Бібліографічні посилання

1. Internet Society – всесвітня громадська організація під управлінням широкої опікунської ради. URL: http://www. internetsociety.org/sites/default/files/bpdeconstructing-cybersecurity-16nov-update. doc.doc_RU_121712.pdf «Погляди на кібербезпеку: 2012г.»
2. CNews|безпека Сергей Попсулин. URL: http:// safe.cnews.ru/news/top/index. shtml?2013/08/02/537614&utm_ source=twitterfeed&utm_medium=twitter «ФБР здатна дистанційно включати мікрофони в смартфонах Android»
3. Hi-tech.UA. Доля iOS втрое ниже чем Android, но денег на приложения в ней тратят в 2 раза больше. URL: https://hi-tech.ua/dolya-ios-vtroe-nizhe-chem-android-no-deneg-na-prilozheniya-v-nej-tratyat-v-2-raza-bolshe/#:~:text=%D0%94%D0%BE%D0%BB%D1%8F%20iOS%20%D0%BD%D0%B0%20%D1%80%D1%8B%D0%BD%D0%BA%D0%B5%20%D0%BC%D0%BE%D0%B1%D0%B8%D0%BB%D1%8C%D0%BD%D1%8B%D1%85,Android%20%D0%B2%20Google%20Play%20Store.

Калашнік Є. О.,
курсант 2-го курсу факультету
підготовки фахівців для органів
досудового розслідування
Науковий керівник – Прокопов С. О.,
старший викладач кафедри
економічної та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ

ПРАВОВЕ РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЯК ПІДҐРУНТЯ ВІЛЬНОГО ІНФОРМАЦІЙНОГО ПРОСТОРУ В УКРАЇНІ

Забезпечення інформаційної безпеки в наш час стає одним із безперечно нагальних питань не тільки для діяльності фахівців з ІТ-сфери й науковців, що здійснюють фахові дослідження з суміжних інформаційних питань, а й для виокремлення такого необхідного, чітко регламентованого нормативного підґрунтя. Доля інформаційного простору, із врахуванням сучасних тенденцій до інформатизації, поставлена під питання, відповіді на які багато в чому залежать від стану і тенденцій розвитку економіки та інформаційної безпеки загалом. Необхідність в дослідженні публічно-правових міжгалузевих та міжсистемних механізмів регулювання й стабільного функціонування інформаційної безпеки є беззаперечною й однією з найбільш актуальних.

Аналізуючи раніше згадану необхідність, варто зазначити один з найбільш показових прикладів зовнішнього інформаційного впливу на

Україну, а саме безпосередні дії Російської Федерації щодо інформаційного забезпечення анексії Автономної Республіки Крим та організації сепаратистських заворушень у південно-східних регіонах нашої держави. Тобто ще від початку 2014 року з боку Росії здійснювався надпотужний інформаційно-психологічний тиск на суб'єкти інформаційного простору України й населення загалом, нарощувалася інформаційна експансія в національний інформаційний простір, захоплювались стратегічні об'єкти вітчизняної телекомунікаційної інфраструктури.

Зазначені події знайшли відображення в реальності на тлі, насамперед, відсутності узгодженої, а також заздалегідь зваженої державної політики України у сфері саме інформаційної безпеки, що характеризувалася низькою ефективністю як системи державного регулювання національним інформаційним простором, так і прогалинами й фрагментарністю вітчизняного нормативно-правового поля у зазначеній сфері.

Опрацьовуючи чинну нормативну базу, досить легко помітити, що поняття «інформаційної безпеки України» досить широко застосовується як в Конституції України, так і в низці інших нормативно-правових актів, що підготовлені та затверджені органами і законодавчої, і виконавчої влади.

Однак, наприклад, в Законі України «Про національну безпеку України», що є безперечно основним орієнтиром забезпечення безпеки нашої держави, сутність «інформаційної безпеки» подано як невід'ємний складник національної безпеки України без точного визначення цього поняття [1].

Справді, істотним зрушенням у нормативно-правовому регулюванні національної безпеки в інформаційному просторі стало розроблення та введення в дію Доктрини інформаційної безпеки України (далі – Доктрина), яка була підготовлена відповідно до статті 107 Конституції України, частини другої статті 2 Закону України «Про основи національної безпеки України» та постановляла «Увести в дію рішення Ради національної безпеки і оборони України від 22 жовтня 2021 року «Про Концепцію реформування Державної служби спеціального зв'язку та захисту інформації України» (додається), затвердити Концепцію реформування Державної служби спеціального зв'язку та захисту інформації України (додається), а також Кабінету Міністрів України забезпечити реалізацію Концепції реформування Державної служби спеціального зв'язку та захисту інформації України [2].

Варто зазначити, що ця Доктрина стала першим вітчизняним нормативно-правовим документом, у якому проголошується особливе місце інформаційної безпеки в системі забезпечення національної безпеки, по-перше, як невід'ємного складника кожної зі сфер забезпечення національної безпеки, а по-друге, як важливої самостійної сфери забезпечення національної безпеки [3]. До того ж вагомою новацією зазначеної Доктрини стало чітке виокремлення трьох головних напрямів «національних інтересів» державної політики у забезпеченні інформаційної безпеки України: технологічного розвитку, захисту інформації та «інформаційно-

психологічного, зокрема щодо «створення сприятливого психологічного клімату в національному інформаційному просторі» [4].

