І н ф о р м а ц і й н а б е з п е к а

УДК 340.13 + 007.51 + 165.12

ФУРАШЕВ В.М., *кандидат технічних наук, старший науковий співробітник, доцент, професор РАЕ*

КІБЕРПРОСТІР ТА ІНФОРМАЦІЙНИЙ ПРОСТІР, КІБЕРБЕЗПЕКА ТА ІНФОРМАЦІЙНА БЕЗПЕКА: СУТНІСТЬ, ВИЗНАЧЕННЯ, ВІДМІННОСТІ

Анотація. *Дослідження сутності кіберпростору та інформаційного простору, визначення на їх базі понять “кібербезпека”, “інформаційна безпека” та відмінностей цих просторів і понять.*

Ключові слова: *інформація, інформаційний простір, інформаційна безпека, національна безпека, захист інформації, кіберпростір, кібербезпека, кібернетична безпека.*

Аннотация. *Исследование сущности киберпространства и информационного пространства, определения на их базе понятий “кибербезопасность”, “информационная безопасность” и отличий этих пространств и понятий.*

Ключевые слова: *информация, информационное пространство, информационная безопасность, национальная безопасность, защита информации, киберпространство, кибербезопасность, кибернетическая безопасность.*

Summary. *Research of the intension of cyberspace and information space, the definition of “cybersecurity” and “information security” concepts based on these terms, and the differences between these spaces and definitions.*

Keywords: *information, information space, information security, national security, information protection, cyberspace, cybersecurity, cybernetic security.*

Постановка проблеми. У дослідженнях [1– 3] було встановлено наступне.

По-перше, у переважній більшості чинних законодавчих та інших нормативно-правових актів, які спрямовані на встановлення, розвиток та регулювання інформаційних відносин, не застосовується поняття “інформаційна безпека”.

По-друге, переважна більшість положень законів України та інших нормативно-правових актів, які мають безпосереднє відношення до інформаційних відносин, спрямовані саме на захист інформації.

По-третє, об’єктами інформаційних відносин є інформація, норми і правила, які визначають ці відносини, а також людина, суспільство, держава, а суб’єктами – держава, суспільство, людина, норми і правила, які визначають ці відносини.

По-четверте, об’єктами інформаційної безпеки є інформація у всіх її проявах, джерела інформації, механізми та засоби її створення, доступу і розповсюдження та наслідки її використання, а також установчі і регуляторні нормативно-правові та адміністративно-організаційні норми і правила, які визначають процеси і процедури формування, використання та припинення дії цих механізмів та засобів, людина, суспільство та держава, а суб’єктами – держава, людина, суспільство.

По-п’яте, об’єктом захисту інформації є інформація, а суб`єктами – дії з інформацією на всіх стадіях її “життєвого циклу” (створення, розповсюдження, збереження, знищення, спотворення, фальсифікація та ін.).

Одним з основних результатів цих досліджень стало надання наступного визначення поняття “інформаційна безпека”: *“інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається завдання шкоди через:*

- негативний інформаційний вплив за допомогою, в першу чергу, несанкціонованого створення, розповсюдження, використання свідомо спрямованої за визначеною метою неповної, невчасної, невірогідної та упередженої інформації;

- негативні наслідки застосування інформаційних технологій;

- несанкціоноване порушення режиму доступу до інформації з подальшим її розповсюдженням та використанням”.

Також було надане наступне визначення поняття “безпека інформації”: *“безпека інформації – склад та стан інформації, а також дії з нею, за яких забезпечується визначений рівень інформаційної безпеки”.*

Наприкінці цього була висловлена необхідність продовження досліджень, об’єктом яких повинні бути механізми та засоби захисту власне інформації, а суб’єктами – принципи, методи та засоби отримання, передачі, обробки та збереження інформації.

Формування мети. Для проведення подальших досліджень у напрямі визначення міри взаємозв`язку понять “інформаційна безпека” та “кібернетична безпека” (“кібербезпека”) спочатку необхідно визначитися із суттю та тлумаченням понять “кібербезпека”, або “кібернетична безпека” та “інформаційний простір”.

Але це можливо зробити, на думку автора, лише у тому випадку, коли буде чітке розуміння сутності поняття “кіберпростір”.

Підтвердженням цьому є висновки дослідників Дубова Д.В. і Ожевана М.А., які дійшли висновку, що: *“незважаючи на широке використання поняття “кіберпростір” як у науковій літературі, так і офіційних документах, існують обґрунтовані сумніви щодо можливості його використання у суто практичній площині. Значною мірою через це більшість держав світу продовжують протидію злочинним діям в кіберпросторі, послуговуючись “традиційним” законодавством (наприклад, щодо порушення телекомунікаційних мереж, отримання несанкціонованого доступу до інформації тощо).*

З огляду на вищезазначену термінологічну невпорядкованість щодо центрального поняття ще більш складною постає проблема визначення похідних від нього понять, що активно використовуються в офіційних документах провідних країн світу та безпекових організацій: “кібервійна”, “кібератака”, “кіберзахист”, “кібербезпека”, “кіберзброя”, “кібертероризм” тощо” [4, с. 13]

Даний висновок було зроблено на підставі аналізу “Національної військової стратегії для операцій у кіберпросторі” (США, 2006 рік) [5], офіційних документів ЄС [6], “Стратегії безпеки кіберпростору для Об’єднаного Королівства: убезпеченість, безпека та еластичність кіберпростору” [7], “Стратегії кібербезпеки для Німеччини” [8], “Національної стратегії кібербезпеки” (Голландія) [9], французьких “Білої книги оборони та національної безпеки” [10] і “Оборони та безпека інформаційних систем. Стратегія для Франції” [11].

