До проблеми забезпечення інформаційної безпеки України

Володимир Остроухов,
доктор філософських наук,
завідуючий кафедрою соціальних технологій
Державного університету
інформаційно-комунікативних технологій
Валентин Петрик,
кандидат наук з державного управління,
доцент кафедри соціальних технологій
Державного університету
інформаційно-комунікативних технологій

У статті розкриваються такі поняття, як „інформаційна безпека" та її різновиди – „інформаційна безпека особистості", „інформаційна безпека суспільства", „інформаційна безпека держави", „інформаційна безпека інформаційно-технічної інфраструктури", а також поняття, тісно пов'язані з інформаційною безпекою. У висновку пропонуються рекомендації щодо навчально-методичного і наукового забезпечення інформаційної безпеки нашої держави.

Визначенням інформаційної безпеки та її різновидів переймалися такі вчені, як В. Крисько, А. Манойло, А. Петренко, Д. Фролов, Г. Почепцов, О. Литвиненко, А. Тарас, В. Толубко, М. Дзюба, Я. Жарков, М. Онищук, Б. Кормич [1 - 8] та інші. Розглядалася ця проблема і нами [9 - 10]. Слід зазначити, що визначення розкривалися частково й по-різному. Це й зумовлює **актуальність дослідження**.

Головна мета статті - визначення понятійного апарату щодо інформаційної безпеки та її різновидів, а також розробка деяких шляхів забезпечення інформаційної безпеки України.

Об'єкт дослідження – інформаційна безпека.

Предмет дослідження – понятійний апарат щодо інформаційної безпеки та навчально-методичне і наукове забезпечення інформаційної безпеки України.

Розглянемо такі базові терміни, як „інформаційна безпека" та її різновиди:

1) інформаційна безпека особистості;
2) інформаційна безпека суспільства;
3) інформаційна безпека держави;
4) інформаційна безпека інформаційно-технічної інфраструктури.

Інформаційна безпека – це стан захищеності об'єкта (особистості, суспільства, держави, інформаційно-технічної інфраструктури), при якому досягається його нормальне функціонування незалежно від внутрішніх і зовнішніх інформаційних впливів.

Інформаційний вплив – організоване цілеспрямоване застосування спеціальних інформаційних засобів і технологій для внесення змін у свідомість населення (корекція поведінки) та (або) інформаційно-технічну інфраструктуру об'єкта.

Інформаційно-психологічний вплив – вплив на свідомість особи чи населення з метою змін (корекції) їх поведінки.

Інформаційно-технічний вплив – вплив на інформаційно-технічну інфраструктуру об'єкта для забезпечення реалізації необхідних змін у її роботі (зупинка роботи, несанкціонований відплив інформації, програмування на певні помилки, зниження швидкості опрацювання інформації тощо).

Інформаційна безпека особистості (у вузькому розумінні) – це стан захищеності психіки людини від негативного впливу, який здійснюється шляхом упровадження деструктивної інформації у свідомість і (або) у підсвідомість людини, що призводить до неадекватного сприйняття нею дійсності.

Інформаційна безпека особистості (в широкому розумінні) це: 1) належний рівень теоретичної і практичної підготовки особистості, при якому досягається захищеність і реалізація її життєво важливих інтересів і гармонійний розвиток незалежно від інформаційних загроз; 2) здатність держави створити можливості для гармонійного розвитку і задоволення потреб особистості в інформації, незалежно від інформаційних загроз; 3) гарантування, розвиток і використання інформаційного середовища в інтересах особистості; 4) захищеність від різного роду інформаційних небезпек.

Інформаційна безпека особистості та суспільства тісно пов'язані.

Інформаційна безпека суспільства — можливість безперешкодної реалізації суспільством та окремими його членами своїх конституційних прав, пов'язаних з можливістю вільного одержання, створення й поширення інформації, а також ступінь їх захисту від деструктивного інформаційного впливу. Необхідний рівень інформаційної безпеки забезпечується сукупністю політичних, економічних, організаційних заходів, спрямованих на запобігання, виявлення й нейтралізацію обставин, факторів і дій, які можуть завдати збитків чи зашкодити реалізації інформаційних прав, потреб та інтересів країни та її громадян.

