УДК [351.741:336-049.5](477)

Сергій Миколайович ГУСАРОВ,
доктор юридичних наук, професор,
член-кореспондент Національної академії правових наук України,
заслужений юрист України,
професор кафедри адміністративного права та процесу
факультету № 1 Харківського національного університету
внутрішніх справ;
ORCID: https://orcid.org/0000-0002-8136-0694

ЗАБЕЗПЕЧЕННЯ ФІНАНСОВОЇ БЕЗПЕКИ ДЕРЖАВИ ДЕПАРТАМЕНТОМ КІБЕРПОЛІЦІЇ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ В УМОВАХ ДІЇ ВОЄННОГО СТАНУ

Нині майже кожен в Україні використовує мобільні засоби комунікації з підключенням до інтернету, державні органи впроваджують електронний документообіг, банківські послуги надаються онлайн, можна замовити послуги з перевезення залізницею, автобусом чи літаком, а підприємницьку діяльність неможливо уявити без онлайн сегмента. Відбулося всеосяжне проникнення кіберпростору у всі сфери життєдіяльності суспільства та держави, в тому числі фінансову. Переоцінити стабільність і безпеку кіберпростору для забезпечення фінансової безпеки держави неможливо.

Істотну роль у забезпеченні фінансової безпеки держави відіграє Департамент кіберполіції Національної поліції України – міжрегіональний територіальний орган Національної поліції України, який входить до структури кримінальної поліції та відповідно до законодавства забезпечує реалізацію державної політики у сфері боротьби з кіберзлочинністю, організовує та здійснює оперативно-розшукову діяльність. Основними завданнями Департаменту кіберполіції Національної поліції України є:

1) участь у формуванні та забезпеченні реалізації державної політики щодо попередження та протидії кримінальним правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку;

2) сприяння у порядку, передбаченому чинним законодавством, іншим підрозділам Національної поліції у попередженні, виявленні та припиненні кримінальних правопорушень [1].

Офіційна статистика свідчить, що за останнє десятиліття кількість виявлених кіберзлочинів суттєво збільшилась. В умовах війни кібератаки і злами можливі з боку ворога для завдання шкоди обороноздатності України. Скористатися ситуацією з перевантаженістю правоохоронних органів та заволодіти коштами громадян мають намір не пов'язані з війною зловмисники. Тому кіберзлочинність в Україні стабільно зростає [2].

Через обмеженість у кадровому ресурсі кіберполіція розслідує лише справи, в яких ідеться про великі суми грошей, втручання в державні реєстри, хакерські атаки на великі мережі та сайти, продаж піратської продукції або баз даних (масштабні інтернет-злочини). Численні ж випадки шахрайства в мережі розслідують здебільшого територіальні органи Національної поліції.

Протягом 2022–2023 рр. Департаментом кіберполіції Національної поліції України здійснюється протидія кіберзлочинності, пов'язаної з війною, та протидія російському ворогу в інформаційному просторі. Наочно продемонструвати внесок кіберполіції в забезпечення фінансової безпеки держави в умовах дії воєнного стану можна на прикладах такої діяльності за останній час. Так, працівники Департаменту кіберполіції викрили злочинну групу, яка оформлювала кредити на зниклих безвісти і полонених військовослужбовців. Для реалізації злочинної схеми зловмисники здійснювали перевипуск сім-карт та отримували доступ до онлайн-банкінгу. Далі оформлювали кредитні картки та привласнювали позики. Загальна сума збитків становить понад 2 млн грн. Було повідомлено про підозру за ч. 3 ст. 190 («Шахрайство») Кримінального кодексу України [3].

