Київський національний університет імені Тараса Шевченка

ІНФОРМАЦІЙНА БЕЗПЕКА
ОСОБИСТОСТІ, СУСПІЛЬСТВА, ДЕРЖАВИ

Київ – 2008

Київський національний університет імені Тараса Шевченка

ІНФОРМАЦІЙНА БЕЗПЕКА ОСОБИСТОСТІ, СУСПІЛЬСТВА, ДЕРЖАВИ

Підручник

Видавничо-поліграфічний центр “Київський університет”
Київ – 2008

УДК 351:007
ББК 66.4

Рекомендовано Міністерством оборони України як підручник для для студентів військових спеціальностей вищих навчальних закладів (лист № 263/2/4817 від 28 грудня 2007 року)

Затверджено до друку вченою радою Військового інституту Київського національного університету імені Тараса Шевченка (протокол № 10 від 17 грудня 2007 року)

Рецензенти:
лауреат Державної премії України в галузі науки і техніки, заслужений діяч науки і техніки України, доктор технічних наук, професор Ю.Г.ДАНИК – професор кафедри Національної академії оборони України;
доктор філософських наук, професор В.О. АНАНЬЇН – професор кафедри військово-гуманітарних дисциплін Військового інституту телекомунікацій та інформатизації Національного технічного університету України "КПІ";
доктор технічних наук, професор С.В. ЛЄНКОВ – начальник наукового центру Військового інституту Київського національного університету імені Тараса Шевченка.

Жарков Я.М., Дзюба М.Т., Замаруєва І.В., ін.
Інформаційна безпека особистості, суспільства, держави: Підручник. – К.: Видавничо-поліграфічний центр "Київський університет", 2008. – 274 с.
ISBN _____

Підручник підготовлений відповідно до навчальної програми дисципліни "Воєнно-прикладні аспекти інформаційної безпеки", яка викладається у Військовому інституті Київського національного університету імені Тараса Шевченка. У підручнику розглянуто основи національної безпеки держави, теоретичні аспекти інформаційної безпеки, проблеми безпеки державного управління як об'єкту інформаційної боротьби, проблеми інформаційної безпеки суспільств

та особистості, а також механізми забезпечення інформаційної безпеки держави, суспільства, особистості.

Авторський колектив: Я.М. Жарков, М.Т. Дзюба, І.В. Замаруєва, М.І. Онищук, М.М. Присяжнюк, А.О. Рось

УДК 351:007
ББК 66.4

ISBN _____

ЗМІСТ

СКОРОЧЕННЯ

АСУ – автоматизована система управління;
ВНЗ – вищий навчальний заклад;
ЕОМ – електронно-обчислювальна машина;
ІК – інформаційна культура;
ЗМІ – засоби масової інформації;
ЗМУ – зброя масового ураження;
ЗНФП – зброя на нових фізичних принципах;
ІАД – інформаційно-аналітична діяльність;
ІАЗ – інформаційно-аналітичне забезпечення;
ІПС – інформаційно-пошукова система;
ІР – інформаційний ресурс;
ІТ – інформаційна технологія;
ІТК – інструментально-технологічний комплекс;
КВ – комп'ютерний вірус;
НАНУ – Національна академія наук України;
НДДКР – науково-дослідні та дослідно-конструкторські роботи;
НЛП – нейролінгвістичне програмування;
ОШ КНШ – Об'єднаний штаб комітету начальників штабів;
ППО – протиповітряна оборона;
ПР – паблік релейшнз;
ПрГ – предметна галузь;
ПТК – програмно-технічний комплекс;
РВК – розвідувально-вогневі комплекси;
РЕБ – радіоелектронна боротьба;
РЕЗ – радіоелектронні засоби;
РЕП – радіоелектронна протидія;
РЛС – радіолокаційна станція;
РУБС – розвідувально-ударні бойові системи;
СНД – Союз незалежних держав;
СПМВ – спеціальний програмно-математичний вплив;
ТБ – телебачення;
ТВД – театр воєнних дій;
ФАУЗІ – Федеральне агентство урядового зв'язку та інформації при Президентові РФ.

ПЕРЕДМОВА

Сучасна епоха побудови інформаційного суспільства, тобто суспільства, в якому більшість працездатного населення (на відміну від аграрного чи індустріального) залучена до інформаційної сфери, сприяє розвитку нових форм і способів досягнення країнами політичних, економічних та інших цілей на інформаційному рівні. Не дивно, що в системі національної безпеки розвинених країн передбачено реалізацію національних стратегій (програм) національної безпеки, до яких входять політичні, воєнні, економічні, соціальні, інформаційні й інші стратегії. Особлива роль при цьому належить інформаційним стратегіям, основне призначення яких полягає в забезпеченні реалізації решти стратегій. Інформаційні стратегії набувають вирішального значення у разі реалізації політичних стратегій співдружності або своєрідної "зброї", якщо реалізуються стратегії суперництва.

