***Довгань О. Д.**, д.ю.н., с.н.с., Науково-дослідний інститут інформатики і права Національної академії правових наук України.*

ІНФОРМАЦІЙНА БЕЗПЕКА: СТАН, ПРОБЛЕМИ, ТЕНДЕНЦІЇ

У статті проаналізовано особливості інформаційної безпеки в контексті розвитку інформаційної сфери. Визначено стан, проблеми, тенденції та перспективи діалектики інформаційної безпеки.

Ключові слова: інформаційне середовище, інформаційна безпека, засоби захисту інформації.

Розвиток інформаційної сфери – це важливий напрям державної політики, безсумнівний курс розвитку України. Від здатності держави розробити та реалізувати ефективну інформаційну політики, доктрину, концепцію та стратегію значною мірою залежить її майбутнє існування.

Інформація та інформаційні ресурси стають стратегічним здобутком і найважливішими чинниками поступу людини, суспільства і держави. Інформаційна сфера дедалі більше впливає на політичну, економічну, соціокультурну, оборонну, інші складові розвитку суспільства й держави, а врешті-решт, на забезпечення національної безпеки в сучасних умовах.

Відповідно до Закону України «Про основи національної безпеки України» інформаційна безпека є окремою сферою забезпечення національної безпеки. Водночас вона також є невід'ємною складовою кожної із сфер національної безпеки. Саме тому розвиток України як суверенної, демократичної, правової та економічно стабільної держави можливий тільки у разі досягнення належного рівня її інформаційної безпеки.

Тому в умовах викликів сьогодення та розвитку інформаційного суспільства проблема забезпечення інформаційної безпеки набуває якісно нового значення і в правовому вимірі виступає як невід'ємна складова сучасної системи управління на шляху до правової держави і як суттєвий

чинник формування громадянського суспільства, забезпечуючи поступальний розвиток його інформаційної основи – національних інформаційних ресурсів. Все це вимагає зміни філософії забезпечення інформаційної безпеки.

Це пояснюється перш за все застосуванням країною-агресором по відношенню до України технологій гібридної війни, у першу чергу в інформаційній сфері, що в свою чергу сформувало нові виклики та загрози інформаційній безпеці держави. Кібернетичні атаки на інформаційні ресурси держави стали невід'ємним компонентом такої гібридної війни. В таких умовах актуальними на сьогодні залишаються питання необхідності створення цілісної та узгодженої системи забезпечення інформаційного суверенітету, управління ризиками і можливостями новітніх викликів в інформаційній сфері, розбудови власних спроможностей надійних та достовірних державних комунікацій та створення тісної взаємодії між органами влади, формування інфраструктури національного інформаційного простору з метою створення умов для його інтегрування у світовий інформаційний простір, налагодження комунікаційного процесу між органами влади та споживачами інформації. Тому питання інформаційної безпеки, у т.ч. її складової - кібербезпеки, та їх правового забезпечення, у нашій державі має надзвичайно велике значення.

По-друге. Динаміка і тенденції розвитку сучасних викликів і загроз інформаційній безпеці України свідчать, що їх виявлення, припинення чи нейтралізація ускладнюється комплексом внутрішніх негативних факторів, до яких відносимо:

- неефективність державної інформаційної політики, в тому числі відсутність цілісної комунікативної політики як всередині держави, так і у зовнішніх зносинах *(заслуговують на підтримку оцінки, що в Україні фактично відсутня цілісна системна інформаційна політика, не має єдиної узгодженої стратегії розвитку інформаційної галузі, плану*

консолідованих дій та спільного бачення засобів реагування на серйозні загрози й виклики);

- неналежний стан національного законодавства з питань інформаційної безпеки України, відсутність концептуальних правових засад її забезпечення, надто повільні темпи проведення відповідних реформ;

- відсутність належної координації діяльності суб'єктів забезпечення інформаційної безпеки, дублювання їх функцій, а також недостатньо ефективне співробітництво державних установ з громадянським суспільством;

- неефективне управління безпекою критичної інфраструктури, уразливість до кібератак її об'єктів та державних інформаційних ресурсів; критична зношеність її основних фондів та недостатній рівень їх фізичного захисту;

- недостатній розвиток національної інформаційної інфраструктури, насамперед, в зоні проведення антитерористичної операції;

- відсутність комплексної системи підготовки фахівців у вищих навчальних закладах для сфери інформаційної безпеки України, зокрема, за напрямом протидії негативним інформаційним впливам.

