КРИМІНАЛЬНИЙ ПРОЦЕС, КРИМІНАЛІСТИКА, ОПЕРАТИВНО-РОЗШУКОВА ДІЯЛЬНІСТЬ, СУДОВА ЕКСПЕРТИЗА, СУДОВІ ТА ПРАВООХОРОННІ ОРГАНИ

Вартовнік А.М.
студентка;
Лугіна Н.А.
кандидат юридичних наук, доцент,
Університет державної фіскальної служби України

ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ВІД КІБЕРЗЛОЧИННОСТІ В ДІЯЛЬНОСТІ СПЕЦІАЛІЗОВАНИХ ПРАВООХОРОННИХ ОРГАНІВ УКРАЇНИ

В даній роботі ми розглянули стан та проблематику забезпечення захисту від кіберзлочинності у сфері ІТ. Аналізуючи роботу щодо викриття та протидії кіберзлочинам таких правоохоронних органів як головне слідче управління МВС України та департаменту кіберполіції Національної поліції України, можемо виділити низку проблемних та спірних питань та недоліків, як от неналежне реагування на серйозні загрози інформаційній безпеці діяльності державних органів, проведення безпідставних обшуків ІТ компаній та створення несприятливого бізнес-середовища, не висока кваліфікація представників правоохоронців, що унеможливлює ефективний захист та протидію кіберзлочинності, тощо.

Мета роботи – дослідження наявних проблем протидії кіберзлочинності, що здійснюються державними правоохоронними органами, а також аналіз суперечностей та прогалин законодавства щодо запобігання та протидії кіберзлочинам.

Аналізуючи сучасні наукові праці у даній сфері, можна прослідкувати швидкий розвиток досліджень, що обумовлено актуальністю проблеми неможливості достатнього захисту від кіберзлочинів у сучасних умовах розвитку держави та швидкістю виникнення нових загроз. Вагомий внесок у дослідженні

кіберзлочинності зробили Фурашев В.М., Лук'янчук Р.В., Ткачук Т.Ю., Діордіца І.В., Островий О.В., Євсеєв С.П. Але, слід зазначити, що втілення нових наукових розробок, а також нових нормативних актів в даній сфері являється не достатньо ефективним. Існує ряд проблем у сфері протидії кіберзлочинності, що потребують нагального вирішення, оскільки під загрозою є нормальне функціонування держави, інтереси приватного сектору та безпека особи [1, с. 204].

Діяльність департаменту кіберполіції Національної поліції України полягає у забезпеченні реалізації державної політики у сфері боротьби з кіберзлочинністю, організації та здійснення оперативно-розшукової діяльності щодо протидії кримінальним правопорушенням, що готуються, вчиняються, та приховуються за допомогою використання електронно-обчислювальних машин та мереж комп'ютерного та електрозв'язку тощо [2].

Варто зазначити, що існує значний брак достатньо кваліфікованих спеціалістів в департаменті кіберполіції, не дивлячись на значне підвищення заробітної платні (від 25 000 до 50 000 гривень), спеціалісти, які відповідають вимогам конкурсу, або мають спеціальні сертифікати (деякі коштують до 5000 доларів), працюють в комерційних IT-компаніях, що створює для них найкращі умови. Спеціалістів до департаменту готує, в основному, факультет кіберполіції Харківського національного університету МВС [3].

Також, варто звернути увагу на методи реалізації державної політики, зокрема, Стратегії розвитку системи Міністерства внутрішніх справ до 2020 року, де зазначено, що одним із пріоритетних напрямів є протидія злочинності, а саме зміцнення безпеки та правопорядку, завдяки впровадженню превентивних програм і підвищенню спроможностей органів системи МВС у протидії злочинності [4]. Реалізується дане положення шляхом винаходження різних методів, що на думку департаменту кіберполіції, підвищить їх можливості в протидії кіберзлочинам. Одним із таких методів є розробка програмного скрипту, який дозволить ідентифікувати анонімних користувачів мережі Інтернет. Листи з пропозицією інсталювати код були надіслані у січні 2020 року власникам сайтів, ЗМІ та IT-компаніям, які поставилися до неї вкрай негативно. Аргументація відмови полягала у звинуваченні кіберполіції у порушенні прав людини та посилання на норми Конвенції про кіберзлочинність щодо отримання інформації про анонімних користувачів. Спеціалісти спільноти «Ukrainian Cyber Alliance» виявили

в цьому скрипті ознаки шпигунського коду. Даний скрипт був видалений з сайту департаменту кіберполіції Національної поліції України [5].