Ще одним напрямом роботи є викриття кіберполіцеєю ботоферм, через які поширюється ворожий контент. Так, наприклад, заходи з викриття ботоферми провели працівники відділу протидії кіберзлочинам у Тернопільській області спільно з оперативниками обласного управління Служби безпеки України та слідчими поліції. Мешканець Тернополя за місцем свого проживання організував роботу апаратно-програмного комплексу, який використовував потужності близько 30 тисяч сім-карт для реєстрації великої кількості облікових записів. Із фейкових акаунтів у соціальних мережах розповсюджували неправдиву інформацію та протиправний контент, у тому числі на вебресурсах, заборонених на території України. Зокрема, дописи й коментарі містили прокремлівські наративи, виправдання окупації українських територій, пропаганду війни, дискредитували захисників України або представників органів влади.

За фактом цього розпочато кримінальне провадження за ч. 3 ст. 361 («Несанкціоноване втручання в роботу інформаційних (автоматизованих), інформаційно-комунікаційних систем, електронних комунікаційних мереж») Кримінального кодексу України [4].

Також поширеним є шахрайство під виглядом постачання товарів військовим. В інтернеті розміщуються оголошення щодо продажу, наприклад, автомобілів, однак, отримавши передплату, особи не виконують взятих на себе обов'язків. Використовуються фейкові облікові записи у соціальних мережах для публікації оголошень щодо продажу автомобілів, які мають попит серед військових та волонтерів, котрих переконують, що про продаж уже домовились з іншим покупцем, але за умови передплати обіцяють «притримати» автівку. Такі дії кваліфікуються за ч. 3 ст. 190 («Шахрайство») Кримінального кодексу України.

Відмітимо діяльність Департаменту кіберполіції з протидії колаборaційній діяльності та пропаганді, спрямованій на підтримку російської агресії. Одним з останніх прикладів є документування працівниками Департаменту кіберполіції протиправної діяльності громадянки України, адвоката і блогерки, яка неодноразово висловлювалася на підтримку країни-агресора, поширювала російську пропаганду та фейки і на початку повномасштабного вторгнення виїхала до рф. Пропагандистці заочно оголошено підозру за ч. 1 ст. 111-1 («Колаборaційна діяльність»), ч. 3 ст. 436-2 («Виправдовування, визнання правомірною, заперечення збройної агресії Російської Федерації проти України, глорифікація її учасників»), ч. 2 ст. 110 («Посягання на територіальну цілісність і недоторканність України»), ч. 3 ст. 109 («Дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади») Кримінального кодексу України [5].

У лютому 2023 р. працівники управління протидії кіберзлочинам у Харківській області викрили протиправну діяльність фігурантів, що створили та адміністрували скам-спільноту в месенджері «Telegram», де розміщували інструкції та фішингові посилання для інших членів шахрайської організації. Далі зловмисники в месенджерах робили розсилку фішингових посилань, що містили пропозицію отримати соціальну допомогу від держави або отримати кошти за проданий товар. Після введення потерпілим реквізитів своєї банківської карти зловмисники отримували доступ до його коштів. Організатору повідомлено про підозру за частинами 1–2 ст. 255 («Створення та участь у злочинній організації»), ч. 4 ст. 28, ч. 3

ст. 190 («Шахрайство»), виконавцям – за ч. 2 ст. 255, ч. 4 ст. 28, ч. 3 ст. 190 Кримінального кодексу України [6].

Наостанок відмітимо, що до завдань кіберполіції входять: реалізація державної політики у сфері протидії кіберзлочинності, завчасне інформування населення про появу нових кіберзлочинців, упровадження програмних засобів для систематизації кіберінцидентів, реагування на запити зарубіжних партнерів, які надходять каналами цілодобової мережі контактних пунктів.

Працівники Департаменту кіберполіції в контексті дії воєнного стану зосереджують увагу на пов'язаному з війною шахрайстві (ст. 190 КК України), несанкціонованому втручанні в роботу інформаційних (автоматизованих), інформаційно-комунікаційних систем, електронних комунікаційних мереж (ст. 361 КК України), колабораційній діяльності (ст. 111-1 КК України), виправдовуванні, визнанні правомірною, запереченні збройної агресії російської федерації проти України, глорифікації її учасників (ст. 436-2 КК України), посяганні на територіальну цілісність і недоторканність України (ст. 110 КК України), діях, спрямованих на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади (ст. 109 КК України).

