Список використаних джерел

1. Антощук А. О. Використання спеціальних знань при розслідуванні вбивства матір'ю своєї новонародженої дитини. *Юридичний вісник. Повітряне і космічне право*. № 2. 2016. С. 162–167.
2. Антощук А. О. Огляд місця події при виявленні трупа новонародженої дитини. *Науковий вісник національної академії внутрішніх справ*. № 2. 2013. С. 243–250.
3. Кримінальний процесуальний кодекс України : Кодекс України від 13 квітня 2012 року № 4651-VI. URL : https://zakon.rada.gov.ua/laws/show/4651-17#Text.
4. Кримінальний кодекс України : Кодекс України від 5 квітня 2001 року № 2341-III. URL : https://zakon.rada.gov.ua/laws/show/2341-14#Text.

Гуцалюк Михайло Васильович,
Міжвідомчий науково-дослідний центр з проблем боротьби з організованою злочинністю при РНБО України, кандидат юридичних наук, старший науковий співробітник, доцент

ПОСИЛЕННЯ КІБЕРБЕЗПЕКИ: ЄВРОПЕЙСЬКИЙ ДОСВІД

У 2014 році розпочалася перша в світі кібервійна між РФ та Україною. Руйнівні дії агресора у кіберпросторі були продовженням військової агресії та важливим елементом гібридної війни. Під час 2014–2021 роками хакерськими угрупованнями та спецслужбами РФ були здійснені кібератаки на українські енергосистеми, залізничні станції та різноманітні державні установи. Вірус NotPetya, який був активізований напередодні дня Конституції України у 2017 році визнаний фахівцями як найбільш руйнівна хакерська атака.

Нова стадія кібервійни розпочалася у 2022 році. У ніч повномасштабного вторгнення 24 лютого 2022 року ворог хотів знищити весь кіберзахист України. За одну ніч було нейтралізовано понад 120 потужних кібератак на ресурси різних органів державної влади та військового управління. А за перший місяць війни за повідомленням Телеграм-каналу Держспецзв'язку кількість кібератак зросла втричі. Найпопулярнішими видами кібератак залишаються фішингові розсилання, розповсюдження шкідливого програмного забезпечення та DDoS-атаки [1].

Зазначені дії країни-агресора змушують шукати нові заходи щодо забезпечення кіберстійкості національного інформаційного простору і в першу чергу об'єктів критичної інформаційної інфраструктури.

Враховуючи нещодавнє прийняття України в кандидати в члени ЄС, доцільно звернути увагу на заходи щодо посилення кіберстійкості в Європейському Союзі.

Відповідно до Директиви Європейського Парламенту і Ради (ЄС) 2016/1148 від 6 липня 2016 року «Про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу» усі держави-члени повинні ухвалити національні стратегії безпеки мережевих та інформаційних систем, створити мережу груп реагування на інциденти, пов'язані з комп'ютерною безпекою («мережа CSIRT»), встановити вимоги до безпеки та повідомлення для операторів основних послуг та надавачів цифрових послуг.

Щоб відповісти на зростаючі загрози, пов'язані з цифровізацією та сплеском кібератак, Європейська Комісія подала пропозицію замінити Директиву NIS на NIS2 [2] і, таким чином, посилити вимоги безпеки. Текст документа був погоджений у травні 2022 року. У ньому зокрема передбачено розглянути питання безпеки ланцюгів постачання, оптимізувати зобов'язання щодо звітності та запровадити більш жорсткі вимоги та наглядові заходи щодо виконання положень директиви, включаючи узгоджені санкції ЄС. Запропоновані заходи допоможуть підвищити рівень кібербезпеки в Європі в довгостроковій перспективі.

У вересні 2022 року Європейською комісією був розроблений Cyber Resilience Act [3]. Даним документом визначено чотири конкретні цілі:

1) забезпечити, щоб виробники покращували безпеку продуктів із цифровими елементами, починаючи з фази проектування та розробки та протягом усього життєвого циклу;

2) забезпечити узгоджену структуру кібербезпеки, сприяючи відповідності для виробників обладнання та програмного забезпечення;

3) підвищення прозорості властивостей безпеки продуктів із цифровими елементами та

4) дозволити компаніям і споживачам безпечно використовувати продукти з цифровими елементами.

В Україні національна Стратегія кібербезпеки була прийнята у травні 2016. Хоча вона мала суттєвий позитивний вплив на розвиток національної системи кібербезпеки, водночас через різні обставин багато завдань, визначені у стратегічному документі за 5 років не були вирішені.

Враховуючи нові виклики та кіберзагрози, зокрема безпосередньо від рф, у серпні 2021 року були прийнята нова Стратегія кібербезпеки України.

Стратегією визначено виклики та кіберзагрози на сучасному етапі, зазначені конкретні цілі та завдання щодо розвитку безпечного кіберпростору. У серпні 2021 року Президент України ввів в дію Рішення РНБО України від 14 травня 2021 року «Про невідкладні заходи з кібероборони держави», яким передбачено створення та функціонування у системі Міністерства оборони України кібервійськ.

Водночас, як було зазначено вище кібервійна внесла свої корективи у методи та способи захисту кіберпростору. Зокрема Законом України на Держспецзв'язку було покладено завдання

створення та забезпечення функціонування системи активної протидії агресії у кіберпросторі.

Починаючи від 23.02.2022, Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA проведено десятки досліджень цільових атак, спрямованих на виведення з ладу інформаційно-комунікаційних систем і порушення конфіденційності інформації, яка в них обробляється.

У переважній більшості інцидентів початковою точкою компрометації є публічна інформаційна система з неоновленим і/або налаштованим за замовчанням програмним забезпеченням. Тому виконання вимог як вітчизняного законодавства так і посилення кібербезпеки на основі європейський стандартів надасть змогу більш ефективно захищати вітчизняний інформаційний простір від кібератак країни-агресора.

Вдосконалення належної правової системи на основі європейських нормативних актів у сфері кібербезпеки є необхідним елементом розбудови дієвої кібероборони України.

Список використаних джерел

1. За місяць війни кількість кібератак зросла втричі – Держспецзв'язку. URL : https://tech.liga.net/ua/ukraine/novosti/za-mesyats-voyny-chislo-kiberatak-vyroslo-v-tri-raza-gosspetssvyazi.

2. The NIS2 Directive: A high common level of cybersecurity in the EU. URL : https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333.

3. Cyber Resilience Act – Impact assessment. URL : https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-impact-assessment.

Дульський Олександр Леонідович,
докторант Національної академії внутрішніх справ, доктор філософії

КРИМІНАЛІСТИЧНЕ ЗАБЕЗПЕЧЕННЯ ЗБИРАННЯ ДОКАЗІВ ОРГАНАМИ ДОСУДОВОГО РОЗСЛІДУВАННЯ В УМОВАХ ВОЄННОГО СТАНУ

На сьогодні, у зв'язку з воєнним станом на території нашої держави, особлива увага прикута до сектору безпеки держави. Зрозуміло, що населення наразі більшою мірою спостерігає за роботою Збройних Сил України та тих правоохоронних органів, які безпосередньо протидіють ворогу «на полі бою». Водночас, не можемо не зауважити на тому, що на теперішній час окремими підрозділами правоохоронної системи відбувається і збір фактичних даних, що можуть бути доказами вчинення кримінальних правопорушень окупантами. Це теж є важливою діяльністю підрозділів правоохоронних органів (органів досудового розслідування), які уповноважені це робити, адже від якісного збирання такої слідової інформації і залежатиме справедливе покарання зловмисників як у