Зупинимося на проблемах стану національного законодавства з питань інформаційної безпеки України. Перед цим зробимо деякі ремарки. Як не дивно, але факт, на сучасному етапі технології, а з ними зміст і особливості суспільних відносин, які базуються на їх використанні, змінюються та розвиваються набагато швидше, ніж нормативно-правове поле, яке має відношення до цього. Все це вимагає створювати правові норми, які будуть не фіксувати, а формувати майбутні суспільні відносини в інформаційній сфері, тобто працювати на випередження розвитку соціуму, а не фіксувати нормами права вже сформовані та усталені підходи до їх регулювання.

Крім того, для інформаційної сфери є критично важливою наявність відповідних політико-правових документів, затверджених на найвищому

державному рівні. Оскільки такі документи формують бажану модель предметної сфери і є важливим чинником формування наукової правосвідомості.

Що ми маємо реально на сьогодні в правовому полі. Далеко в історію заглиблюватися не будемо. Візьмемо період з 2014 року, після «Революції гідності», анексії Криму, окупації окремих районів Донецької та Луганської областей. За цей період на державному рівні прийнято ряд нормативно-правових актів: Указ Президента України № 449/2014 від 1 червня 2014 р. [522], яким уведено в дію рішення Ради національної безпеки і оборони України від 28 квітня 2014 р. «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України». Вказаним документом, серед іншого, передбачено (передбачалося) приведення національного законодавства у відповідність із міжнародними стандартами з питань інформаційної та кібернетичної безпеки, вдосконалення системи формування та реалізації державної політики у сфері інформаційної безпеки України тощо.

Тепер зробимо невелику оцінку, прийнятих актів з питань кібербезпеки та інформаційної безпеки. Що ми бачимо. По кібербезпеці:

Прийнята Стратегія національної безпеки України *(травень 2015р.)* визначила загрози кібербезпеці і безпеці інформаційних ресурсів та безпеці критичної інфраструктури. При цьому до пріоритетів забезпечення кібербезпеки і безпеки інформаційних ресурсів Стратегією віднесено (розвиток інформаційної інфраструктури держави; створення системи забезпечення кібербезпеки, розвиток мережі реагування на комп’ютерні надзвичайні події (CERT); моніторинг кіберпростору з метою своєчасного виявлення, запобігання кіберзагрозам і їх нейтралізації; розвиток спроможностей правоохоронних органів щодо розслідування кіберзлочинів; забезпечення захищеності об’єктів критичної інфраструктури, державних інформаційних ресурсів від кібератак, відмова від програмного забезпечення, зокрема антивірусного, розробленого у

Російській Федерації; реформування системи охорони державної таємниці та іншої інформації з обмеженим доступом, захист державних інформаційних ресурсів, систем електронного урядування, технічного і криптографічного захисту інформації з урахуванням практики держав - членів НАТО та ЄС; створення системи підготовки кадрів у сфері кібербезпеки для потреб органів сектору безпеки і оборони; розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки, інтенсифікація співпраці України та НАТО, зокрема в межах Трастового фонду НАТО для посилення спроможностей України у сфері кібербезпеки.)

Якщо детально розглянути ці пріоритети, то видно, що фактично був визначений реальний дороговказ, що потрібно робити і куди далі рухатися.

