дослідження для ефективного розв'язання експертних завдань цього напрямку.

Перелік джерел посилання

1. Науково-методичні рекомендації з питань підготовки та призначення судових експертиз та експертних досліджень (додаток до Інструкції про призначення та проведення судових експертиз та експертних досліджень, затвердженої наказом Міністерства юстиції України від 08 жовтня 1998 р. № 53/5 (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/z0705-98#Text (дата звернення: 03.03.2023).
2. Реєстр методик проведення судових експертиз, затверджений наказом Міністерства юстиції України від 2 жовтня 2008 р. № 1666/5 (зі змін. та допов.). URL: http://rmpse.minjust.gov.ua (дата звернення: 03.03.2023).
3. Коваль Н. Л. Розроблення методичних рекомендацій з проведення судово-психологічних експертиз у кримінальних справах з питань застосування психологічного впливу (заключ.). Київ, 2011. 67 с.
4. Методика судово-психологічної експертизи комунікативної взаємодії між особами, зафіксованої у матеріалах відеозапису з камери зовнішнього спостереження (реєстр. код – 14.1.76).
5. Експертиза відео-, звукозапису. URL: https://www.hniise.gov.ua/7-products.html (дата звернення: 03.03.2023).

Проблема кібертероризму та шляхи боротьби з кіберзлочинністю

Світлана Ходосевич,
ННЦ «ІСЕ ім. Засл. проф. М. С. Бокаріуса», м. Харків, Україна, ORCID: https://orcid.org/0000-0001-7885-7766, e-mail: hodosevichsvetlana07@gmail.com

Висвітлено сучасні проблеми боротьби з кіберзлочинністю на державному рівні. Ураховуючи глобалізацію злочинів через інтернет, висловлено думку про необхідність побудови протидії та попередження таких злочинів, використовуючи світовий досвід.

Ключові слова: кіберзлочини; кібертероризм; комп'ютерна злочинність.

The issue of cyberterrorism and ways of countering cybercrime

Svitlana Khodosevych

Current problems of countering cybercrime at the state level are emphasized. Taking into account globalization of crimes through the Internet, a suggestion was made about the need to counteract and prevent such crimes, using world experience.

Keywords: cybercrime; cyberterrorism; computer crime.

На сучасному етапі розвитку міжнародних відносин дедалі більшого значення набувають передові комп'ютерні технології, еволюція яких призвела до широкого використання інтернету.

Кіберпростір поєднав тисячі комп'ютерних мереж і мільйони комп'ютерів у всьому світі та став важливим інструментом для обміну політичною, економічною, торговельною та споживчою інформацією.

Унаслідок зростання популярності інтернету виник один із найнебезпечніших видів кіберзлочинності — кібертероризм. Проблема кібертероризму є глобальною та актуальною в сучасному інформаційному суспільстві. За відносно короткий проміжок часу кібератаки перетворилися з поодиноких випадків на одну з основних загроз інформаційній безпеці держав.

Для досягнення своїх цілей кібертероризм використовує електронні мережі, сучасні інформаційно-комунікаційні технології та радіоелектроніку. Особлива небезпека кібертероризму полягає в тому, що він не має меж, адже всі події відбуваються у віртуальному світі, де відсутнє належне правове регулювання на думку міжнародного і вітчизняного законодавства.

Особливо небезпечними є втручання в інформаційну безпеку критично важливих інфраструктур: комп'ютерних систем управління банківською сферою, обороною, промисловістю та ін. Реалізація таких загроз може призвести до небезпечних наслідків для суспільства та держави [1, с. 86]. Наприклад, 2015 р. було зламано сайт для знайомств одружених людей *Ashley Madison* із 40 млн користувачів. Хакери отримали доступ

до бази даних та виклали в публічний доступ із можливістю пошуку за адресами електронної пошти. У травні 2021 р. хакери атакували бази даних нафтової компанії *Pipeline*, унаслідок чого кілька днів не працював нафтовий трубопровід, що доставляв 45 % пального для східного узбережжя США [2].