Останнім часом визначальної ваги інформаційна безпека набуває у воєнній сфері. Безпосередньо у воєнній справі рівень інформаційного потенціалу все більшою мірою обумовлює оперативність прийняття рішень, структуру і якість озброєнь, оцінку рівня їх достатності, дієвість пропаганди, ефективність дій союзників і власних збройних сил і, в підсумку, результат збройного протистояння.

Концепція тотальної війни в традиційному розумінні себе зживає. Проте наступає епоха так званих "цивілізованих" війн, в яких політичні й економічні цілі досягаються не прямим збройним втручанням, а використанням нових форм насилля та підриву могутності противника зсередини.

Отже, у сучасному суспільстві одним з основних джерел загроз національній безпеці держави стали "нетрадиційні", зокрема інформаційні війни, які розвиненими країнами розглядаються як найбільш ефективний засіб забезпечення своїх національних інтересів.

У сучасних умовах Україна є об'єктом безперервного інформаційно-психологічного впливу, що обумовлено її геополітичним положенням і наявністю політичних, економічних та інших інтересів щодо нашої держави з боку розвинених країн та сусідніх держав, що зумовлює велику ймовірність втягнення її в інформаційну війну.

У цьому контексті проблеми забезпечення інформаційної безпеки національних інтересів у будь-якій сфері останнім часом набувають усе більшої значущості. Згідно зі ст.17 Конституції України, забезпечення інформаційної безпеки держави стоїть на одному рівні із захистом суверенітету й територіальної цілісності України, забезпеченням її економічної безпеки як найважливішими функціями держави.

Державна політика забезпечення інформаційної безпеки України є невід'ємною складовою державної політики національної безпеки України і являє собою офіційно прийняту систему поглядів та практичну діяльність органів державної влади і управління, спрямовану на забезпечення такого стану соціальних суб'єктів, при якому дія будь-якої інформаційної загрози не призводить до зниження рівня їх інформаційної безпеки нижче припустимого, небезпечного з високою ймовірністю реалізації негативних інформаційних впливів.

Нині кожний громадянин України має володіти високим рівнем культури у сфері інформаційної безпеки країни, суспільства, особистості, розуміти механізми інформаційного (інформаційно-психологічного впливу) та захисту від нього. Її формування тісно пов'язане як з вихованням, так і професійною підготовкою, становленням індивіда і як особистості, і як фахівця у певній галузі знань. Особливо це стосується воєнної сфери.

Даний підручник посідає особливе місце серед чисельної навчальної літератури, присвяченої проблемам інформаційної безпеки. Його унікальність полягає у тому, що вперше на єдиних системних засадах викладені основи національної безпеки держави, місце і роль інформаційної безпеки в системі національної безпеки держави, сутність інформаційних воєн як джерела інформаційних загроз національним інтересам держави, зокрема у воєнній сфері, сутність інформаційної боротьби як інструмента забезпечення інформаційної безпеки держави, категоріальний апарат і теоретичні

основи інформаційної безпеки, а під цим кутом – напрями і механізми інформаційного впливу на систему державного управління, інформаційні технології в управлінні як об'єкт інформаційної боротьби, інформаційно-аналітична діяльність як фактор безпеки прийняття управлінських рішень в умовах інформаційної боротьби.

Особлива увага приділена дослідженню проблем інформаційної безпеки суспільства та особистості: розглядаються суспільна свідомість та її роль у формуванні національної ідеї, сучасні технології маніпуляції масовою свідомістю, сучасні засоби впливу на суспільство та фактори негативного інформаційно-психологічного впливу на суспільну свідомість і шляхи їх нейтралізації, як модель особистості – морально-семантичний фільтр – його складові та механізми сприймання інформації з оточуючого середовища, свідомість і підсвідомість особистості та механізми їх взаємодії, рефлексивне управління як технологія маніпуляції поведінкою особистості, безпека життєдіяльності людини в інформаційному просторі.

Підручник має воєнно-прикладну спрямованість, оскільки саме у воєнній сфері найбільш рельєфно виявляються проблеми інформаційної безпеки, можливості та наслідки застосування технологій інформаційного впливу для забезпечення провідними країнами своїх інтересів у будь-якому регіоні світу. Разом з тим, розглянутий категоріальний апарат у сфері інформаційної безпеки, досліджені закономірності та механізми реалізації інформаційного (інформаційно-психологічного) впливу на країну, суспільство, особистість є загальними і прийнятними у будь-якій сфері державної і суспільної діяльності.