Виклад основних положень. У роботі [3] автор вже торкався проблеми визначення поняття “кібербезпека” і з’ясував, без детальних пояснень, що ***кібербезпека –*** *стан спроможності людини, суспільства і держави запобігання та уникнення спрямованого, в першу чергу – несвідомого, негативного впливу (управління) інформації,* запропонувавши це визначення до широкого обговорення.

Але наскільки це запропоноване визначення відповідає його сутності та кореспондується із сутністю поняття “кіберпростір”, спробуємо детальніше розібратися.

Цілком логічно, що поняття “кіберпростір”, “кіберзахист”, “кіберзлочинність”, “кібервійна”, “кіберзброя”, “кібератака”, “кібертероризм” як вираження визначених явищ, сфер, дій, взаємопов`язані і не можуть існувати один без одного, причому домінуюче положення має саме “кіберпростір”.

У словосполученні “кіберпростір” є два слова – “кібер”, або “кібернетичний” та “простір”. У цьому словосполученні основним є слово “простір”, а спрямованість, характер цього простору визначає слово “кібернетичний”.

Енциклопедичне визначення поняття “простір” має два значення:

“***Простір*** *(математ.) – множина об’єктів, між якими встановлені відношення, подібні за своєю структурою зі звичайними просторовими відношеннями типу околу, відстані та ін.*

Простір *– форма співіснування матеріальних об’єктів процесів (характеризує структурність і протяжність матеріальних систем). Загальні властивості простору – протяжність, єдність дискретності та неперервності*” [12].

Для розуміння спрямованості простору, якій розглядається, слід згадати, що означає поняття “кібернетика”, похідною якого є “кібернетичний”.

Кібернетика *– наука про управління, зв’язки і переробку інформації. Основний об`єкт дослідження – так звані кібернетичні системи, що розглядаються абстрактно, незалежно від їх матеріальної природи. Приклади кібернетичних систем – автоматичні регулятори у техніці, ЕОМ, людський мозок, біологічні популяції, людське суспільство. Кожна така система є множиною взаємопов’язаних об’єктів (елементів системи), здатних сприймати, запам’ятовувати та переробляти інформацію, а також обмінюватися нею* [12].

Виходячи з наведеного можна зробити попередній висновок, що ***кіберпростір – це форма співіснування сукупності матеріальних та нематеріальних об’єктів і процесів, спрямованих на породження, сприйняття, запам’ятовування, переробку та обмін інформацією.***

Деякою мірою, кіберпростір – це віртуальний світ, який базується на реальному матеріальному фундаменті та з реальними наслідками свого “існування та розвитку”.

Кіберпростір є дуже складним явищем, що об’єднує в собі реальність і віртуальність, матеріальне і нематеріальне, абстрактність і дійсність.

Кіберпростір має наступні властивості:

- протяжність;
- єдність дискретності та неперервності;
- матеріальність та нематеріальність;
- абстрактність і дійсність;
- реальність загальнодіючого впливу.

Кіберпростір має свою розмірність/протяжність, яка визначаєтьсь кількістю наявних матеріальних і нематеріальних об`єктів на даний період часу. Коли протяжність кіберпростору з точки зору наявності матеріальних об’єктів, обмежена поверхнею земної кулі, то з точки зору наявності нематеріальних об’єктів – протяжність кіберпростору практично необмежена.

Процеси, які відбуваються у кіберпросторі, мають, в основному, як дискретний, так і неперервний характер. Але вони є взаємодоповнюючими один одного, а часто-густо й взаємопов’язаними, які забезпечують існування та розвиток цього простору.

Кіберпростір включає в себе як матеріальну складову, наприклад, засоби обчислювальної техніки, засоби зв`язку, матеріальні складові телекомунікаційних мереж, написання алгоритмів і кодів та ін., так нематеріальну – інформацію, процеси зчитування кодів, процеси передачі інформації та ін. Але при цьому необхідно зауважити, що під матеріальністю, у даному випадку, ми розуміємо, на відміну від філософського розуміння, все те, що можна побачити, відчути або доторкнутися.

Кіберпростір, в цілому, неможливо побачити, відчути, почути або до нього доторкнутися. Він, а особливо процеси, які у ньому відбуваються, людиною сприймається як щось абстрактне. Але окремі складові цього простору можна не тільки побачити, але й доторкнутися.

Але сам по собі кіберпростір не міг ані сформуватися, ані розвиватися. Потрібні були спонукальні мотиви.

Цими спонукальними мотивами є діяльність людини, суспільства, їх намагання до удосконалення свого особистого і громадського життя, особистого та суспільного розвитку, удосконалення і розширення обміну інформацією та ін.

Таким чином, кіберпростір є рукотворним дітищем людини, яке він формував для себе та під себе для задоволення своїх потреб, не думаючі про “побічні” явища, мова про які буде нижче.