В Україні перша масштабна хакерська атака сталася у червні 2017 р., у результаті якої було заблоковано діяльність аеропорту «Бориспіль», ЧВЕС, «Укртелекому», «Укрпошти», «Ощадбанку», «Укрзалізниці» та ін. [3]. Починаючи з січня 2022 р., кількість масштабних кібератак на українські державні сайти суттєво зросла. Наприклад, 14 січня 2022 р. було атаковано близько 70 українських державних сайтів, побудованих на *CMS October* компанії *Kitsoft*, унаслідок чого постраждала значна кількість державних сайтів, зокрема Міністерства оборони, Міністерства закордонних справ, Державної служби України з надзвичайних ситуацій та ін. [4]. Атака 15—16 лютого 2022 р. на державні та банківські сайти України тривала більше 5 год, спричинивши проблеми з доступом до близько 15 українських банків (зокрема «Приватбанку» й «Ощадбанку») та сайти домена gov.ua. Вартість наслідків цих атак склала мільйони доларів, однак злочинцям не вдалося досягти своєї мети через швидку реакцію відповідальних за кібербезпеку органів та допомогу аналогічних служб США [5]. Унаслідок атаки на державні ресурси та банки 23 лютого 2022 р. постраждали вебпортали Кабміну, Верховної Ради, МЗС та ін., на зламаних сайтах почали працювати шкідливі програмні засоби *HermeticWiper*, метою яких є знищення інформації з баз даних [6].

У день нападу Російської Федерації на Україну 24 лютого 2022 р. було атаковано сайт Київської облдержадміністрації, на сайтах meta.ua та i.ua було виявлено електронні листи з фішинговими посиланнями на приватні адреси українських військових та пов'язаних з ними осіб [7].

У відповідь на такі масштаби загрози світовій спільноті необхідно розробити відповідні міжнародні стратегії боротьби з кіберзлочинністю та унормувати їх. Перші кроки в цьому напрямі здійснили поки тільки окремі країни. Так, у Великій Британії основним документом, спрямованим на забезпечення кібербезпеки, є Стратегія національної кібербезпеки, основна мета якої полягає в забезпеченні стійкості державних і приватних інституцій до кіберзагроз. У Німеччині у липні 2015 р. було прийнято Закон про інформаційну безпеку з метою запобігання нападам на важливі інформаційні системи, який визначає стандарти кібербезпеки для більше ніж 2000 компаній критичної інфраструктури. Цих стандартів безпеки можна досягти завдяки покращенню доступності, достовірності, конфіденційності та цілісності безпеки по всій країні; а також поліпшенню захисту критичної інфраструктури загальнодержавного значення.

Україна протягом останніх років так само крокує в напрямі розбудови інформаційного суспільства, забезпечення кібербезпеки та боротьби з кібертероризмом. Нормативно-правову базу в цих сферах діяльності становлять Конвенція Ради Європи про кіберзлочинність, ратифікована Законом України від 07.09.2005 р. № 2824-IV, а також Закони України «Про основні засади кібербезпеки України», «Про Державну службу спеціального зв'язку та захисту інформації України», «Про інформацію» тощо; відповідні Укази Президента України (наприклад, «Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року "Про план реалізації Стратегії кібербезпеки України"» від 01.02.2022 р. № 37/2022), положення Кримінального кодексу України, окремі постанови Кабінету Міністрів та рішення Ради національної безпеки та оборони України. Також діє команда реагування на комп'ютерні надзвичайні події України (*CERT-UA*) [8], що постійно вживає заходів щодо взаємодії з іншими командами CERT інших країн, а також із розвідувальною групою *Cisco Talos* із питань подолання наслідків кібератак на критичну інформаційну інфраструктуру та виявлення причин та обставин кіберінцидентів.

