КІБЕРСТІЙКІСТЬ І ПРАВА ЛЮДИНИ: ПРАВОВІ КРИТЕРІЇ ДОПУСТИМОГО ВТРУЧАННЯ

Юрій Олександрович ВИХОДЕЦЬ,

доктор філософії, доцент, професор кафедри кримінології та інформаційних технологій Національної академія внутрішніх справ

В умовах воєнного стану, інтенсивної цифровізації публічного управління та зростання залежності держави від електронних комунікацій забезпечення кіберстійкості набуває не лише технічного, а й виразного правового значення. Кіберстійкість у цьому аспекті слід розглядати як здатність держави, її органів, операторів критичної інфраструктури та інших уповноважених суб'єктів забезпечувати безперервність цифрових функцій, своєчасно реагувати на кіберінциденти та водночас не допускати невиправданого обмеження прав людини.

Особливого значення набувають чотири критерії допустимого втручання у права людини: законність, легітимна мета, необхідність та пропорційність. Їх застосування дозволяє відмежувати правомірні заходи кіберзахисту від надмірного цифрового контролю, невизначеного збору даних, непрозорого обміну інформацією, тривалого зберігання технічних журналів або необґрунтованого обмеження доступу до цифрових ресурсів.

Конституційною основою такого підходу є положення статті 32 Конституції України, відповідно до якої не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини [1]. Близьку логіку закріплено у статті 8 Конвенції про захист прав людини і основоположних свобод (Європейська Конвенція з прав людини), яка допускає втручання органів державної влади у право на повагу до приватного і сімейного життя лише тоді, коли таке втручання здійснюється згідно із законом, переслідує легітимну мету та є необхідним у демократичному суспільстві [2].

Закон України «Про основні засади забезпечення кібербезпеки України» визначає правові й організаційні основи захисту життєво важливих інтересів людини і громадянина, суспільства та держави у кіберпросторі [3]. Водночас сам факт наявності кіберзагрози або кіберінциденту не може автоматично виправдовувати будь-який обсяг втручання у приватність, персональні дані чи цифрову комунікацію особи. Саме тому питання допустимості такого втручання має вирішуватися не лише через призму технічної доцільності, а передусім через правовий тест законності, легітимної мети, необхідності та пропорційності.

У науковій та нормативній площині проблематика кібербезпеки традиційно розглядається через захист інформаційних систем, електронних комунікацій, протидію кіберзлочинності, забезпечення цифрової

безперервності та реагування на інциденти. Окремий блок досліджень і нормативного регулювання становлять питання захисту персональних даних, права на приватність, процесуального використання цифрової інформації та відповідальності держави у цифровому середовищі.

Закон України «Про захист персональних даних» прямо пов'язує регулювання обробки персональних даних із захистом основоположних прав і свобод людини, зокрема права на невтручання в особисте життя [4]. У праві Європейського Союзу подібна логіка розвинута в Загальному регламенті про захист даних – GDPR, який закріплює принципи законності, справедливості, прозорості, обмеження мети, мінімізації даних, точності, обмеження строку зберігання, цілісності, конфіденційності та підзвітності обробки персональних даних [5].

Разом із тим менш розробленим залишається питання про те, яким саме юридичним механізмом має перевірятися допустимість заходів кіберстійкості, якщо вони пов'язані з обробкою даних, моніторингом цифрового середовища, фіксацією технічних журналів, обміном інформацією між державними і приватними суб'єктами або подальшим використанням отриманої інформації у правоохоронній діяльності.

У цьому контексті важливе значення має Директива ЄС NIS2, яка вводить підхід, за яким суб'єкти мають застосовувати належні та пропорційні технічні, операційні й організаційні заходи управління кіберризиками, а також забезпечувати повідомлення про значні інциденти [6]. Такий підхід є важливим для України, оскільки він демонструє перехід від вузького технократичного розуміння кібербезпеки до ризик-орієнтованої, підзвітної та процедурно врегульованої моделі кіберстійкості.

Кіберстійкість у правовому вимірі не може зводитися лише до здатності цифрової системи витримати кібератаку, локалізувати її наслідки та відновити функціонування. У демократичній правовій державі така здатність повинна супроводжуватися юридичними гарантіями, які визначають межі втручання у приватність, персональні дані, таємницю комунікацій, доступ до цифрових сервісів і право на ефективний засіб правового захисту.

Першим критерієм є законність. Заходи кіберстійкості, які передбачають обробку персональних даних, доступ до технічних журналів, моніторинг мережевої активності, передачу інформації між суб'єктами або обмеження доступу до цифрових ресурсів, мають здійснюватися на підставі чіткої правової норми. Така норма повинна визначати уповноважений суб'єкт, підстави втручання, мету обробки даних, категорії інформації, межі доступу, строки зберігання, порядок документування та механізми контролю. Формальне посилання на потреби кібербезпеки без конкретизації правового режиму не відповідає вимогам правової визначеності, що випливає зі змісту ст. 32 Конституції України та ст. 8 Конвенції [1; 2].