Саме це та вищенаведене дає підстави сказати, що:

- об’єктами кіберпростору є живі істоти та їх угруповання, які спроможні сприймати, запам’ятовувати та переробляти інформацію, а також обмінюватися нею, серед яких, в першу чергу, людина, визначені верстви суспільства та суспільство в цілому, держава, природні та штучні інформаційні відносини між ними та їх формування і використання, а також матеріальні та нематеріальні об`єкти і процеси, спрямовані на породження, сприйняття, запам`ятовування, збереження, переробку та обмін інформацією;

- суб’єктами кіберпростору є людина, суспільство, держава, а також жива істота, яка спроможна сприймати, запам`ятовувати та переробляти інформацію, а також обмінюватися нею.

Автор не помилився – людина, суспільство, держава одночасно є як об’єктами кіберпростору, так і – його суб’єктами.

Але для подальших досліджень по визначенню поняття “кібербезпека” напрошується необхідність визначення відмінностей у поняттях “інформаційний простір” та “кіберпростір”.

В роботі [1] автор вже торкався питання інформаційного простору, але під іншим кутом зору. Тому наразі необхідно повернутися до цього питання.

Ще задовго до появи людини вже існував інформаційний простір. Фактично він ровесник планети під назвою “Земля”, тому що навіть неживі елементи природи були і є джерелами різноманітної інформації. Справа полягала лише в тому, що на той час були відсутні істоти, які були спроможні сприймати, запам’ятовувати, переробляти та використовувати цю інформацію.

З появою живих істот, навіть простіших, інформаційний простір почав “оживати”, наповнюватися змістом, сенсом та усвідомлюватися. З розвитком життя на Землі одночасно розвивався й інформаційний простір.

Взагалі людство існує в суцільному інформаційному просторі, в якому кожна жива істота є елементарною (простою) або більш розвинутою (складною) інформаційною системою та одночасно є джерелом і користувачем інформації. Навіть, як було вже зазначено, неживі суб’єкти природи, навколишнього середовища є джерелами інформації.

Саме тому можна говорити про те, що ***інформаційний простір – це форма співіснування сукупності матеріальних та нематеріальних об`єктів і процесів, спрямованих на задоволення інформаційних потреб всіх живих істот на Землі.***

Дане визначення охоплює інформаційний зв’язок та інформаційні відносини між суб’єктами “живої” і “неживої” природи.

Особливо важливим інформаційний простір є для людства.

Виходячи з наведеного визначення можна сказати, що:

- ***об’єктами інформаційного простору є суб’єкти природного середовища, природні та штучні інформаційні відносини між ними та їх формування і використання, матеріальні та нематеріальні об’єкти і процеси, спрямовані на задоволення інформаційних потреб для забезпечення збереження життя та життєдіяльності живої істоти, угрупування живих істот;***
- ***суб’єктами інформаційного простору є живі істоти та їх угруповання, які спроможні сприймати, запам’ятовувати та переробляти інформацію, а також обмінюватися нею.***

Інформаційний простір має властивості, які, за великим рахунком, збігаються з властивостями кіберпростору, а саме:

- протяжність;
- єдність дискретності та неперервності;
- матеріальність та нематеріальність;
- абстрактність і дійсність;
- реальність загальнодіючого впливу.

Порівнюючи надані визначення понять “кіберпростір” та “інформаційний простір”, одразу бачимо, що це – два різних “простори”, і відмінність їх полягає у їх спрямованості.

Кіберпростір, який охоплює ***лише живі істоти***, які спроможні сприймати, запам’ятовувати та переробляти інформацію, а також обмінюватися нею, є невід’ємною складовою інформаційного простору, якій охоплює абсолютно ***всі джерела інформації*** без вимог щодо спроможності сприймати, запам`ятовувати та переробляти інформацію, а також обмінюватися нею.

Запропоновані визначення, які, до речі, не претендують на істину в останній інстанції, є, скоріше, загальноохоплюючими, філософськими.

У реальній життєдіяльності людина, визначена верства суспільства або суспільство в цілому, держава користуються принципом практичного прагматизму, реальними або ілюзійними уявленнями щодо свого буття та розвитку, вирішення тих чи інших питань та проблем.

Саме це визначає вибір об’єктів інформаційного простору та кіберпростору для вибудовування штучних або пристосування природних інформаційних відносин, що, у свою чергу, здійснює вплив на вибір або формування, створення матеріальних та нематеріальних об’єктів і процесів, спрямованих на задоволення визначених інформаційних потреб.

Вся історія появи та розвитку життя на Землі пов’язана з інформацією.

Будь-яка жива істота є інформаційною системою. Простою або складною, але інформаційною системою.

Найскладнішою інформаційною системою в сучасному світі є саме людина. Отримання інформації людиною здійснюється через всі чотири органи, якими її наділила природа: зір, слух, відчуття та дотик.

Можна сказати, що людина стала людиною тоді, коли змогла не тільки видавати та сприймати інформаційні сигнальні звуки, не тільки сприймати та на початковому рівні

аналізувати інформаційні знаки суб’єктів навколишнього середовища, а тоді, коли почала породжувати, збирати та використовувати у власних цілях цю інформацію.

Важливість та цінність інформації, як суспільної, так й особистої, відома людству здавна. В епоху виникнення людства питання наявності або відсутності необхідної інформації було еквівалентом питання “жити або померти”. Тому з давніх часів зусилля людини, племені, суспільства концентрувалися, з одного боку, на отриманні, збереженні, переробці та використанні у своїх цілях необхідної інформації будь-яким способом, а з другого – на недопущенні витоку цієї інформації.

Здавна людина, хай на інтуїтивному рівні, усвідомила, що інформація має вплив на іншу людину, іншу живу істоту, що за допомогою інформації можна вирішувати багато питань особистого та суспільного життя, інтересів соціальних інституцій.