З набуттям чинності Стратегії кібербезпеки України *(січень 2016 року)* наша країна підтвердила наміри у напрямі розбудови національної системи кібербезпеки (на державному рівні задекларовано, що пріоритетами й напрямами забезпечення кібербезпеки в сучасних умовах є: розвиток безпечного, стабільного та надійного кіберпростору; кіберзахист державних електронних інформаційних ресурсів і критичної інформаційної інфраструктури; розвиток потенціалу сектору безпеки і оборони у сфері забезпечення кібербезпеки; боротьба з кіберзлочинністю тощо).

Далі було ухвалено низку доктринальних документів і підзаконних нормативно-правових актів, серед яких *Концепція розвитку сектору безпеки і оборони України,* затверджена Указом Президента України від 14.03.16 р. № 92/2016 (визначає, що одним із основних завдань сектору безпеки і оборони є забезпечення інформаційної та кібербезпеки, створення національної системи кібербезпеки з використанням можливостей суб’єктів сектору безпеки і оборони для ефективної боротьби із кіберзагрозами воєнного характеру, кібершпигунством, кібертероризмом та кіберзлочинністю, розвитку мережі реагування на комп’ютерні надзвичайні події (CERT).), *Стратегічний оборонний бюлетень,* введений

в дію Указом Президента України від 06.06.16 р. № 240, *Положення про Національний координаційний центр кібербезпеки*, затверджено Указом Президента України від 07.06.16 р. № 242/2016, *Порядок формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави,* затверджений постановою Кабінету Міністрів України від 23.08.16 р. № 563. Указами Президента України від 16 січня №8/2017 введено в дію рішення РНБО України від 29 грудня 2016 року «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури» та від 13 лютого 2017 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації» та інші.

На виконання Стратегії кібербезпеки України розпорядженням Кабінету Міністрів України від 24.06.16 р. № 440-р було затверджено план заходів на 2016 рік з реалізації зазначеної Стратегії. Крім цього, цілий розділ 4.4. Річної національної програми «Україна - НАТО» *(квітень 2017р.)* присвячено кібербезпеці.

Все це є підтвердженням важливості питань, що стосуються кібербезпеки, а зазначені акти по суті вказують на поштовх до розгортання національної системи забезпечення кібербезпеки.

Однак, на жаль, у нашій державі існує негативна тенденція щодо невжиття окремими суб'єктами, які наділені владними повноваженнями, планових заходів, затверджених на державному рівні. Тому, була відповідна реакція з боку держави і рішенням Ради національної безпеки і оборони України від 29.12.16 р., уведеним в дію Указом Президента України від 13.02.17 р. № 32/2017, в якому акцентовано увагу на необхідності термінової підготовки законодавчих пропозицій щодо кіберзахисту об'єктів критичної інформаційної інфраструктури, посилення відповідальності за невиконання вимог законодавства стосовно захисту інформації в інформаційно-телекомунікаційних системах та законних вимог посадових осіб органів Державної служби спеціального зв'язку та захисту інформації України, а також щодо запровадження відповідальності

за невиконання законних вимог посадових осіб Служби безпеки України, розробки низки правових новел у сфері кібербезпеки.

Окремо потрібно говорити про проект Закону України "Про основні засади забезпечення кібербезпеки України", який було прийнято за основу Верховною Радою України у вересні 2016 р. Проте, зазначений проект далекий від досконалого, на що науковцями справедливо було звернуто увагу.

Нещодавно стало відомо, що вже існує доопрацьований проект для другого читання та прийняття в цілому. Нажаль замало залучають науковий світ до обговорення та проведення наукової експертної оцінки законопроектів.

Що ми маємо в цілому по інформаційній безпеці. До 2014 року діяла Доктрина інформаційної безпеки України від 8 липня 2009 року, яка втратила силу на підставі Указу Президента України від 6 червня 2014 року №504/2014. І майже 2,5 роки не було прийнято жодного документу на заміну, вже не кажучи про розробку та прийняття відповідного закону. Згодом, лише у лютому 2017 р. була схвалена нова Доктрина інформаційної безпеки України *(Указ Президента України від 25 лютого 2017 року №47/2017)*. Що це за доктрина? Приведемо вислови експертів, які дали як позитивну, а здебільшого негативну оцінку.

