

інфраструктури України сприяє експансії іноземними компаніями ринку інформаційних послуг, що створює сприятливі умови для перерозподілу ефірного часу на користь іноземних програм, окремі з яких засмічують український інформаційний простір своїм баченням подій, пропагують спосіб життя та традиції, тим самим деструктивно впливаючи на суспільство і державу, руйнуючи морально-етичні основи генофонду української нації.

Недостатній професійний, інтелектуальний і творчий рівень вітчизняного виробника інформаційного продукту та послуг, його не конкурентоспроможність не лише на світовому ринку, а й в Україні, призводить до того, що українська аудиторія, природно, віддає перевагу іноземним інформаційним програмам. Недостатній контроль з боку держави за дотриманням законів України політичними силами, ЗМІ та окремими особами, які займаються підприємницькою діяльністю в інформаційній сфері, призводить до того, що нині трапляються непоодинокі випадки надання ефірного часу теле- та радіопрограм, спрямованим на руйнування моральних цінностей, свідомості української нації.

З метою протидії негативним впливам інформаційної пропаганди та інформаційних війн, задля нейтралізації та упередження реальних та потенційних загроз в інформаційному просторі України виникає необхідність удосконалення нормативно-правового забезпечення та запобігання й нейтралізації потенційних і реальних загроз національній безпеці в інформаційній сфері.

Використані джерела:

1. Почепцов Г. Сучасні інформаційні війни / Г. Почепцов. – К.: Вид. дім «Києво-Могилянська академія», 2015. – 497 с.
2. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції [Текст] : навч. посіб. / В. А. Ліпкан, Ю. Є. Макименко, В. М. Желіховський. – К.: КНТ, 2006. – 345 с.
3. Медвідь Ф. Інформаційна безпека України: виклики та загрози Електронний ресурс. – Режим доступу. URL: <http://www.nato.ru.if.ua/journal/2009-2-28.pdf>.

Староконь Ю.М. – студентка 1 курсу юридичного факультету
Науковий керівник: Синиціна Ю.П. доцент кафедри економічної та інформаційної безпеки, к.т.н., доцент (Дніпропетровський державний університет внутрішніх справ, м. Дніпро)

РОЛЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ СУЧАСНОГО СУСПІЛЬСТВА

Мабуть, кожен студент замислюється над тим, навіщо він вивчає той чи інший предмет. Також і всі люди в нашому суспільстві хоч раз замислювались, навіщо нам

ті чи інші поняття, сфери діяльності тощо. Теж саме з інформаційною безпекою, не всі люди усвідомлюють її важливість в нашому житті.

Інформаційна безпека є однією із найсуттєвіших складових частин національної безпеки країни, її забезпечення, завдяки послідовній реалізації та бездоганно сформульованій інформаційній стратегії, значною мірою сприяла б забезпеченню досягнення успіхів при вирішенні проблем з політичної, військово-політичної, військової, соціальної, економічної та інших державних сфер діяльності.

Вивченням ролі держави у формуванні інформаційного суспільства займаються такі вчені, як Арістова І. [1], Почепцов Г. [2] та ін. Ряд публіцистів Супрун В. [3], Ярочкін В. [4] розробили основні принципи забезпечення інформаційної безпеки. В той же час, окремого дослідження вимагають структурно-функціональні аспекти процесу гарантування інформаційної безпеки.