Розділ 1.

ОСНОВИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ДЕРЖАВИ – ОРГАНІЗАЦІЙНО-ПРАВОВІ АСПЕКТИ

В розділі викладено організаційно-правові основи національної безпеки України у відповідності із Законом України «Про основи національної безпеки». Детально розглянуто роль і місце інформаційної безпеки в системі національної безпеки України.

1.1. Загальні положення

Основні засади державної політики, спрямованої на захист національних інтересів і гарантування в Україні безпеки особи, суспільства і держави від зовнішніх і внутрішніх загроз в усіх сферах життєдіяльності містяться в *законі України "Про основи національної безпеки України"* [1]. У ньому наведені такі визначення базових термінів:

національна безпека – захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам;

національні інтереси – життєво важливі матеріальні, інтелектуальні і духовні цінності Українського народу як носія суверенітету і єдиного джерела влади в Україні, визначальні потреби суспільства і держави, реалізація яких гарантує державний суверенітет України та її прогресивний розвиток;

загрози національній безпеці – наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України.

Корисним у методичному плані є таке визначенням *національної безпеки*: це сукупність зв'язків і відношень, які характеризують такий стан особистості, соціальної групи, суспільства, держави, народу, при якому забезпечуються їх тривале, стабільне існування, задоволення і

реалізація життєвих потреб, спроможність до ефективного відбиття внутрішніх і зовнішніх загроз, саморозвитку і прогресу [2].

Правову основу у сфері національної безпеки України обумовлюють Конституція, закони України, міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, а також видані на виконання законів інші нормативно-правові акти.

Відповідно до цього Закону розробляються і затверджуються Президентом України Стратегія національної безпеки України і Воєнна доктрина України, доктрини, концепції, стратегії і програми, якими визначаються цільові настанови та керівні принципи воєнного будівництва, а також напрями діяльності органів державної влади в конкретній обстановці з метою своєчасного виявлення, відвернення і нейтралізації реальних і потенційних загроз національним інтересам України. Стратегія національної безпеки України і Воєнна доктрина України є документами, обов'язковими для виконання, і основою для розробки конкретних програм за складовими державної політики національної безпеки.

Об'єктами національної безпеки є:

– людина і громадянин - їхні конституційні права і свободи;

– суспільство – його духовні, морально-етичні, культурні, історичні, інтелектуальні та матеріальні цінності, інформаційне і навколишнє природне середовище і природні ресурси;

– держава – її конституційний лад, суверенітет, територіальна цілісність і недоторканність.

Суб'єктами забезпечення національної безпеки є: Президент України; Верховна Рада України; Кабінет Міністрів України; Рада національної безпеки і оборони України; міністерства та інші центральні органи виконавчої влади; Національний банк України; суди загальної юрисдикції; Прокуратура України; місцеві державні адміністрації та органи місцевого самоврядування; Збройні Сили України, Служба безпеки України, Служба зовнішньої розвідки України, Державна прикордонна служба України та інші військові формування, утворені відповідно до законів України; громадяни України, об'єднання громадян.

У законі України “Про основи національної безпеки України” визначені сфери національної безпеки, які наведені на рис. 1.1. У

дужках на рисунку наведені найбільш вживані назви різновиду безпеки національних інтересів у відповідній сфері.

Рис. 1.1. Сфери національної безпеки

Основними принципами забезпечення національної безпеки є:

– пріоритет прав і свобод людини і громадянина;

– верховенство права;

– пріоритет договірних (мирних) засобів у розв'язанні конфліктів;

– своєчасність та адекватність заходів захисту національних інтересів реальним і потенційним загрозам;

– чітке розмежування повноважень та взаємодія органів державної влади в забезпеченні національної безпеки;

– демократичний цивільний контроль над Воєнною організацією держави та іншими структурами в системі національної безпеки;

– використання в інтересах України міждержавних систем та механізмів міжнародної колективної безпеки.

Національна безпека України втілюється шляхом проведення виваженої державної політики відповідно до прийнятих в установленому порядку доктрин, концепцій, стратегій і програм у політичній, економічній, соціальній, воєнній, екологічній, науково-технологічній, інформаційній та інших сферах.

Вибір конкретних засобів і шляхів забезпечення національної безпеки України обумовлюється необхідністю своєчасного вжиття заходів, адекватних характеру і масштабам загроз національним інтересам.

