Internal Affairs

OSINT: A SCIENTIFIC APPROACH TO INFORMED DECISION-MAKING

In the current era of rapid technological progress and widespread internet availability, Open Source Intelligence (OSINT) technologies hold significant sway over the sourcing, analysis, and utilization of information. This dominance stems from their capacity to systematically navigate the vast expanse of digital data, extracting valuable insights crucial for informed decision-making across various domains.

OSINT entails the systematic gathering, examination, and utilization of publicly available information from diverse sources to draw meaningful conclusions and comprehend various situations. This methodology finds application across intelligence, cybersecurity, competitive analysis, law enforcement, and other sectors where access to open information enhances decision-making processes. It relies on sources like social media, public databases, websites, and forums.

Within the domain of OSINT, researchers and analysts harness specialized tools and techniques to collect, assess, and interpret vast amounts of data, thereby extracting