Поняття інформаційна безпека можна розглядати з двох сторін. З одного боку, це захищеність інформаційного середовища суспільства, що забезпечує його формування, використання та розвиток в інтересах громадян, організацій чи держави. А з іншого боку, інформаційна безпека - це стан захищеності потреб в інформації певної особи, суспільства, держави, при якому забезпечується їх існування та розвиток, що не залежить від наявності зовнішніх та внутрішніх інформаційних загроз. Інформаційним середовищем називають сферу діяльності суб'єктів, пов'язану зі створенням, обробленням й споживанням будь-якої інформації. Стан інформованості визначає ступінь адекватності сприйняття суб'єктами дійсності, і як наслідок – обґрунтованість прийняття будь-яких рішень та дій [5]. В правових аспектах інформаційна безпека – це одна із сторін розгляду інформаційних відносин, в межах інформаційного законодавства з позиції захисту життєво необхідних інтересів певної особистості, суспільства чи держави. Акцентування уваги на можливих загрозах, цим інтересам і на механізмах усунення або запобігання цих загроз суто правовими методами. Принципи забезпечення інформаційної безпеки містять: законність, баланс інтересів особи, суспільства і держави, комплексність, системність, інтеграція з міжнародними системами безпеки, економічна ефективність (рис. 1).

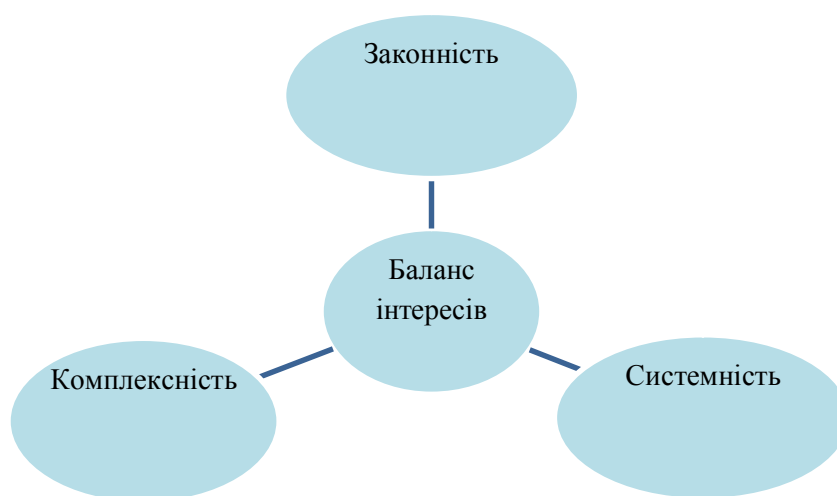


Рис. 1. Принципи забезпечення інформаційної безпеки

Об'єктами інформаційної безпеки можуть бути: свідомість та психіка людини, інформаційні системи різного масштабу та призначення. Соціальних об'єктами інформаційної безпеки є: особистість, колектив, держава, суспільства, світове товариство.

До суб'єктів інформаційної безпеки відносять: державу, що здійснює свої функції через відповідні органи; громадян; суспільні або інші організації та об'єднання, яка володіють повноваженнями стосовно забезпечення інформаційної безпеки відповідно до чинного законодавства (рис. 2).

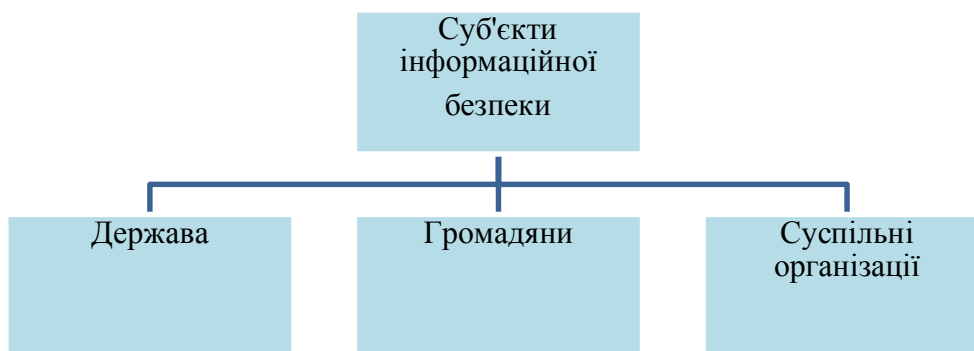


Рис. 2. Складові інформаційної безпеки

Інформаційну безпеку поділяють на інформаційну безпеку особистості та інформаційну безпеку держави.