З розвитком людства, появою писемності шляхи та засоби як отримання, так й збереження інформації постійно розвивалися та вдосконалювалися. Але в центрі цих процесів знаходилась інформація.

Ситуація почала змінюватись принципово з появою нових засобів комунікацій – телефонізації, радіомовлення, телебачення, засобів обчислювальної техніки, інформаційно-комунікаційних технологій.

Роль інформації у суспільному житті почала суттєво змінюватися в бік стрімкого зростання її значення. Інформація перестає бути доступною лише для визначеного кола адресатів, зі всіма наслідками, що витікають з цього. Вона стає доступнішою, глибше проникає у свідомість як конкретної людини, групи людей, так і цілого суспільства.

Інформація починає впливати на людину на рівні не тільки свідомості, а й підсвідомості, тобто попри її волю. Інформація починає здійснювати домінуючий вплив на свідомість, поведінку людини та, відповідно, на суспільство в цілому.

Розуміючи “силу” інформації, людство постійно створювало та вдосконалювало механізми управління інформацією, інформаційними потоками.

В цьому криється як позитив, так й негатив у розвитку людини і всього суспільства. Це привело до того, що у даний час інформація перетворилася на справжню зброю, інформаційну зброю.

Але це вірно лише у тому випадку, коли інформація виступає як додаток до звичних видів озброєння чи коли вона виконує або функції, які зазвичай виконують окремі складові звичайних видів озброєння, або функції, які повністю або частково заміщують окремі складові звичайних видів озброєння.

Але питання управління інформацією у напрямі перетворення та застосування інформації у якості зброї, зміни свідомості людини, визначених верств суспільства, суспільства в цілому є об’єктом кіберпростору як невід`ємної складової інформаційного простору.

Питання управління інформацією є елементом забезпечення національної безпеки, державної безпеки.

Виходячи з наведеного, визначення, які надані у роботі [3], що *“**кібербезпека** – стан спроможності людини, суспільства і держави запобігання та уникнення спрямованого, в першу чергу – несвідомого, негативного впливу (управління) інформації*” та у роботі [2] – *“**інформаційна безпека** – стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається завдання шкоди через:*

- негативний інформаційний вплив за допомогою, в першу чергу, несанкціонованого створення, розповсюдження, використання свідомо спрямованої із визначеною метою неповної, невчасної, невірогідної та упередженої інформації;

- негативні наслідки застосування інформаційних технологій;

- *несанкціоноване порушення режиму доступу до інформації з подальшим її розповсюдженням та використанням”*, є справедливими.

Порівняння цих визначень показує їх тотожність. Вони й не могли бути різними, бо кіберпростір є невід’ємною складовою інформаційного простору, а це означає, що об’єкти і суб’єкти, в даному випадку, в них одні і ті ж, матеріальні та нематеріальні об’єкти і процеси та їх спрямованість – одне і те ж.

Висновки.

1. На основі проведених досліджень сутності понять “кіберпростір” та “інформаційний простір” встановлено, що:

- ***кіберпростір*** – це форма співіснування сукупності матеріальних та нематеріальних об`єктів і процесів, спрямованих на породження, сприйняття, запам`ятовування, переробку та обмін інформацією;
- ***інформаційний простір*** – це форма співіснування сукупності матеріальних та нематеріальних об’єктів і процесів, спрямованих на задоволення інформаційних потреб всіх живих істот на Землі.

2. ***Об’єктами кіберпростору*** є живі істоти та їх угруповання, які спроможні сприймати, запам’ятовувати та переробляти інформацію, а також обмінюватися нею, серед яких, в першу чергу, людина, визначені верстви суспільства та суспільство в цілому, держава, природні та штучні інформаційні відносини між ними та їх формування і використання, а також матеріальні та нематеріальні об`єкти і процеси, спрямовані на породження, сприйняття, запам’ятовування, збереження, переробку та обмін інформацією;

Суб’єктами кіберпростору є людина, суспільство, держава, жива істота, яка спроможна сприймати, запам’ятовувати та переробляти інформацію, а також обмінюватися нею.

3. ***Об’єктами інформаційного простору*** є суб’єкти природного середовища, природні та штучні інформаційні відносини між ними та їх формування і використання, матеріальні та нематеріальні об’єкти і процеси, спрямовані на задоволення інформаційних потреб для забезпечення збереження життя та життєдіяльності живої істоти, угруповання живих істот;

Суб’єктами інформаційного простору є живі істоти та їх угруповання, які спроможні сприймати, запам’ятовувати та переробляти інформацію, а також обмінюватися нею.

4. Кіберпростір є невід’ємною складовою інформаційного простору.

5. Поняття “кібербезпека” та “інформаційна безпека” є тотожними за своєю сутністю. Застосування будь-якого з цих понять не змінює сутності процесу або явища, лише може внести термінологічну плутанину. Тому краще застосовувати поняття “кібербезпека” як термін, що більш чітко відображає сутність процесу, явища.

Перспективи щодо подальших досліджень. Базуючись на результатах проведених досліджень можна та потрібно розглядати питання сутності понять “кібервійна”, “кібератака”, “кіберзахист”, “кібербезпека”, “кіберзброя”, “кібертероризм” тощо, їх визначення та відмінності.

Використана література

1. В. Фурашев. Питання законодавчого визначення понятійно-категоріального апарату у сфері інформаційної безпеки // “Інформація і право”. – № 1(4)/2012. – С. 46 – 55.

