Враховуючи наведене представляється доцільним використання окремих аспектів американського досвіду у вітчизняній правоохоронній практиці протидії кіберзлочинам стосовно дітей.

Одержано 26.10.2018

УДК 004.056:341.4

Володимир Георгійович ПЯДИШЕВ,
кандидат технічних наук, доцент
доцент кафедри кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішніх справ

ЗАХОДИ ЄВРОСОЮЗУ ЩОДО БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

У 2010 році ЄС встановив чотирирічний цикл політики, щоб забезпечити більший ступінь наступності у боротьбі з серйозною міжнародною та організованою злочинністю. Ця політика передбачає ефективну співпрацю правоохоронних органів, інших агентства і установ ЄС, відповідних третіх сторін. З цією метою ЄС також закликає до рішучих дій, спрямованих на боротьбу з найбільш нагальними кримінальними погрозами, з якими стикається ЄС. На своєму засіданні 18 травня 2017 року: Рада ЄС визначила пріоритети щодо боротьби з організованою і серйозною міжнародною злочинністю на період з 2018 по 2021 рік. серед них перше місце посіла кіберзлочинність, При цьому вона випередила незаконний обіг наркотиків, сприяння нелегальній імміграції, торгівлю людьми, шахрайство з акцизами і податком на додану вартість, незаконний обіг вогнепальної зброї, екологічну злочинність, кримінальну діяльність з фінансами та відмиванням коштів і шахрайство з документами [1].

У зв'язку з цим, Євросоюз приступив до всебічного розвитку заходів щодо боротьби з кіберзлочинністю.

Законодавчі заходи. Для боротьби з кіберпреступростью [2], ЄС запровадив необхідне законодавство і організував підтримку співпраці в рамках стратегії ЄС з кібербезпеки 2013 року [3].

З урахуванням зростання частоти і суворості кіберзлочинів [4], 3 жовтня 2017 року Європарламент прийняв резолюцію про боротьбу з кіберзлочинністю [5].

Члени Європарламенту, серед іншого, «засуджують будь-яке втручання до системи, здійснюване або що направляється іноземною нацією або її агентами, з метою порушення демократичного процесу іншої держави». Крім того, Європарламент підкреслює, що «підвищення обізнаності про ризики, пов'язані з кіберзлочинністю, збільшилася, але запобіжні заходи, вжиті окремими користувачами, державними установами та підприємствами, залишаються абсолютно недостатніми, в першу чергу через нестачу знань і ресурсів».

Ключовими питаннями, що позначені в резолюції, є запобігання, підвищення відповідальності постачальників послуг, розширення співпраці поліції та судових органів, а також тісна співпраця між правоохоронними органами. Більше інформації міститься в прес-релізі Європарламенту від 3 жовтня 2017 року [6].

Інституційні заходи. 13 вересня 2017 року у своєму щорічному зверненні до держав Євросоюзу [7] Президент Жан-Клод Юнкер заявив, що Комісія пропонує новітні інструменти для захисту від подальших кібератак. 19 вересня 2017 Комісія оголосила про подальші дії по боротьбі з кіберзлочинністю, включаючи нову європейську систему сертифікації, спрямовану на забезпечення безпечного використання продуктів і послуг у цифровому світі [8].

Агентство Європейського союзу з мережевої та інформаційної безпеки (ENISA) підтримує обмін передовим досвідом між державами-членами ЄС [9]. Щоб посилити відповідь правоохоронних органів на кіберзлочинність в ЄС, у 2013 році Європол створив Європейський центр з кіберзлочинності (EC3). Він виступає в якості координатора у боротьбі з кіберзлочинністю в ЄС, об'єднуючи європейський досвід протидії кіберзлочинності на підтримку розслідування кіберзлочинів в державах-членах [10].

Інші заходи. До числа заходів, спрямованих на боротьбу з кіберзлочинністю на міжнародному рівні, належить створення Глобального альянсу проти онлайн сексуального насильства над дітьми [11]. Альянс є спільною ініціативою ЄС і США, яка об'єднує 54 країни з усього світу для спільної боротьби з сексуальним насильством над дітьми.