«Доктрина – документ компромісу між інтересами суспільства й держави. Доктрина інформаційної безпеки України – це лише декларація. Документ є, але нічого не регулює».

На питання чого так довго розроблявся акт. У керівників МІП знайшлося пояснення: *«*...затягування з ухваленням Доктрини пояснюється бюрократизмом, а також бажанням зробити процес її розробки максимально прозорим*»*. Це було сказано не дивлячись на такий стан в державі та тих подій, що відбуваються навколо України.

Більше коментувати з цього приводу не будемо, лише поставимо питання: Де було експертне середовище?, у т.ч. наукове, громадське

обговорення. Чи відповідає зміст (наповнення) доктрини її назві? Набагато з них ми відповіді не знайдемо.

Напевно, потрібно сьогодні (мабуть в черговий раз) піднімати питання щодо розробки нормативного акту (закону), яким буде визначено єдиний понятійно-категоріальний апарат, державну політику забезпечення інформаційної безпеки, об'єкти інформаційної безпеки та суб'єкти її забезпечення, правові зони відповідальності відомств, залучених до сфери забезпечення інформаційної безпеки, механізми координування їх діяльності щодо реагування на виклики та загрози національній безпеці в інформаційній сфері, порядок правового закріплення взаємовідносин державних безпекових структур із іншими органами та відомствами, віднесеними законодавством до суб'єктів забезпечення національної безпеки України та ін. Таким чином потрібно говорити про створення загальнодержавної системи забезпечення інформаційної безпеки.

Тому, прийняття цілого ряду нормативно-правових актів має не просто убезпечити країну та захистити її від ряду нових загроз, але і переформатувати роботу і спецслужб, й інших державних органів. Звичайно, це стане можливим за наявності політичної волі та комплексного бачення майбутнього розвитку країни.

Простого виходу із такої ситуації не має. Рішення повинно бути комплексним і комбінованим. Питання інформаційної безпеки, а також її складової кібербезпеки – це питання виживання країни і можливості її розвитку. Час стискається, світ змінюється і, якщо не вжити необхідних заходів сьогодні, через декілька років ми будемо не в змозі наздогнати ці процеси.

Список використаної літератури:

1. Стратегія національної безпеки України, затверджена Указом Президента України від 26 травня 2015 року № 287/2015 // Офіційне інтернет-представництво Президента України [Електронний ресурс]. − Режим доступу: http: //www.president.gov.ua.

2. Стратегія кібербезпеки України, затверджена Указом Президента України від 15.03.16 р. № 96/2016 // Офіційне інтернет-представництво Президента України [Електронний ресурс]. − Режим доступу: http: //www.president.gov.ua.

3. Концепція розвитку сектору безпеки і оборони України, затверджена Указом Президента України від 14.03.16 р. № 92/2016// Офіційне інтернет-представництво Президента України [Електронний ресурс]. − Режим доступу: http: //www.president.gov.ua.

4. Стратегічний оборонний бюлетень, уведений в дію Указом Президента України від 06.06.16 р. № 240// Офіційне інтернет-представництво Президента України [Електронний ресурс]. − Режим доступу: http: //www.president.gov.ua.

5. Положення про Національний координаційний центр кібербезпеки, затверджене Указом Президента України від 07.06.16 р. № 242/2016// Офіційне інтернет-представництво Президента України [Електронний ресурс]. − Режим доступу: http: //www.president.gov.ua.

6. Порядок формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави, затверджений постановою Кабінету Міністрів України від 23.08.16 р. № 563 // http://zakon0.rada.gov.ua/laws/show/563-2016-%D0%BF

Dovgan Olexandr

INFORMATION SECURITY: STATE, PROBLEMS, TRENDS

The article analyzes the peculiarities of information security in the context of the development of the information sphere. The state, problems, tendencies and perspectives of the dialectic of information security are determined.

Key words: information environment, information security. Means of information protection.

----------***----------