2. В. Фурашев Сутність та визначення понять “інформаційна безпека” і “безпека інформації” // “Правова інформатика”. – № 2(34)/2012. – С. 51 – 59.

3. Фурашев В.М. Ключові аспекти проекту Закону України “Про безпеку інформації” // “Віче”. – 2012. – № 6/2012(315). – С. 29 – 30.

4. Дубов Д.В. Кібербезпека : світові тенденції та виклики для України / Д.В. Дубов, М.А. Ожеван. – К. : НІСД, 2011. – 30 с.

5. National Military Strategy for Cyberspace Operations. – Режим доступу : //www.dod.gov/pubs/foi/ojcs/07-F-2105doc1.pdf

6. Glossary and Acronyms (Archived) / European Commission. – (Accessed 03 Nov 2009). – Режим доступу : //www.ec.europa.eu/information_society/tl/help/glossary/index_en.htm#c

7. Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space. – Режим доступу : //www.official-document/cm76/7642/7642.pdf

8. – Режим доступу : //www.enisa.europa.eu/media/news-items/german-cyber-security-strategy-2011-1

9. – Режим доступу : //www.enisa.europa.eu/media/news-items/dutch-cyber-security-strategy-2011

10. The French White Paper on defence and national security. – Режим доступу : //www.livreblancdefenseetsecurite.gouv.fr/IMG/pdf/white_paper_press_kit.pdf

11. – Режим доступу : //www.enisa.europa.eu/media/news-items/french-cyber-security-strategy-2011

12. Советский энциклопедический словарь ; гл. ред. Прохоров А.М. – [4-е изд.]. – М. : Сов. энциклопедия, 1986. – 1600 с.

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~

УДК 351.746.1

СКУЛИШ Є.Д., *доктор юридичних наук, професор, Заслужений юрист України*

ІНФОРМАЦІЙНА БЕЗПЕКА: НОВІ ВИКЛИКИ УКРАЇНСЬКОМУ СУСПІЛЬСТВУ

Анотація. *Проведено аналіз сучасних загроз та викликів інтересам держави в інформаційній сфері з урахуванням тенденцій розвитку останньої, а також наукового осмислення знань, накопичених у галузі забезпечення інформаційної безпеки. На основі аналізу визначено пріоритетні завдання суб’єктам забезпечення національної безпеки України.*

Ключові слова: *інформаційна сфера, національна безпека України, загрози.*

Аннотация. *Осуществлен анализ современных угроз и вызовов интересам государства в информационной сфере с учетом тенденций развития последней, а также научного осмысления знаний, накопленных в области обеспечения информационной безопасности. На основе анализа определены приоритетные задачи субъектам обеспечения национальной безопасности Украины.*

Ключевые слова: *информационная сфера, национальная безопасность Украины, угрозы.*

Summary. *Whereas the latest trends in information sphere, as well as scientific comprehension of the knowledge gained in the field of information security, the analysis of up-to-date threats and challenges to the state's interests in this domain is carried out. Based on the analysis priorities tasks to the subjects of national security of Ukraine are identified.*

Keywords: *information sphere, national security of Ukraine, threats.*

Постановка проблеми. Інформаційна революція, що триває протягом останніх десятиріч, зумовила кардинальні зміни в суспільстві: зароджуються нові культурні та економічні тенденції, формуються нові види соціальної комунікації, інформація стає не лише товаром, а й новим фактором виробництва.

З огляду на сучасні тенденції суспільного розвитку національна безпека України не могла залишитися поза впливом внутрішнього інформаційного фактора. Адже в умовах інформаційного суспільства всі без винятку об’єкти національної безпеки (людина, суспільство, держава) стають чутливими до інформації, яка їх оточує. Таким чином, цілеспрямовано змінюючи інформацію, зафіксовану на певних носіях, керуючи каналами комунікації, впливаючи на технічні засоби обробки інформації, можна змінювати рішення, а відтак, і дії об’єктів національної безпеки [1, с. 23].

Водночас, об’єкти національної безпеки перебувають під впливом зовнішнього інформаційного фактора, що визначається змінами у сфері міжнародних відносин:

- руйнуванням біполярної моделі світу та формуванням поліполярної;
- виходом на міжнародну арену не лише окремих держав та їх об’єднань, а й таких нетрадиційних гравців, як, наприклад, транснаціональні корпорації, міжнародні терористичні рухи тощо;
- загостренням протиборства між традиційними та новими геополітичними центрами;
- інтенсифікацією глобалізаційних процесів, з одного боку, та зростанням тенденцій дезінтеграції, навіть у досить стабільних суспільствах, з іншого;
- перенесенням дій щодо розгортання та вирішення міжнародних конфліктів в інформаційний простір;
- переформатуванням інформаційного суспільства в інформаційно-комунікативне [2, с. 146].

Об’єктивним результатом впливу цих факторів на систему національної безпеки є поява нових викликів інтересам держави. З огляду на це перед інститутами сектору безпеки постають завдання зі створення нової парадигми, теорії і практики національної безпеки в умовах інформаційно-комунікативного суспільства.

