Виходом з подібних ситуацій є застосування до викривачів заходів безпеки у вигляді забезпечення конфіденційності даних про особу, що передбачено ст. 15 Закону України «Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві», а саме зміна анкетних даних викривача. Однак це вимушений захід.

Підсумовуючи, конфіденційність – це основа співробітництва правоохоронних органів з відповідальними громадянами, це основоположна гарантія прав викривача і суворий обов'язок для правоохоронців, а тому персональна інформація про викривача може бути відома тільки конкретній уповноваженій особі на таке співробітництво і зберігатися в порядку та в умовах, які забезпечують її конфіденційність.

Тому гарантія конфіденційності повинна бути безумовною та безвиключною, а персональна інформація про викривача може бути розкрита тільки за його згодою і тільки з метою вирішення питання про виплату йому грошової винагороди в суді. Також на викривача може бути покладений обов'язок не розголошувати відомості про факт і деталі конфіденційного співробітництва та вжиті заходи безпеки.

Список використаних джерел

1. Презентація: Корупція в Україні 2020: розуміння, сприйняття, поширеність. Національне агентство з питань запобігання корупції: [офіційний вебсайт]. URL: https://nazk.gov.ua/wp-content/uploads/2020/05/Corruption_Survey_2020_Presentation_Info-Sapiens.pdf, вільний.

Когут Юрій Іванович,
генеральний директор ТОВ «Консалтингова компанія «СІДКОН», член Всесвітньої Асоціації Детективів (WAD), здобувач Навчально-наукового інституту права ім. князя Володимира Великого Міжрегіональної академії управління персоналом

РЕАЛІЗАЦІЯ ДЕРЖАВНОЇ АНТИКОРУПЦІЙНОЇ ПОЛІТИКИ В ПРОЦЕСІ УПРАВЛІННЯ НАЦІОНАЛЬНОЮ СИСТЕМОЮ КІБЕРБЕЗПЕКИ

Указом Президента України від 14.09.2020 р. №392/2020 [6] затверджено Стратегію національної безпеки України «Безпека людини – безпека країни», якою, у тому числі, визначені основні пріоритети розвитку національної системи кібербезпеки в державі, наголошено основне завдання розвитку системи кібербезпеки – гарантування кіберстійкості та кібербезпеки національної інформаційної інфраструктури, зокрема в умовах цифрової трансформації. Стратегією національної безпеки України передбачено завершити створення національної системи кібербезпеки, сформувати

сучасні спроможності суб'єктів забезпечення кібербезпеки і кібероборони та зміцнити систему їх координації.

Відповідно до чинного законодавства [5] до основних суб'єктів національної системи кібербезпеки відносяться Державна служба спеціального зв'язку та захисту інформації (Держспецв'язку), Національна поліція України, Служба безпеки України (СБУ), Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України. Крім того, Рада національної безпеки і оборони України (РНБОУ) фактично виступає координатором цих суб'єктів національної системи кібербезпеки. Приватний бізнес та кіберспільнота до вирішення важливих питань із забезпечення кібербезпеки та протидії кібертероризму в Україні майже не залучаються. Національна система кібербезпеки обмежується переважною участю в ній правоохоронних органів (Національна поліція України, СБУ) та Держспецв'язку тощо.

На сьогодні відсутній трансформаційний підхід до управління національною кібербезпекою, що передбачає наявність організації (організацій), яка (які) керуватиме впровадженням державної програми з кібербезпеки, та регулярного контролю за процесом її впровадження [7], внесення відповідних змін у чинне законодавство. Закон України «Про основні засади забезпечення кібербезпеки України» [5] не визначає державний орган, який би управляв упровадженням кібербезпеки на загальнонаціональному рівні [3, с. 57].

Крім того, Законом України «Про основні засади забезпечення кібербезпеки України» [5] не визначено єдиний орган, основною функцією якого мало б стати оперативне управління над всіма суб'єктами забезпечення кібербезпеки у мирний час [3, с. 57]. Це може стати значною проблемою, адже функції інших державних органів, які входять у склад національної системи кібербезпеки, чітко не розмежовані, а це приводить до дублювання деяких повноважень, що, на нашу думку, є недопустимим. Наприклад, у сфері захисту кіберпростору від кіберзагроз завданням РНБОУ є здійснення лише координації та стратегічного управління, а Генштабу – оперативне командування в «особливий період».

Також значною проблемою у процесі здійснення протидії кібертероризму є наділення Держспецзв'язку надмірними повноваженнями щодо аудиту об'єктів критичної інфраструктури, що є приватною власністю. Так, згідно з п.1 ч. 2 ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України» [5] Держспецзв'язку забезпечує впровадження аудиту інформаційної безпеки на об'єктах критичної інфраструктури, встановлює вимоги до аудиторів інформаційної безпеки, визначає порядок їх атестації (переатестації); координує, організовує та проводить аудит захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість.