Зауважимо, що існує проблема швидкого та адекватного реагування на різні за вагомістю загрози в державному секторі ІТ, що повинна здійснюватись правоохоронними органами України. Причиною цьому, на нашу думку, є недостатньо повне та ефективне нормативне забезпечення діяльності департаменту кіберполіції Національної поліції України, який повинен дотримуватися, зокрема, Закону про Національну поліцію України від 2015 року, Положення про підрозділи особливого призначення, затвердженого Наказом Міністерства внутрішніх справ України від 04.12. 2018 року № 987, норм Конвенції Ради Європи про кіберзлочинність, що ратифікована Верховною Радою України від 07.09.2005 року, Доктрина інформаційної безпеки України, Законів України «Про основи національної безпеки», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», Кримінального, Кримінально-процесуального кодексів, а також Кодексу про адміністративні правопорушення, та інших підзаконних нормативних актів, положень, посадових інструкцій. Це призводить до порушення принципів верховенства права та законності, нечіткості в розподілу пріоритетів роботи кіберполіції та інших проблем [6].

На підтвердження цього існують такі факти, як наприклад, за даними Інтернет-партії України портали Міністерства охорони здоров'я України мають суттєві вразливості, також визначається перелік інших «вразливих» державних порталів. Це може призвести до отримання злочинниками прав адміністратора всього сервера. Наслідки недостатньої захищеності сайтів вже добре відомі державі та громадськості. При зараженні вірусами комп'ютерних систем у 2017 році кібератаці піддались такі державні структури та приватні компанії як: Кабінет Міністрів, «Укренерго», аеропорт Бориспіль та інші. Розв'язати цю проблему вдалось із неофіційним залученням спеціалістів із Держспецзв'язку, комерційних структур та громадських організацій. За 2019 рік CERT-UA зареєструвала 330 кіберінцидентів, пов'язаних з кібератаками на сайти органів державної влади України, наразі перелік міністерств та кількість атак є інформацією з обмеженим доступом.

Також, зазначимо, що департамент кіберполіції, Національної поліції та головне слідче управління МВС України проводить обшуки ІТ-компаній, та відкриває кримінальні провадження, що потім не доходять до суду. Причини обшуків: пошук терористів, неліцензійного і

порнографічного контенту, податкові правопорушення. Так, 27 лютого 2020 року на основі Постанови Печерського суду міста Києва був проведений обшук в міжнародній компанії MGID. Причина проведення слідчих дій – підозра у фінансуванні злочинних сайтів. При чому, як повідомляють представники компаній в Поставі суду були відсутні такі відомості як: перелік злочинних сайтів, час і місце злочину, спосіб вчинення злочину [7].

Отже, можемо зробити висновок про існування проблем та недоліків в діяльності правоохоронних органів щодо забезпечення захисту від кіберзлочинності. Низка проблем, наприклад, низька якість кваліфікації кіберполіції, нездатність протидіяти кіберзлочинам в інформаційній сфері діяльності державних органів, проведення безпідставних обшуків ІТ компаній тощо. Розв'язати ці питання можна шляхом подальшого наукового та практичного дослідження наявних проблем протидії кіберзлочинності, усунення суперечностей та прогалин законодавства щодо запобігання та протидії кіберзлочинам та суттєве його доповнення, а також залучення спеціалістів з комерційних сфер задля перевірки та допомоги в захисті об'єктів критичної інформаційної інфраструктури України.

Список використаних джерел:

1. Матеріали всеукр. наук.-практ. конф. Кібербезпека в Україні: правові та організаційні питання (Одеса, 21 жовтня 2016 р.). – Одеса : ОДУВС, 2017, 204 с.

2. Департамент кіберполіції Національної поліції України // Офіційний сайт. URL: https://cyberpolice.gov.ua/contacts/

3. Наказ Міністерства внутрішніх справ України від 17.11.2015 № 1465 «Про затвердження Інструкції про порядок проведення атестування поліцейських». URL: https://zakon.rada.gov.ua/laws/show/z1445-15

4. Розпорядження Кабінету Міністрів України Про схвалення Стратегії розвитку органів системи Міністерства внутрішніх справ на період до 2020 року від 15 листопада 2017 року, № 1023-р. URL: https://zakon.rada.gov.ua/laws/show/1023-2017-%D1%80

5. Кіберполіція пропонує інтернет-ЗМІ встановити скрипт для деанонімізації користувачів. Інтернет видання. 2020. URL: https://ukr.lb.ua/society/2020/01/30/448590_kiberpolitsiya_proponuie_internetzmi.html

6. Основні засади забезпечення кібербезпеки. Електронне видання. 2018. URL: https://uteka.ua/ua/publication/news-14-delovye-novosti-36-osnovnye-principy-obespecheniya-kiberbezopasnosti-ukrainy

7. Електронний ресурс спільноти програмістів. 2020. URL: https://dou.ua/forums/topic/29851/