Проте для продуктивного забезпечення всебічного становлення зазначеної Доктрини необхідно мати документи, які б послідовно деталізували її в аспектах, наприклад, концепції інформаційної безпеки України, створенні чітких схем чи форм стратегії інформаційної безпеки України, формуванні програми та плану імплементації положень попереднього документа. Однак такі документи й досі не розроблені і не введені в дію. Вже декілька років серед актуальних є низка нових законопроєктів стосовно інформаційної безпеки держави, а саме «Про засади інформаційної безпеки України», «Про кібернетичну безпеку України», «Про внесення змін до деяких законів України щодо забезпечення кібернетичної безпеки України». Саме в цих законопроєктах встановлено та зазначено спроби до вирішення наявних недоліків чинного законодавства.

Підсумовуючи, зазначимо: забезпечення суверенітету інформаційного простору та гарантування інформаційної безпеки України з нормативно-правового погляду має бути комплексним і містити:

– уніфікацію та чітке тлумачення загальних положень законодавства;

– конструктивно обмірковане забезпечення державою стратегічно важливих напрямів розвитку і захисту національного інформаційного простору;

– визначення та врегулювання засад і меж діяльності як вітчизняних, так і закордонних суб’єктів інформаційних відносин у національному інформаційному просторі України;

– зосередження принципів, засад та методів щодо захисту національних інтересів України як у міжнародних, так і в національних, визначених законом, інформаційних відносинах.

Визначаючи ж позитивні зрушення в зазначеній тематиці інформаційної безпеки, їх доцільно зазначити не лише завдяки затвердженню рекомендацій Комітету цифрової трансформації України від 31 березня 2021 року «Електронна демократія в Україні – дорожня мапа для цілі – Україна в ТОП-20 країн за розвитком електронної демократії» для Кабінету Міністрів України та відповідним органам влади щодо прискорення процесу розробки законопроєктів, що дозволять ефективно протидіяти наявним кіберзагрозам, здійсненню перевірки та вжиття невідкладних заходів щодо припинення можливих витоків інформації та здійсненню заходів щодо перевірки наявності комплексних систем захисту інформації в кожній із зазначених у ЗУ «Про основні засади забезпечення кібербезпеки України» установах, а й завдяки здійсненим владними ешелонами загалом крокам, що полягають як у затвердженні офіційного курсу країни на вдосконалення наявного стану безпеки інформаційного простору, так і в поступовому й раціональному прокладанні шляху до створення повноцінної об’єктивно комплексної системи захисту інформації.

Бібліографічні посилання

1. Про національну безпеку України : Закон України. Документ 2469-VIII, чинний, поточна редакція. Редакція від 01.08.2021, підстава – 1702-IX.
2. Рішення Ради національної безпеки і оборони України від 22 жовтня 2021 року «Про Концепцію реформування Державної служби спеціального зв'язку та захисту інформації України» : Указ Президента України від 22 жовтня 2021 року № 544/2021.
3. Конах В. К. Нормативно-правові засади державної політики України у сфері інформаційно-психологічної безпеки. *Стратегічні пріоритети*. 2012. № 3 (24). С. 152–157.
4. У Комітеті з питань цифрової трансформації відбулися слухання на тему: «Електронна демократія в Україні – дорожня карта для цілі – Україна в ТОП-20». URL: https://thedigital.gov.ua/news/komitet-rozglyanuv-4-zakonoproekti-ta-obgovoriv-praktiku-vikonannya-zakonodavstva-pro-kiberbezpeku-z-derzhavnimi-organami

Калюжна А. О., слухачка
магістратури юридичного факультету
Науковий керівник – Косиченко О. О.,
доцент кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

РИЗИКИ ВИКОРИСТАННЯ СИСТЕМ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ

Біометрія все частіше використовується для ідентифікації громадян у різних сферах життя: для отримання банківських послуг, для складання он-лайн іспитів, оплати проїзду на транспорті тощо [1–3]. Біометричні дані вважаються «надчутливими». При цьому виникають питання довіри до штучного інтелекту стосовно ухвалення остаточних рішень. І збереження паперових копій документів у багатьох випадках має сенс. Тобто є певні ризики використання біометричних даних.

Біометричні дані, на відміну будь-яких інших, що використовуються для ідентифікації, є невід'ємною частиною кожної людини. На відміну від пароля, номера телефону та прізвища, що використовуються зараз, не можна в разі витоку або компрометації даних, змінити своє обличчя, сітківку, фігуру, відбитки пальців тощо. Це надчутливі, але при цьому незмінні дані, які, в принципі, можна вкрасти.

Біометрична інформація та інші, персональні або платіжні дані, що зберігаються в конкретних базах даних, схильні до банальних витоків, кількість яких у всіх сферах життя неухильно зростає. Це відбувається