Відносно надання допомоги жертвам кіберзлочинів Європейська комісія рішуче підтримує Будапештську конвенцію Ради Європи про кіберзлочинність [12], а також партнерство між державним і приватним секторами і механізми співпраці за допомогою цільових проектів.

Окрім того, вебсайт Експертного центру Європарламенту надає численні публікації з кіберзлочинів. У додатку до законодавчого зібрання Європейського парламенту міститься додаткова інформація щодо усунення юридичних перешкод для кримінального розслідування кіберзлочинів [13]. Доступні також бюлетені по ініціативам Євросоюзу з кіберзлочинності [14] і за оцінками Єврокомісією її успіхів в боротьбі з кібератаками [15].

Одним з останніх прикладів висвітлення масштабу зростаючої проблеми може служити видана Європолом у 2017 році «Оцінка загрози організованої злочинності в Інтернеті» (IOCTA 2017 report) [16].

Оцінка результатів. На підставі дослідження статистичних даних, в яких були враховані такі особливості всіх держав Євросоюзу:

– як багато резидентів вже піддалися кіберзлочинам;

– як часто вони зустрічалися зі шкідливим програмним забезпеченням і вірусами;

– в якій мірі Інтернет з'єднання в кожній державі піддавалися атакам;

– наскільки та чи інша держава віддана ініціативам по боротьбі з кіберзлочинністю, – було проведено інтегральне ранжування держав за ступенем захищеності від кіберзлочинів.

В результаті ранжирування в країнах Євросоюзу визначилася п'ятірка держав, найбільш незахищених від кіберзлочинності: Мальта (найбільш незахищена), Греція, Румунія, Словаччина, Іспанія, – а також п'ятірка найбільш захищених держав: Великобританія, Нідерланди, Німеччина, Естонія, Фінляндія (найбільш захищена) [17].

Висновки:

1. Погроза кіберзлочинності, що нависла над сучасним світом, є об'єктивною реальністю. При цьому на рівень кібер-загроз в тій чи іншій державі впливає значна кількість об'єктивних факторів (рівень економічного розвитку та інші).

2. У зв'язку з цим на рівні керівництва Євросоюзу активно вживаються заходи на законодавчому, інституційному та інших рівнях.

3. Однак рівень кібербезпеки в державі залежить не тільки від об'єктивних чинників. Отже, він може сильно відрізнятися навіть в державах, що мають географічну, економічну та історичну близькість,. наприклад:

– Естонія посідає в Євросоюзі друге місце з кібербезпеки;

– Латвія знаходиться точно посередині;

– Литва посідає шосте місце від кінця.

4. Вказана обставина визначає важливість суб'єктивного фактора: ступеня орієнтованості держави на боротьбу з кіберзлочинністю, зокрема, її прихильності відповідним ініціативам Євросоюзу.

Список бібліографічних посилань

1. EU Policy Cycle – EMPACT. Europol : URL: https://www.europol.europa.eu/crime-areas-and-trends/eu-policy-cycle-empact [Accessed 16 October, 2018].

2. Cybercrime // European Commission on Migration and Home Affairs. URL: https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en [Accessed 16 October, 2018].

3. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. EUR-Lex: Access to European Union Law: URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52013JC0001 [Accessed 16 October, 2018].

4. Cybercrime // Europol. URL: https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime [Accessed 16 October, 2018].

5. European Parliament resolution of 3 October 2017 on the fight against cybercrime (2017/2068(INI)) // European Parliament. URL: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0366+0+DOC+XML+V0//EN&language=EN [Accessed 16 October, 2018].

6. Step up measures to prevent cyber-attacks and online sexual abuse, urge MEPs. // European Parliament News. 03-10-2017: URL: http://www.europarl.europa.eu/news/en/press-room/20171002IPR85128/step-up-measures-to-prevent-cyber-attacks-and-online-sexual-abuse-urge-meps [Accessed 16 October, 2018].

7. President Jean-Claude Juncker's State of the Union Address 2017. Brussels, 13 September 2017. *European Commission Press Release Database*. URL: http://europa.eu/rapid/press-release_SPEECH-17-3165_en.htm [Accessed 16 October, 2018].