Інформаційна безпека інформаційно-технічної інфраструктури — це

стан її захищеності, який забезпечує її ефективне використання і захист від можливого інформаційно-технічного впливу. Інформаційна безпека інформаційно-технічної інфраструктури поділяється на безпеку: 1) машинно-технічних засобів; 2) програмного забезпечення; 3) засобів та режиму захисту від несанкціонованого витоку інформації.

Інформаційна безпека держави — це стан її захищеності, при якій спеціальні інформаційні операції, акти зовнішньої інформаційної агресії, інформаційний тероризм, незаконне зняття інформації (за допомогою спеціальних технічних засобів) та комп'ютерні злочини не завдають суттєвої шкоди національним інтересам.

Спеціальні інформаційні операції (СІО) — це сплановані дії, спрямовані на ворожу, дружню чи нейтральну аудиторію, які передбачають вплив на її свідомість і поведінку за допомогою використання організованої інформації та інформаційних технологій для досягнення певної мети.

Акти зовнішньої інформаційної агресії (АЗА) — легальні та (або) протиправні акції, реалізація яких може чинити негативний вплив на безпеку інформаційного простору держави.

Інформаційний тероризм (ІТ) — небезпечні діяння з інформаційного впливу на соціальні групи осіб, державні органи влади та управління, пов'язані з поширенням інформації, яка містить погрози переслідуванням, розправою, вбивствами, а також спотворення об'єктивної інформації, що спричиняє появу кризових ситуацій у державі, нагнітання страху і напруги в суспільстві.

Комп'ютерна злочинність — протиправні діяння у сфері використання електронних обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж, за які Кримінальним кодексом (КК) України передбачено відповідальність.

Чим досконаліша інформаційна безпека держави, тим важче вести проти неї інформаційні війни.

Інформаційна війна (ІВ) — вид протиборства між різними суб'єктами (державами, неурядовими, економічними чи іншими структурами), який здійснюється з метою досягнення односторонніх воєнних, соціально-політичних чи економічних переваг над супротивником.

Завдання ІВ: 1) здійснення деструктивного ідеологічного впливу; 2) створення атмосфери бездуховності, негативного ставлення до культури та історичної спадщини в суспільстві конкурента; 3) маніпулювання громадською думкою і політичною орієнтацією населення для створення політичної напруги та стану, близького до хаосу; 4) дестабілізація політичних відносин між партіями, об'єднаннями і рухами з метою розпалення конфліктів, стимулювання недовіри, підозри, загострення ворожнечі, боротьби за владу, провокування, застосування репресивних дій з боку влади щодо опозиції; 5) зниження рівня інформаційного забезпечення органів влади та управління, інспірація помилкових управлінських рішень; 6) уведення населення в оману щодо роботи

державних органів влади, підрив їх авторитету, дискредитація їх дій; 7) провокування соціальних, політичних, національно-етнічних та релігійно-конфесійних зіткнень; 8) ініціювання страйків, масових заворушень, інших акцій протесту і непокори; 9) підрив міжнародного авторитету держави, її співпраці з іншими державами; 10) створення чи посилення опозиційних угруповань чи рухів; 11) дискредитація фактів історичної, національної самобутності народу, зміна системи цінностей, які визначають спосіб життя і світогляд людей; 12) применшення та нівелювання визнаних світових досягнень у науці, техніці та інших галузях, перебільшення значення помилок, наслідків хибних дій та некваліфікованих урядових рішень; 13) формування передумов до економічної, духовної чи військової поразки, втрати волі до боротьби й перемоги; 14) представлення свого способу життя як поведінки та світогляду майбутнього, які мають наслідувати інші народи; 15) спонукання осіб чи певних груп до організації акцій громадської непокори, інших радикальних протиправних дій; 16) підрив морального духу населення і, як наслідок, зниження обороноздатності та бойового потенціалу.