Незважаючи на проведену роботу з розроблення і прийняття нормативно-правових документів у сфері кіберзлочинності, Україна перебуває на початкових етапах розвитку цієї сфери.

Тому загальне оцінювання проблем інформаційної безпеки, пошук шляхів та методів протидії кіберзлочинності є ключовими напрямами забезпечення національної безпеки України. До них належать:

- визначення міжнародно-правового статусу кіберпростору;
- нормативно-правове закріплення юрисдикції держави щодо національних складових кіберпростору і подальше врегулювання питань, пов'язаних із кібервійною та кібератаками;

- упровадження уніфікованого поняття кіберзлочинності та чіткої систематизації відповідних діянь;
- посилення контролю в інтернеті та ін.

Також необхідно продовжувати та розширяти міжнародне співробітництво в галузі кібербезпеки, що може містити розроблення узгоджених критеріїв і методів оцінювання ефективності систем і засобів забезпечення інформаційної безпеки, взаємне визнання сертифікатів продукції у сфері захисту інформації, розширення взаємодії у розв'язанні науково-технічних і правових питань забезпечення безпеки інформації. Необхідною умовою успішної взаємодії є зміцнення взаємодії правоохоронних органів різних країн щодо запобігання комп'ютерним злочинам та притягнення до юридичної відповідальності за них.

Перелік джерел посилання

1. Інформаційні виклики гібридної війни: контент, канали, механізми протидії: аналіт. доп. / за заг. ред. А. Баровської. Київ, 2016. 109 с.
2. PaySpace Magazine. URL: https://psm7.com (дата звернення: 09.03.2023).
3. Кібератаки на українські державні сайти (2022) / Вікіпедія. URL: https://uk.wikipedia.org (дата звернення: 09.03.2023).
4. Російські хакери атакували 70 державних сайтів, українські активи падають / Економічна правда. URL: https://www.epravda.com.ua (дата звернення: 09.03.2023).
5. Кібератака в Україні 15 лютого була найбільшою в історії держави: в Кабміні назвали вартість / УНІАН. URL: https://www.unian.ua (дата звернення: 09.03.2023).
6. Федоров розповів подробиці чергової атаки хакерів проти України / Слово і діло. URL: https://www.slovoidilo.ua (дата звернення: 09.03.2023).
7. Ворог атакує email-адреси українських військових на сервісах i.ua і meta.ua — Держспецзв'язку / Економічна правда. URL: https://www.epravda.com.ua (дата звернення: 09.03.2023).
8. Computer Emergency Response Team of Ukraine. URL: https://cert.gov.ua (дата звернення: 09.03.2023).

Концептуальні засади проведення комплексних судових економічних та товарознавчих експертиз, пов'язаних із визначенням розміру матеріальної шкоди, завданої власникам пошкодженого майна у зв'язку зі збройною агресією Російської Федерації

Ольга Холодова,
канд-ка техн. наук, доцентка, смт. Слобожанське, Дніпропетровська обл., Україна,
ORCID: https://orcid.org/0000-0001-8678-3955, e-mail: kholodova1984@ukr.net,
Алла Лисенко,
м. Підгородне, Дніпропетровська обл., Україна, ORCID: https://orcid.org/0000-0001-8193-4267,
e-mail: dnipro.sed@gmail.com,

Наведено концептуальні засади проведення комплексної судової економічної та товарознавчої експертизи в контексті визначення розміру реальних збитків унаслідок пошкодження, втрати і / або знищення єдиних майнових комплексів підприємств, установ та організацій усіх форм власності, керуючись положеннями Методики визначення шкоди та обсягу збитків, завданих підприємствам, установам та організаціям усіх форм власності внаслідок знищення та пошкодження їх майна у зв'язку із збройною агресією РФ, а також упущеної вигоди від неможливості чи перешкод у провадженні господарської діяльності.

Ключові слова: комплексна судова економічна та товарознавча експертиза; матеріальна шкода; збитки; єдиний майновий комплекс підприємств.