Список бібліографічних посилань

1. Про підрозділ // Кіберполіція України : офіц. сайт. URL: https://cyberpolice.gov.ua/contacts/.

2. Боротьба з кіберзлочинністю в умовах дії воєнного стану: Закон 2149-IX // LIGA ZAKON : сайт. 13.04.2022. URL: https://jurliga.ligazakon.net/analitycs/210562_borotba-z-kberzlochinnstyu-v-umovakh-d-vonnogo-stanu-zakon-2149-ix.

3. Кіберполіція викрила злочинну групу, яка оформлювала кредити на зниклих безвісти і полонених військовослужбовців // Кіберполіція України : офіц. сайт. 03.03.2023. URL: https://www.cyberpolice.gov.ua/news/kiberpolicziya-vykryla-zlochynnugrupu-yaka-oformlyuvala-kredyty-na-znyklyx-bezvisty-i-polonenyx-vijskovosluzhbovcziv-8913/.

4. Кіберполіцейські спільно з оперативниками СБУ викрили ботоферму, через яку поширювали ворожий контент // Головне управління Національної поліції в Тернопільській області : офіц. сайт. 03.01.2023. URL: https://tp.npu.gov.ua/news/kiberpolitseiski-spilno-z-operatyvnykamy-sbu-vykryly-botofermu-cherez-iaku-poshyriuvaly-vorozhyi-kontent.

5. Правоохоронці оголосили підозру у колабораційній діяльності пропагандистці, яка підтримує російську агресію // Кіберполіція

України : офіц. сайт. 10.02.2023. URL: https: //www.cyber-police.gov.ua/news/pravooxoronczi-ogolosyly-pidozru-u-kolaboraczijnij-diyalnosti-propagandystczi-yaka-pidtrymuye-rosijsku- agresiyu-3412/.

6. Поліцейські Харківщини викрили в онлайн шахрайстві злочинну організацію, члени якої підозрюються у нанесенні потерпілим мільйонних збитків // Кіберполіція України : офіц. сайт. 02.02.2023. URL: https://www.cyberpolice.gov.ua/news/policzejski-xarkivshhyny-vykryly-v-onlajn-shaxrajstvi-zlochynnu-organizacziyu-chleny-yakoyi-pidozryuyutsya-u-nanesenni-poterpilym-miljonnyx-zbytkiv-5622/.

УДК 004.7:538.56:519.25

Олександр Анатолійович МОРГУНОВ,
доктор юридичних наук, професор,
заслужений тренер України,
перший проректор Харківського національного
університету внутрішніх справ;
ORCID: https://orcid.org/0000-0003-2259-3620

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ ФІНАНСОВОЇ БЕЗПЕКИ ПІДПРИЄМСТВА В УМОВАХ ВОЄННОГО СТАНУ

Економічно-політичні виклики в країні, що постали сьогодні, стали причиною фінансової незахищеності більшості громадян. Зокрема, початок повномасштабної війни та запровадження воєнного стану спровокували появу реальних ризиків і загроз у веденні підприємницької діяльності [1]. Огляд наукових джерел з питань трактування сутності поняття «фінансова безпека підприємства» свідчить, що більшість учених дотримуються лінії, яка базується на визначенні фінансової безпеки держави, тільки екстраполюють її на мікрорівень: «І в загальному випадку фінансову безпеку підприємств представляють як механізм, що, з одного боку, забезпечує стабільність фінансової системи суб'єкту шляхом використання захисних фінансових інструментів, а з іншого, – забезпечує її ефективність шляхом організації раціонального використання фінансових ресурсів» [2;3].