Характер деструктивних впливів на інформаційний простір, тобто на процеси отримання, опрацювання, збереження й поширення інформації будь-якого виду визначає три форми ІВ: 1) вплив на форму повідомлень, механізми їх передачі, зберігання, опрацювання даних тощо; 2) блокування передачі повідомлень; 3) вплив на зміст повідомлень шляхом проведення СІО та АЗА.

Визначають сім складових елементів ІВ: 1) стратегія і тактика нейтралізації органів управління противника (командна війна); 2) розвідувальна війна; 3) електронна війна; 4) психологічна війна; 5) комп'ютерна війна; 6) ІВ в економічній сфері; 7) ІТ.

Основними компонентами ІВ у військовій сфері прийнято вважати: 1) розвідку; 2) контррозвідку (насамперед протидію розвідці противника, включаючи маскування і дезінформацію); 3) радіоелектронну боротьбу; 4) автоматизоване управління військами і зброєю; 5) з'ясування державної приналежності військових об'єктів, їх ідентифікацію; 6) навігаційне забезпечення своїх військ (сил) і засобів; 7) морально-психологічне забезпечення дій власних військ (сил), психологічну боротьбу з противником.

ІВ, СІО та АЗА є різновидами інформаційної боротьби (ІБ). Її у наукових колах прийнято розрізняти в широкому і вузькому розумінні. Так, у широкому розумінні ІБ — це форма боротьби, що становить сукупність спеціальних (політичних, економічних, дипломатичних, технологічних, військових та інших) методів, способів і засобів впливу на інформаційну сферу конфронтуючої сторони і захисту власної в інтересах досягнення поставлених цілей.

У вузькому розумінні ІБ (у військовій, оборонній сферах) — це комплекс заходів інформаційного характеру, що здійснюються з метою захоплення й

утримання стратегічної ініціативи, досягнення інформаційної переваги над супротивником і створення сприятливого пропагандистського підґрунтя при підготовці й веденні бойової та іншої діяльності збройних сил.

У військовій сфері визначають два види ІБ – інформаційно-технічну та інформаційно-психологічну. Головними об'єктами впливу та захисту інформаційно-технічної боротьби є системи телекомунікацій і зв'язку, радіоелектронні засоби тощо. Об'єктом інформаційно-психологічного впливу залишаються свідомість і психіка населення й особового складу збройних сил, спецслужб противника та системи формування суспільної думки і прийняття концептуальних рішень.

Інформаційно-психологічний вплив передбачає цілеспрямовану розробку та поширення спеціальної актуальної інформації, здатної безпосередньо чи опосередковано впливати на суспільну свідомість, психологію і поведінку населення, військовослужбовців. При цьому інформація психологічного і пропагандистського типу може бути не тільки усного, друкованого, письмового, аудіо- та візуального походження, а й екстрасенсорного, телепатичного та іншого, розрахованою на підсвідомість реципієнта.

ІБ ведеться на трьох рівнях: стратегічному, оперативному і тактичному. На стратегічному рівні інформаційне протиборство планують і координують найвищі органи державної влади. На оперативному і тактичному рівнях ця діяльність проводиться силами і засобами збройних сил, спецслужб, а також суспільно-політичних інститутів держави.

Висновки

Існує нагальна потреба виконати науково-дослідну роботу „Шляхи і механізми забезпечення інформаційної безпеки", замовником якої має бути, на нашу думку, РНБО України. До її виконання необхідно залучити: Національну академію Служби безпеки України, Інститут Служби зовнішньої розвідки України, Інститут військової розвідки Міністерства оборони України, Національний інститут стратегічних досліджень, Військовий інститут Київського національного університету ім. Т. Шевченка, Національну академію оборони України, Інститут міжнародних відносин, Державний університет інформаційно-комунікаційних технологій.