Аналіз останніх досліджень і публікацій. Багатоаспектність проявів інформаційної складової у різних сферах національної безпеки України обумовила появу широкого кола наукових досліджень з питань забезпечення інтересів особи, суспільства та держави з урахуванням зазначених вище факторів. Так, окремі питання інформаційних загроз інтересам держави у контексті національної безпеки розглядали Г. Новицький [3], В. Хлевицький [4]. Дослідження політико-правових питань забезпечення інформаційної безпеки проводились І. Бачило [5], В. Брижком [6], Р. Калюжним [7], Б. Кормичем [8], А. Марущаком [9]. Вплив інформаційно-комунікативних технологій на військовий потенціал держави був предметом вивчення В. Толубка [10]. Моніторинг актуальних загроз національній безпеці України в інформаційній сфері систематично здійснюється фахівцями Національного інституту стратегічних досліджень [11]. На думку автора, настав час для наукового осмислення та упорядкування здобутих знань у сфері забезпечення інформаційної безпеки держави з метою отримання своєчасного зворотного зв’язку та коригування відповідних завдань суб’єктам забезпечення національної безпеки України.

Метою статті є визначення актуальних загроз інтересам держави в інформаційній сфері з урахуванням тенденцій її розвитку як складової системи національної безпеки України.

Виклад основних положень. Насамперед, розглянемо умови, в яких відбувалося становлення системи забезпечення інформаційної безпеки в Україні.

Ретроспективний аналіз свідчить, що на момент проголошення незалежності на території України були зосереджені найкращі наукові розробки та фахівці інформаційної галузі:

- академік Лебедєв С.А. у Києві створив першу в СРСР і третю у світі електронно-обчислювальну машину;
- у 1964 році перший директор Інституту кібернетики НАН України академік Глушков В.М. запропонував радянському уряду проект загальнодержавної системи збирання й обробки інформації для керування економікою країни. Таким чином було введено розуміння основ інформаційно-комп’ютерних технологій;
- в Україні розроблено такі наукові напрямки як штучний інтелект, теорія самоорганізації, системний аналіз, що ґрунтуються на відтворенні діяльності мозку людини при вирішенні складних прикладних завдань. Ці напрями характеризуються як якісний стрибок у кібернетиці;
- Україна входила до п’ятірки країн із найбільшим кадровим потенціалом фахівців із комп’ютерних наук [12].

Період входження України в “інформаційну цивілізацію”, на думку автора, розпочався з прийняття нормативних актів, що регулюють суспільні інформаційні відносини. Підґрунтям для їх розробки та впровадження стала Конституція України, відповідно до ст. 17 якої забезпечення інформаційної безпеки є однією із найважливіших функцій держави. Правові засади інформатизації українського суспільства утворюють закони України “Про інформацію” [13], “Про Національну програму інформатизації” [14], “Про телекомунікації” [15], “Про електронні документи та електронний документообіг” [16], “Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки” [17], “Про доступ до публічної інформації” [18] тощо. Низка нормативних актів спрямована на захист інтересів особи, суспільства, держави в інформаційній сфері, а саме:

укази Президента України “Про затвердження Положення про технічний захист інформації в Україні” [19], “Про Положення про порядок здійснення криптографічного захисту інформації в Україні” [20], “Про Доктрину інформаційної безпеки України” [21], а також закони України “Про захист інформації в інформаційно-телекомунікаційних системах“ [22], “Про захист персональних даних” [23] та ін.

Аналіз зазначених нормативних актів надає підстави стверджувати, що на державному рівні пріоритет надається наступним напрямам розвитку інформаційного суспільства:

- забезпеченню широкого доступу до Інтернету пересічним громадянам;
- розвитку цифрового телебачення;
- розміщенню в Інтернеті всебічної (правової, політичної та ін.) інформації про Україну, діяльність органів державної влади;
- впровадження технологій електронного урядування;
- розвитку електронної комерції.

Водночас, фахівці в галузі національної безпеки дійшли висновку, що розвиток інформаційного суспільства в Україні стримується внаслідок впливу таких трьох основних процесів. По-перше, це зміна основ суспільного ладу, поступовий відхід від ідеології “реального соціалізму”, що отримав назву постколоніального транзиту. По-друге, формування України як самостійної держави відбувається в умовах фінансової нестабільності. По-третє, однією з актуальних проблем національної безпеки України є недосконалість державної інформаційної політики [24].

Зокрема, аналіз Стратегії національної безпеки України [25] свідчить, що основними чинниками, які заважають повноцінному розвитку інформаційного суспільства в Україні, є:

- неструктурованість та неузгодженість інформаційного законодавства;
- відсутність повноцінної комплексної національної програми соціально-економічного розвитку на базі інформаційного суспільства;
- погляд на розвиток інформаційного суспільства як на міжвідомчу проблему, а не на пріоритетний напрям розвитку всієї країни;
- недостатня загальнодержавна координація щодо створення елементів інформаційної інфраструктури, зокрема при побудові загальнодержавних, корпоративних і відомчих інформаційно-телекомунікаційних мереж;
- низька державна координація впровадження послуг, побудованих на використанні Інтернет-технологій.

Зазначені проблемні питання створюють передумови для ескалації окремих загрозливих тенденцій в інформаційній сфері. Так, на думку автора, з огляду на глобалізацію інформаційних процесів, обумовлену впровадженням Інтернет-технологій, актуалізується проблема ***співвідношення відкритості та обмеження доступу до інформації*** (ст. 7 Закону України “Про основи національної безпеки України” [26]). Зауважимо, що мова йде не лише про інформацію, яка містить державну таємницю, а й про іншу передбачену законом таємницю (комерційну, банківську тощо), й зокрема службову інформацію. Адже, як свідчить моніторинг матеріалів ЗМІ, останнім часом питання комерційного шпигунства набуває все більшої актуальності.