Інформаційна безпека особистості – це захищеність психіки та свідомості людини від небезпечного інформаційного впливу - маніпулювання свідомістю: дезінформування, спонукання до образливих дій, самогубства тощо.

Інформаційна безпека держави - міра захищеності держави чи державного суспільства, стійкості основних сфер життєдіяльності (економіки, науки, технологічної сфери, сфери управління, військової справи тощо), відносно небезпечних інформаційних впливів. Інформаційна безпека держави характеризується здатністю протистояти цим впливам. Концепція інформаційної безпеки держави – це систематизована сукупність відомостей про інформаційну безпеку держави та шляхи її забезпечення. В рамках цієї концепції проводиться системна класифікація руйнівних факторів та інформаційних загроз безпеці особистості, суспільства, держави; обґрунтовують основні положення з організації забезпечення інформаційної безпеки держави; розробляються пропозиції стосовно способів і форм забезпечення інформаційної безпеки.

Загрози інформаційній безпеці – сукупність умов і факторів, що створюють небезпеку життєвонеобхідним інтересам особистості, суспільства й держави в інформаційній сфері. Загрози інформаційній безпеці поділяються на три основні групи (рис 3): загрози впливу неякісної інформації (недостовірної, фальшивої, дезінформації) на особистість, суспільство, державу; загрози несанкціонованого й неправомірного впливу сторонніх осіб на інформацію і інформаційні ресурси, їх виробництво, формування й використання; загрози інформаційним правам і свободам особистості (праву на виробництво інформації, її поширення, пошук,

одержання, передавання та використання; праву на інтелектуальну власність на інформацію, в тому числі й речову).

Дестабілізуючі фактори - це явища або процеси, які породжують інформаційні загрози. Джерелами дестабілізуючих факторів можуть бути як окремі особи, так й організації та їх об'єднання. Особливу групу джерел складають інформаційні системи та засоби, так як вони одночасно є знаряддями приведення в дію інформаційних загроз, каналом їхнього проникнення у свідомість особистості або суспільну свідомість і творцем загроз, що виникають внаслідок технічних несправностей або інших причин.