Для навчально-методичного забезпечення інформаційної безпеки держави необхідно запровадити у вищих спеціальних навчальних закладах системи Служби безпеки, Служби зовнішньої розвідки, Головного управління розвідки МО України, Військовому інституті Київського національного університету ім. Т. Шевченка та Державному університеті інформаційно-комунікаційних технологій спецкурс для підготовки кваліфікованих фахівців із захисту інформаційного простору від деструктивного інформаційного впливу, а також налагодити взаємодію щодо обміну науковими і навчально-методичними розробками з протидії

СІО та АЗА.

Нині існує немало літератури щодо різних аспектів здійснення спеціальних інформаційних операцій, актів зовнішньої інформаційної агресії та іншого деструктивного інформаційного впливу, але ця література або чисто популярна, або суто наукова (монографії, дисертації). До того ж більшість таких праць виконано російськими публіцистами і вченими, і тому в них, природно, не враховується специфіка інформаційної безпеки України. Отже нагальною є необхідність розробки відповідної навчальної літератури (посібники, підручники), методичних розробок (програми навчальних курсів) для підготовки висококваліфікованих фахівців.

Слід зазначити, що 2007 року вийшов друком посібник „Соціально-правові основи інформаційної безпеки" – перша вітчизняна праця, призначена для підготовки фахівців з протидії деструктивному інформаційному впливу. Вона може використовуватися й практикуючими психологами, представниками соціальних служб і силових відомств. У цій праці автори подали своє бачення змісту й сутності інформаційного протиборства, виходячи з аналізу і узагальнення різних точок зору щодо цієї проблеми. У ній здійснено й аналіз технологій проведення інформаційних війн, спеціальних інформаційних операцій та актів зовнішньої інформаційної агресії, а також розкрито основні загрози національній безпеці України в інформаційній сфері. У праці розглядаються основні функції суб'єктів системи забезпечення інформаційної безпеки України.

Нині готується до друку новий навчальний посібник – „Інформаційна безпека в епоху глобалізації: соціально-правові аспекти", у якому глибше розглядаються проблеми захисту держави, суспільства та особи від деструктивних інформаційних впливів.

Література:

1. **Крысько В. Г.** Секреты психологической войны (цели, задачи, методы, формы, опыт). – Мн.: Харвест, 1999.

2. **Манойло А. В., Петренко А. И., Фролов Д. Б.** Государственная информационная политика в условиях информационно-психологической войны. - 2-е изд., стереотип. – М.: Горячая линия. Телеком, 2006.

3. **Почепцов Г. Г.** Пропаганда и контрпропаганда. – М.: Центр, 2004.

4. **Литвиненко О. В.** Спеціальні інформаційні операції та пропагандистські кампанії: Монографія. – К.: Сатсанга, 2000.

5. Методы и приёмы психологической войны / Сост., ред. А. Т. Тарас. – М.: АСТ, – Мн.: Харвест, 2006.

6. Інформаційна безпека держави у контексті протидії інформаційним війнам: Навчальний посібник // За заг. ред. В. Б. Толубка. – К.: НАОУ, 2004.

7. Нарис теорії і практики інформаційно-психологічних операцій /

Дзюба М. Т., Жарков Я. М., Ольховой І. О., Онищук М. І.: Навч. посібник// За заг. ред. В. В. Балабіна. – К.: ВІТІ НТУУ „КПІ", 2006.

8. **Кормич Б. А.** Організаційно-правові засади політики інформаційної безпеки України: Монографія. — Одеса: Юридична література, 2003.

9. **Петрик В. М., Остроухов В. В.** та ін. Сучасні технології та засоби маніпулювання свідомістю, ведення інформаційних війн і спеціальних інформаційних операцій: Навчальний посібник. – К.: Росава, 2006.

10. **Петрик В. М., Кузьменко А. М., Остроухов В. В.** та ін. Соціально-правові основи інформаційної безпеки: Навчальний посібник. – К.: Росава, 2007.