8. State of the Union 2017 – Cybersecurity: Commission scales up EU's response to cyber-attacks. Brussels, 19 September 2017. *European Commission Press Release Database.* URL: http://europa.eu/rapid/press-release_IP-17-3193_en.htm [Accessed 16 October, 2018].

9. ENISA lists top cyber-threats in this year's Threat Landscape Report. *ENISA : European Union Agency for Network and Information Security* : URL: https://www.enisa.europa.eu/news/enisa-news/enisa-lists-top-cyber-threats-in-this-year2019s-threat-landscape-report [Accessed 16 October, 2018].

10. European Cybercrime Centre – EC3. // Europol. URL: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 [Accessed 16 October, 2018].

11. We Protect Global Alliance to End Child Sexual Exploitation Online // European Commission Migration and Home Affairs. URL: https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse [Accessed 16 October, 2018].

12. Convention on Cybercrime. Budapest, 23.XI.2001 // Council of Europe Portal. Treaty Office: URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 [Accessed 16 October, 2018].

13. Removing Legal Obstacles To Criminal Investigations On Cybercrime // Europarliament. URL: http://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-removing-legal-obstacles-to-criminal-investigations-on-cybercrime [Accessed 16 October, 2018].

14. EU cybersecurity initiatives. URL: http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf [Accessed 16 October, 2018]

15. State of the Union 2017: The Commission scales up its response to cyber-attacks. Brussels, 19 September 2017. European Commission Press Release Database. URL: http://europa.eu/rapid/press-release_MEMO-17-3194_en.htm [Accessed 16 October, 2018].

16. Internet Organised Crime Threat Assessment // Europol Cybercrime Centre. URL: https://www.europol.europa.eu/iocta/2017/index.html [Accessed 16 October, 2018]

17. T. Watts. Which EU Country Is Most Vulnerable To Cybercrime? // WebSiteBuilderexper. June 27, 2018. URL: https://www.websitebuilderexpert.com / eu-cybercrime-risk/ [Accessed 16 October, 2018].

Одержано 31.10.2018

УДК 327(045)

Андрій Володимирович СЕРВАТОВСЬКИЙ,
слухач магістратури факультету № 1 (слідства)
Харківського національного університету внутрішніх справ;
Юрій Миколайович ОНИЩЕНКО,
кандидат наук з державного управління, доцент,
доцент кафедри кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ;
ORCID: https://orcid.org/0000-0002-7755-3071;
Павло Валентинович МАКАРЕНКО,
кандидат психологічних наук, доцент,
заступник декана з навчально-методичної роботи
факультету № 4 (кіберполіції)
Харківського національного університету внутрішніх справ;
ORClD: https://orcid.org/0000-0002-9055-3287

МІЖНАРОДНИЙ ДОСВІД ВИКОРИСТАННЯ OSINT

На сьогоднішній день немає такої людини яка б не користувалася соціальними мережами, багато злочинів які відбуваються у сучасному світі плануються саме в інтернет-просторі, через спілкування в месенджерах, надсилання фото з зашифрованим місцем злочину тощо. «OSINT» є продуктивною системою протидії злочинам які відбуваються у кіберпросторі, треба лише правильно використовувати цей метод, враховуючи міжнародний досвід.

Одним з методів збирання оперативної інформації є використання розвідки з відкритих джерел, а саме «OSINT» (open-source intelligence). Сьогодні можна спостерігати збільшення зацікавленості в OSINT не лише з боку журналістів, аналітиків приватних компаній та пересічних громадян, але й аналітиків спецслужб, тому що «OSINT» має певні переваги перед збором, обробкою та аналізом інформації з обмеженим доступом, на сам перед тому, що не вимагає спеціального доступу до інформації, а значить зберігає час користувача, не вимагає спеціальних навичок, витрат значних коштів. Використання «OSINT» в деяких випадках дає змогу запобігти вчиненню злочинну, адже вираз «Краще попередити злочин, ніж карати» здобуває все більшого значення.

«OSINT» (Open Source INTelligence) – це збір, аналіз, обробка даних які знаходяться у загальному доступі, але ці данні завжди специфічні, тобто зібрані та структуровані особливим способом, задля