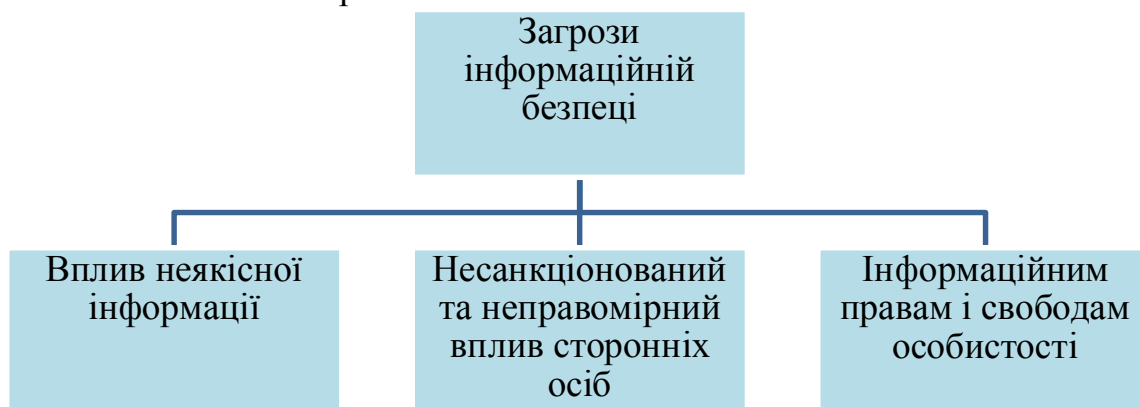


Рис. 3. Класифікація загроз інформаційної безпеки

Джерелом дестабілізуючих факторів також може бути природне середовище. Кожному джерелу властиві певні види дестабілізуючих факторів, які можна подати у вигляді міждержавних і внутрішньодержавних. До внутрішньодержавних дестабілізуючих факторів відносять: правовий вакуум у більшості питань забезпечення інформаційної безпеки, порушення законодавства з питань інформаційної безпеки, політичні конфлікти, відмови, збої, технічні помилки інформаційних засобів, природні явища, що ускладнюють передачу, прийом і зберігання інформації або руйнують інформаційні системи. Міждержавні дестабілізуючі фактори – це конфлікти різноманітних масштабів і проявів (в економіці, політиці, ідеології, дипломатії тощо).

Отже, як висновок я хочу сказати що інформаційне суспільство може існувати тільки лише за умови, що його члени оволодіють інформаційною культурою – будуть дотримуватись етичних норм поведінки в інформаційному просторі. Це сформує інформаційний захист кожної людини та суспільства у цілому. Формування інформаційного середовища не у відповідності з глобальними законами функціонування природних систем може наблизити критичну ситуацію на планеті не менш, ніж ядерна загроза. Інформація вже стала стратегічним озброєнням. Тому кожна людина мусить знати, що коли вона вносить нову інформацію в інформаційний простір, вона тим самим керує формуванням інформаційного середовища людей, тобто безпосередньо впливає на свідомість та розвиток інших людей. Кожен новий блок інформації, який надходить в інформаційне середовище людства, повинен мати правила безпечного користування. Як окрема людина, так і суспільство в цілому має можливість запобігати інформаційних небезпек, завдяки

формуванню інформаційного щита: системи цінностей, яка орієнтована на глобальні принципи безпеки життєдіяльності людства [6].

Використані джерела:

1. Арістова, І.В. Діяльність органів внутрішніх справ щодо реалізації державної інформаційної політики : монографія [Текст] / І. В. Арістова. –Х. : Нац. ун-т внутр. справ, 2006. –354 с.

2. Почепцов Г.Г., Чукут С.А. Інформаційна політика: навч. посіб. — Київ: Знання, 2006. – 665 с.

3. Suprun, V.M. Information sovereignty as part of information security: theoretical and legal aspects. Електронний ресурс. URL: <http://www.nbu.gov.ua/portal/natural/vkhnu/Pravo/2009>.

4. Yarochkin, V. The security system company. Електронний ресурс. URL: <http://www.nbu.gov.ua>.

5. Костецький Р. Інформаційна безпека особистості: Інформаційна безпека Електронний ресурс. URL: <https://sites.google.com/site/infobezpekaosobu/informacijna-bezpeka>

6. Варивода К.С. Інформаційна безпека підлітків в Інтернет мережі / К.С. Варивода // Молодий вчений. – 2016. – № 3. – С. 365-368. Електронний ресурс. URL: <http://molodyvcheny.in.ua/files/journal/2017/9.1/10.pdf>

Стеценко В.В., курсант

Травина Д. В., курсант

Науковий керівник: Богучарова О.І.

професор кафедри юридичної лінгвістики
та практичної психології,

доктор психологічних наук, доцент

Луганського державного університету
внутрішніх справ імені Е.О. Дідоренка

ХМАРНІ ТЕХНОЛОГІЇ У ФОРМУВАННІ МЕДІАЦІЙНОЇ КОМПЕТЕНТНОСТІ МАЙБУТНІХ ПРАВООХОРОНЦІВ

Осмилення та подальша імплементація у вітчизняну правову систему програм відновного правосуддя, особливо в частині роботи з дітьми, наприклад, відпрацювання та захист виявлених жертв жорстокого поводження, шкільного булінгу, експлуатації і торгівлі людьми (підлітки і жінки) має на меті, звісно, відновлення справедливості та збалансування потреб потерпілого, правопорушника та громади. Проте, не менш важливим у всіх таких випадках є також намагання