Отже, суперечливими є норми, що визначають порядок впровадження кібераудиту на об'єктах національної критичної інфраструктури. Насамперед, це зачепить весь великий та середній

бізнес. У той же час, Держспецзв'язку наділений правом визначення вимог для аудиторів, що здійснюють кібераудит, та щодо порядку їх атестації [3, с. 57]. Це несе в собі загрозу тиску зі сторони держави на бізнес, адже можна надавати «своїм підприємствам» ліцензії щодо проведення такого кібераудиту. Це також може стати поштовхом для розвитку корупційних схем.

Законом «Про основні засади забезпечення кібербезпеки України» [5] встановлено, що порядок та методика здійснення аудиту кібербезпеки здійснюються на основі міжнародних стандартів, проте в його прикінцевих та перехідних положеннях немає жодної згадки про чинний Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [4], згідно з ч. 2 ст. 8 якого «державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю». Очевидно, що під дію цієї норми потрапляють практично всі об'єкти критичної інформаційної інфраструктури, значна кількість яких перебуває в недержавному секторі (наприклад, в енергетиці, транспортній системі, телеком-індустрії, фармацевтиці тощо) [2, с. 56]. При цьому Комплексна система захисту інформації (КСЗІ)[1], базована на українському стандарті КСЗІ НД ТЗІ 2.5–004–99, і вимога її обов'язкового застосування на об'єктах національної критичної інформаційної інфраструктури здебільшого піддається гострій критиці у вітчизняних експертних та бізнесових колах [2, с. 56].

Водночас, досі у відповідності до ст. 10 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» [4] Держспецзв'язку визначає вимоги та порядок створення комплексної системи захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом; організовує проведення державної експертизи комплексних систем захисту інформації, експертизи та підтвердження відповідності засобів технічного і криптографічного захисту інформації.

Поряд із розкритими вище недоліками чинного законодавства з питань кібербезпеки, які стосуються суперечливих положень щодо особливостей проваджуваної діяльності Держспецзв'язку, відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» [5] Службі безпеки України також надається надмірне право проводити таємні перевірки щодо кібербезпеки критичних об'єктів [3, с. 58]. Це, по суті, є загрозою тотального шпигунства.

З метою запровадження саморегуляції у кіберпросторі та зменшення корупційних ризиків у діяльності державних регулюючих органів у сфері забезпечення кібербезпеки доцільно суттєво зменшити

[1] Комплексна система захисту інформації – взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації.

повноваження Держспецзв'язку. Необхідно створити інституцію оперативного реагування на кіберінциденти у приватному секторі приватними фахівцями, досвід і кваліфікація яких буде підтверджена Держспецзв'язком. Після отримання підтвердження кваліфікації державного зразка вони зможуть надавати консультаційну допомогу будь-якій державній чи приватній структурі, яка цього потребує [1].

Список використаних джерел

1. Демедюк С. Кібербезпека у цифрову епоху: чи готова Україна до нових викликів? URL: https://www.pravda.com.ua/columns/2020/08/7/7262150/.

2. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України: аналіт. доп. / за заг. ред. Д. Дубова. К.: НІСД, 2018. 84 с.

3. Петровський О. М., Лівчук С. Ю. Проблеми боротьби з кіберзлочинністю: міжнародний досвід та українські реалії. *Young Scientist*. 2019. № 12.1 (76.1). С. 55–59.

4. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 р., № 80/94-ВР (із змінами). URL: https://zakon.rada.gov.ua/laws/main/80/94-вр#Text.

5. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р., № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/main/2163-19#Text.

6. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»: Указ Президента України від 14.09.2020 р., № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#n7.

7. Янковський О. Україні потрібна нова кіберстратегія. URL: https://www.pravda.com.ua/columns/2019/09/14/7226291/.

Крижна Валентина Володимирівна,
старший науковий співробітник наукової лабораторії з проблем протидії злочинності Національної академії внутрішніх справ, кандидат юридичних наук, старший науковий співробітник

ПРАВОВІ АСПЕКТИ ПРОТИДІЇ КОРУПЦІЇ НА МІЖНАРОДНОМУ РІВНІ

В Україні на сучасному етапі розвитку суспільства та державного механізму проблема протидії корупції є однією із провідних. У зв'язку із цим в останні декілька років ведеться трансформація антикорупційного законодавства, що також пов'язано з активними європейськими інтеграційними процесами, прагненням України стати повноправним учасником міжнародних відносин та наблизити вітчизняне законодавство до міжнародних стандартів.