Другим критерієм є легітимна мета. Забезпечення кіберстійкості може переслідувати захист національної безпеки, громадської безпеки, стабільності критичної інфраструктури, прав інших осіб, безперервності електронних комунікацій і належного функціонування публічних цифрових

сервісів. Однак легітимна мета не повинна перетворюватися на універсальне виправдання будь-якого втручання. Кожний захід має бути пов'язаний із конкретною кіберзагрозою, інцидентом, ризиком або потребою запобігання істотній шкоді. Саме таке розуміння відповідає логіці Закону України «Про основні засади забезпечення кібербезпеки України», який пов'язує кібербезпеку із захистом життєво важливих інтересів людини, суспільства та держави [3].

Третім критерієм є необхідність. Втручання у права людини може бути виправданим лише тоді, коли без нього неможливо або істотно ускладнено досягнення мети кіберстійкості. Необхідність означає, що суб'єкт владних повноважень або оператор відповідної системи повинен обґрунтувати, чому саме цей захід є потрібним, чому менш інтенсивні засоби є недостатніми, а також чому втручання не виходить за межі конкретної ситуації. У сфері обробки персональних даних це узгоджується з принципом мінімізації даних, закріпленим у ст. 5 GDPR, відповідно до якого персональні дані мають бути адекватними, релевантними та обмеженими тим, що є необхідним для відповідних цілей обробки [5].

Четвертим критерієм є пропорційність. Навіть законний, легітимний і необхідний захід не може вважатися правомірним, якщо його наслідки для прав людини є надмірними порівняно з очікуваним безпековим результатом. Пропорційність вимагає співмірності між масштабом кіберзагрози та глибиною втручання. Наприклад, тривале зберігання технічних журналів, передача даних між різними суб'єктами, блокування інформаційного ресурсу, автоматизований аналіз мережевої активності або подальше використання технічних даних у кримінальному провадженні мають отримувати окреме правове обґрунтування. Такий підхід кореспондує з NIS2, яка вимагає застосування належних і пропорційних технічних, операційних та організаційних заходів управління кіберризиками [6].

У правоохоронній діяльності ці критерії мають особливе значення. Дані, отримані під час реагування на кіберінцидент, можуть мати оперативну, аналітичну або доказову цінність, однак їх подальше використання повинно залежати від дотримання належної правової процедури. Технічна корисність інформації не замінює її процесуальної допустимості. Тому між кіберзахисним реагуванням і кримінальним процесом має існувати чіткий правовий перехід: із фіксацією походження даних, способу їх отримання, цілісності, автентичності, суб'єкта доступу, мети обробки та меж подальшого використання.

Висновки.

1. Критерії законності, легітимної мети, необхідності та пропорційності доцільно розглядати як базовий правовий тест допустимості заходів кіберстійкості. Його застосування дозволяє оцінювати не лише технічну ефективність реагування на кіберзагрози, а й правомірність впливу таких заходів на приватність, персональні дані, доступ до цифрових сервісів і процесуальні гарантії особи.

2. Забезпечення кіберстійкості потребує переходу від моделі ситуативного реагування до моделі юридично контрольованого втручання.

Практичне значення має не тільки факт наявності кіберзагрози, а й належне обґрунтування того, чому конкретний захід є правово визначеним, спрямованим на легітимну мету, необхідним у конкретній ситуації та співмірним із відповідним ризиком.

3. Для України перспективним є закріплення процедурного стандарту правозахисного оцінювання кіберзахисних заходів. Такий стандарт має охоплювати визначення меж обробки даних під час кіберінцидентів, документування підстав втручання, контроль за передачею інформації між суб'єктами, аудит рішень після завершення реагування та окремі гарантії використання технічних даних у кримінальному провадженні.

Список використаних джерел:

1. Конституція України: Закон України від 28.06.1996 № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80
2. Конвенція про захист прав людини і основоположних свобод (з протоколами) : Конвенція Ради Європи, міжнародний документ, Протокол від 04.11.1950 р. : ст. 8.
3. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII. Офіційний вебпортал Верховної Ради України.
4. Про захист персональних даних: Закон України від 1 червня 2010 року № 2297-VI. Офіційний вебпортал Верховної Ради України.
5. Regulation (EU) 2016/679 (GDPR). OJ L 119, 4.5.2016, p. 1-88. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj
6. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) № 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive). *Official Journal of the European Union.* L 333/80. 27.12.2022. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555