6. Ramsaroop P. Cybercrime, Cyberwarfare, Terrorism, and Sabotage: Critical Issues in Data Protection for Health Services Information Pan American Health Organization. Washington, D.C.: PAHO, 2003. 85 p.
7. Струков В. М. До визначення напрямів протидії кіберзлочинності URL: http://bit.ly/2imbPQe (дата звернення: 23.10.2017).

Одержано 01.11.2017

УДК 343.98

Сергій Павлович ЛАПТА,
кандидат юридичних наук, доцент, доцент кафедри криміналістики та судової експертології факультету №1 Харківського національного університету внутрішніх справ

ФБР У БОРОТЬБІ З КІБЕРЗЛОЧИННІСТЮ

Проблема боротьби зі злочинами у кіберпросторі наразі визнається одною із найгостріших серед проблем боротьбі зі злочинністю. Викликано це рядом факторів, які у значній мірі ускладнюють протидію кіберзлочинності. Для того щоб розпочати «бізнес» злочинцям іноді потрібні лише незначні грошові кошти. Злочинці можуть «атакувати» одночасно значну кількість потенційних жертв, рахунок яких іноді йде на сотні тисяч. Відповідно, якщо злочинна діяльність направлена на отримання кримінальних прибутків, вони значно збільшуються порівняно з іншими, традиційними способами. Так, у ході масованої кібератаки із застосуванням вірусу-вимагача Petya, яка відбулася 27 червня 2017 року, тільки в Україні постраждало близько 12,5 тисяч комп'ютерів та вийшла з ладу система радіаційного моніторингу Чорнобильської АЕС. У світі жертвами стали такі гіганти, як британська рекламна компанія WPP; датський бізнес-конгломерат Maersk, який є найбільшим оператором корабельної контейнерної доставки у світі; німецька логістична компанія DHL; американська продуктова компанія Mendelez; група американських госпіталів Heritage Valley Health System. та багато інших [1]. Перед цим, 12 травня 2017 року від вірусу-вимагача WannaCry постраждало більше 300 тисяч комп'ютерів у 150 країнах світу, а злочинці отримали понад 100 тисяч доларів [2].

Є й інші фактори, що ускладнюють протидію кіберзлочинності порівняно із злочинністю традиційною:

- повністю виключений реальний контакт злочинців і жертв;

- у момент вчинення злочину злочинці можуть перебувати, фактично, у будь-якій країні світу;

- співучасники кіберзлочинів можуть не знати один одного особисто.

Усі ці моменті значно ускладнюють викриття кіберзлочинців та притягнення їх до кримінальної відповідальності.

Знаходячись на передньому краї боротьби із злочинами у мережі Інтернет, США визначилися із основними напрямами такої боротьби та з розподілом обов'язків і сфер відповідальності державних агенцій. Так, у 2016 році були прийняті Національний план з протидії кіберзлочинності [3] та Директива-41 Президентської політики (PPD-41) [4]. У них Федеральному бюро розслідувань (ФБР) визначена ключова роль у боротьбі з кіберзагрозами. ФБР підключається у випадках значних кіберінцидентів і забезпечує координацію дій як власних «польових» агентів, так і взаємодію з іншими державними агенціями. На ФБР також покладено обов'язок забезпечити необхідну правоохоронну та слідчу діяльність, до яких відноситься збір доказів та збір розвідувальної інформації щодо осіб, які можуть представляти загрозу кібербезпеці Сполучених Штатів. Крім того, у випадку масштабних надзвичайних подій у сфері кібербезпеки, представники ФБР включаються до складу Кібернетичної об'єднаної координаційної групи (Cyber Unified Coordination Group) до якої входять представники інших федеральних агенцій, місцевих органів управління, а за необхідності залучаються також представники недержавних організацій та міжнародної спільноти.

На теперішній час у структурі ФБР, діють наступні підрозділи, метою яких є протидія комп'ютерній злочинності [5]:

- Кібернетичне Управління (Cyber Division) при штабквартирі ФБР для здійснення максимальної координації сил, задіяних у боротьбі з кіберзлочинами;

- Кібернетичні підрозділи (Cyber Squads) при штабквартирі ФБР та при кожному із 56 «польових» офісів ФБР, укомплектовані агентами та аналітиками, завданням яких є протидія незаконному втручанню у роботу комп'ютерних мереж, викраденню інтелектуальної власності та персональних даних, дитячій порнографії та експлуатації дітей, кібершахрайствам;

- Команди кібернетичної дії (Cyber Action Teams), які працюють по всьому світу та оперативно реагують на вчинення глобальних кіберзлочинів. Крім того, їхнім завдання є збір роз-

відувальної інформації стосовно можливих кіберзагроз безпеці Сполучених Штатів;

- Підрозділи боротьби з комп'ютерними злочинами (Computer Crime Task Forces), які працюють на території США і здійснюють протидію комп'ютерній злочинності, використовуючи всі доступні федеральні та місцеві ресурси.

Реалізуючи програму по боротьбі з кіберзлочинністю, ФБР тісно співпрацює з Міністерством оборони та Міністерством національної безпеки, які часто вирішують схожі задачі. Для найбільш оперативного отримання інформації щодо вчинених комп'ютерних злочинів, у рамках ФБР створено Центр з прийому заяв стосовно вчинених інтернет-злочинів (Inernet Crime Complaint Center), де як потерпілі, так і треті особи, заповнивши спеціальну форму онлайн або просто зателефонувавши, можуть надати інформацію стосовно вчинених злочинів у мережі Інтернет.

Список використаних джерел:

1. Petya (Malware). URL: https://en.wikipedia.org/wiki/Petya_(malware) (дата звернення: 28.10.2017).
2. 64 країни і 12,5 тисяч заражених комп'ютерів: у Microsoft підтвердили провину M.E.Doc. URL: https://tsn.ua/nauka_it/64-krayini-i-12-5-zarazhenih-komp-yuteriv-u-microsoft-pidtverdili-provinu-m-e-doc-953003.html (дата звернення: 28.10.2017).
3. Cybersecurity National Action Plan. URL: https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan (дата звернення: 28.10.2017).
4. Presidential Policy Directive-41. URL: https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident (дата звернення: 28.10.2017).
5. Cyber Crime – FBI. URL: https://www.fbi.gov/investigate/cyber (дата звернення: 28.10.2017).

Одержано 30.10.2017