Таким чином, в процесі становлення державності перехід від інформаційної ізоляції за часів СРСР до інформаційної відкритості сучасного українського суспільства потребує не лише формування нових поглядів на роль і місце інформаційної складової в усіх сферах життєдіяльності, забезпечення управлінської діяльності органів державної влади в нових

інформаційних умовах, а й оновлення практики інститутів сектору безпеки через взаємодію з інститутами громадянського суспільства.

Бурхливий розвиток інформаційно-телекомунікаційних технологій, поряд із беззаперечними перевагами, створив передумови для реалізації інформаційних загроз у кіберпросторі. З одного боку, інформація набула системоутворювального значення, з іншого – інформаційно-телекомунікаційна інфраструктура отримала статус критичної (життєво важливої для існування держави) і потребує високотехнологічного захисту. З огляду на перспективи подальшої інформатизації українського суспільства тенденція до поширення ***комп’ютерної злочинності*** та проявів ***комп’ютерного тероризму*** буде зберігатись.

З огляду на системоутворювальне значення, якого набула інформація у сучасному суспільстві, поширеним явищем стало її використання в якості засобу для досягнення мети, тобто інформація з об’єкта захисту перетворилась на інструмент впливу. Індивідуальна, суспільна й масова свідомість все більшою мірою піддаються агресивним інформаційним впливам, що нерідко завдає шкоди моральному здоров’ю громадян, руйнує духовні норми життя суспільства, призводить до дестабілізації соціально-політичної обстановки. Сучасне розуміння безпеки в контексті визначення оптимального співвідношення інтересів особи, суспільства та держави ставить завдання розгляду нового аспекту цієї проблеми – ***інформаційно-психологічної безпеки***. Принциповий характер для безпеки України мають на сьогодні такі проблеми, як протидія деструктивним культам, запобігання інформаційним агресіям, транснаціональним інформаційним впливам, маніпулюванню суспільною свідомістю через засоби масової інформації та соціально орієнтовані сервіси Інтернету.

Виокремлення інформаційно-психологічної безпеки особи із загальної проблематики інформаційної безпеки в самостійний напрям визначається низкою чинників:

1. У зв’язку з переходом до інформаційно-комунікативного суспільства, збільшенням масштабів і ускладненням змісту та структури інформаційних потоків та всього інформаційного середовища, багатократно посилюється його вплив на психіку людини, а темпи цього впливу стрімко зростають. Це визначає формування нових механізмів захисту людини від інформаційно-психологічних впливів, а суспільства – від глобальних інформаційних втручань.

2. Взаємодія психіки людини з інформаційним простором відрізняється якісною специфікою і не має відповідних аналогів серед інших типів структур (технічних, соціальних, соціотехнічних тощо).

3. Людина та її свідомість – центральна мета інформаційного впливу. Від окремих осіб, їхніх взаємозв’язків і взаємин залежить нормальне функціонування соціально-політичної системи.

Висновки.

Проведений у статті аналіз передумов формування в Україні інформаційного суспільства, нормативно-правових актів, які регулюють інформаційні суспільні відносини, наукових публікацій з проблем інформаційної безпеки свідчить, що найбільш актуальними питаннями забезпечення національної безпеки України в інформаційній сфері на сьогодні є:

1) співвідношення відкритості та обмеження доступу до інформації – захист інформації з обмеженим доступом в умовах відкритого інформаційного суспільства є нетривіальним завданням, що потребує збалансованої державної політики, і насамперед – гнучкого нормативного регулювання;

2) протидія комп’ютерній злочинності та комп’ютерному тероризму – захист інформаційно-телекомунікаційної інфраструктури є необхідною передумовою функціонування усіх галузей виробництва, водночас критично важливою – для банківських

установ, транспортних організацій, об’єктів підвищеної небезпеки;

3) забезпечення інформаційно-психологічної безпеки – захист суспільної, масової, індивідуальної свідомості від прихованих інформаційних впливів, які загрожують безпеці особи, суспільства і держави, є новим завданням, актуальність якого обумовлена ефективністю сучасних комунікативних технологій.

З огляду на викладене, пріоритетними завданнями для суб’єктів забезпечення національної безпеки України в умовах глобального інформаційно-комунікативного суспільства є:

- стимулювання впровадження новітніх інформаційних технологій і виробництва конкурентоздатного національного інформаційного продукту, зокрема, сучасних засобів і систем захисту інформаційних ресурсів;
- забезпечення безпеки інформаційно-телекомунікаційних систем, які функціонують в інтересах управління державою, забезпечують потреби оборони та безпеки держави, кредитно-банківської та інших сфер економіки, систем управління об’єктами критичної інфраструктури;
- створення національної системи кібербезпеки, що потребує залучення суспільства, бізнесу й держави до активних дій з розбудови інформаційно-телекомунікаційної інфраструктури;
- чітке визначення місця й ролі кожного сектору (держави, бізнесу, громадськості) в процесі розвитку інформаційно-комунікативного суспільства, адже забезпечення інформаційної безпеки вимагає об’єднання зусиль різних державних і недержавних відомств, інститутів громадянського суспільства;
- підвищення рівня свідомості суспільства, зосередження ресурсів для розвитку інформаційно-комунікативного суспільства з метою досягнення національних пріоритетів.

Подальші дослідження автора будуть спрямовані на розробку організаційно-правових засад реалізації зазначених завдань.

Використана література

1. Панченко В.М. Поняття інформаційної безпеки в сучасному юридичному дискурсі / В.М. Панченко // Інформаційна безпека людини, суспільства, держави. − 2009. − № 2 (2). − С. 22 − 27.

2. Горошко Е.И. Информационно-коммуникативное общество в тендерном измерении / Е.И. Горошко. – Х. : ФЛП Либуркина Л.М., 2009. – 816 с.

3. Новицький Г.В. Теоретико-правові основи забезпечення національної безпеки України / Г.В. Новицький. – К. : Інтертехнологія, 2008. – 496 с.

4. Хлевицький В.Б. Інформаційна безпека як одна із складових національної безпеки України / В.Б. Хлевицький // Євроатлантикінформ. – 2006. – № 1(7). – С. 70 – 72.

5. Бачило И.Л. Методология решения правовых проблем в области информационной безопасности / І.Л. Бачило // Информатика и вычислительная техника. – 1992. – №2. – С. 22 – 30.

6. Брижко В. До питання застосування у правотворчості понять “інформація” та “дані” / В. Брижко // Правова інформатика. – 2005. – № 4 (8). – С. 31 – 37.

7. Калюжний Р. Проблеми та перспективи правового забезпечення безпеки інформації з обмеженим доступом, що не становить державної таємниці / Р. Калюжний, Д. Прокоф‘єва // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : науково-технічний збірник / НТУУ “КПІ”, Міністерство освіти і науки України, Департамент спеціальних телекомунікаційних систем та захисту інформації СБ України. – К., 2000. – С. 27 – 31.

8. Кормич Б.А. Організаційно-правові засади політики інформаційної безпеки України : монографія / Б.А. Кормич. – Одеса : Юридична література, 2003. – 472 с.

9. Марущак А.І. Правомірні засоби доступу громадян до інформації : науково-практичний посібник / А.І. Марущак. – Біла Церква : Вид-во “Буква”, 2006. – 432 с.

10. Толубко В.Б. Інформаційна боротьба (концептуальні, теоретичні, технологічні аспекти) : монографія / В.Б. Толубко. – К. : НАОУ, 2003. – 315 с.

11. Дубов Д.В. Кібербезпека: світові тенденції та виклики для України : аналітична доповідь / Д.В. Дубов, М.А. Ожеван. – К. : НІСД, 2011. – 30 с.

12. Колодюк О.В. Національні стратегії інформаційного суспільства: необхідність, переваги та стан щодо запровадження в Україні / О.В. Колодюк // Сайт “Информационное общество”. – Режим доступу : http: //www.isu.org.ua/viewarticale/publications/117?new_lang=u.

13. Про інформацію : Закон України від 02.10.92 р. 2657-XII // Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650.

14. Про Національну програму інформатизації : Закон України від 04.02.98 р. № 74/98-ВР // Відомості Верховної Ради України. – 1998. – № 27 – 28. – Ст. 181.

15. Про телекомунікації : Закон України від 18.11.03 р. № 1280-IV // Відомості Верховної Ради України. – 2004. – № 12. – ст. 155.

16. Про електронні документи та електронний документообіг : Закон України від 22.05.03 р. № 851-IV // Відомості Верховної Ради України. – 2005. – № 26. – Ст. 349.

17. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : Закон України від 09.01.07 р. № 537-V // Відомості Верховної Ради України. – 2007. – № 12. – Ст. 102.

18. Про доступ до публічної інформації : Закон України від 13.01.11 р. № 2939-VI // Відомості Верховної Ради України. – 2011. – № 32. – Ст. 314.

19. Про затвердження Положення про технічний захист інформації в Україні : Указ Президента України від 27.09.99 р. № 1229 // Офіційне Інтернет-представництво Президента України. – Режим доступу : http://www.president.gov.ua/stateauthority /authofstate /prezidlist /prezidentadmin.

20. Про Положення про порядок здійснення криптографічного захисту інформації в Україні : Указ Президента України від 22.05.98 р. № 505/98 // Офіційне Інтернет-представництво Президента України. – Режим доступу : http://www.president.gov.ua/statea uthority /authofstate /prezidlist /prezidentadmin.

21. Про Доктрину інформаційної безпеки України : Указ Президента України від 08.07.09 р. № 514/2009 [Електронний ресурс] // CD-вид-во “Інфодиск”, 2010. – 1 електрон. опт. диск (CD-ROM). – Назва з титул. екрану.

22. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.94 р. № 80/94-ВР // Відомості Верховної Ради України. – 1994. – № 31. – Ст. 286.

23. Про захист персональних даних : Закон України від 01.06.10 р. № 2297-VI // Відомості Верховної Ради України. – 2010. – № 34. – С. 481.

24. Шерр Дж. Політика національної руйнації / Дж. Шерр / Дзеркало тижня. – 2008, 02 серпня року. – Режим доступу : http://www.dt.ua/1000/1550/63671.

25. Про Стратегію національної безпеки України : Указ Президента України від 12.02.07 р. № 105/2007 // Офіційне Інтернет-представництво Президента України. – Режим доступу : http://www.president.gov.ua/stateauthority/authofstate /prezidlist /prezidentadmin.

26. Про основи національної безпеки України : Закон України від 19.06.03 р. № 964-IV // Відомості Верховної Ради України. – 2003. – № 39. – Ст. 351.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~