Пріоритетами національних інтересів України є:

– гарантування конституційних прав і свобод людини і громадянина;

– розвиток громадянського суспільства, його демократичних інститутів;

– захист державного суверенітету, територіальної цілісності та недоторканності державних кордонів, недопущення втручання у внутрішні справи України;

– зміцнення політичної і соціальної стабільності в суспільстві;

– забезпечення розвитку і функціонування української мови як державної в усіх сферах суспільного життя на всій території України, гарантування вільного розвитку, використання і захисту російської, інших мов національних меншин України;

– створення конкурентоспроможної, соціально орієнтованої ринкової економіки та забезпечення постійного зростання рівня життя і добробуту населення;

– збереження та зміцнення науково-технологічного потенціалу, утвердження інноваційної моделі розвитку;

– забезпечення екологічно та техногенно-безпечних умов їх життєдіяльності громадян і суспільства, збереження навколишнього природного середовища та раціональне використання природних ресурсів;

– розвиток духовності, моральних засад, інтелектуального потенціалу Українського народу, зміцнення фізичного здоров'я нації, створення умов для розширеного відтворення населення;

– інтеграція України в європейський політичний, економічний, правовий простір та в євроатлантичний безпековий простір; розвиток рівноправних взаємовигідних відносин з іншими державами світу в інтересах України.

1.2. Основні напрями державної політики з питань національної безпеки України

Основними напрямами державної політики з питань національної безпеки України є:

У зовнішньополітичній сфері **–** проведення активної міжнародної політики України з метою:

– створення сприятливих зовнішньополітичних умов для прогресивного економічного і соціального розвитку України;

– запобігання втручанню у внутрішні справи України і відвернення посягань на її державний суверенітет і територіальну цілісність з боку інших держав;

– забезпечення повноправної участі України в загальноєвропейській та регіональних системах колективної безпеки, набуття членства у Європейському Союзі та Організації Північноатлантичного договору при збереженні добросусідських відносин і стратегічного партнерства з Російською Федерацією, іншими країнами Співдружності Незалежних Держав, а також з іншими державами світу;

– сприяння усуненню конфліктів, насамперед у регіонах, що межують з Україною;

– участь у міжнародній миротворчій діяльності під егідою ООН, ОБСЄ, інших міжнародних організацій у сфері безпеки;

– участь у заходах щодо боротьби з міжнародними організованими злочинними угрупованнями та міжнародним тероризмом, протидія поширенню ядерної та іншої зброї масового ураження і засобів її доставки;

– адаптація законодавства України до законодавства Європейського Союзу.

У сфері державної безпеки:

– реформування правоохоронної системи з метою підвищення ефективності її діяльності на основі оптимізації структури, підвищення рівня координації діяльності правоохоронних органів, покращення їх фінансового, матеріально-технічного, організаційно-правового і кадрового забезпечення;

– зосередження ресурсів і посилення координації діяльності правоохоронних, розвідувальних і контррозвідувальних органів України для боротьби з організованою злочинністю та наркобізнесом;

– участь України в міжнародному співробітництві у сфері боротьби з міжнародною злочинністю, тероризмом, наркобізнесом, нелегальною міграцією;

– відпрацювання ефективно діючої системи контролю за поставками продукції і технологій оборонного призначення і подвійного використання.

У воєнній сфері та сфері безпеки державного кордону України:

– прискорення реформування Збройних Сил України та інших військових формувань з метою забезпечення їх максимальної ефективності та здатності давати адекватну відповідь реальним та потенційним загрозам Україні; перехід до комплектування Збройних Сил України на контрактній основі;

– здійснення державних програм модернізації наявних, розроблення та впровадження новітніх зразків бойової техніки та озброєнь;

– посилення контролю за станом озброєнь і захищеністю військових об'єктів; активізація робіт з утилізації зброї;

– впровадження системи демократичного цивільного контролю над Воєнною організацією та правоохоронними органами держави;

– забезпечення соціального захисту військовослужбовців та членів їх сімей;

– дотримання угод щодо тимчасового розташування Чорноморського флоту Російської Федерації на території України;

– прискорення процесу делімітації та демаркації кордонів України;

– боротьба з організованими злочинними угрупованнями, у тому числі з міжнародними, які намагаються діяти через державний кордон України, в пунктах пропуску та виключній (морській) економічній зоні України;

– поглиблення транскордонного співробітництва з суміжними державами.

У внутрішньополітичній сфері:

– забезпечення неухильного додержання конституційних прав і свобод людини і громадянина, захист конституційного устрою, удосконалення системи політичної влади з метою зміцнення демократії, духовних та моральних підвалин суспільства; підвищення ефективності функціонування політичних інститутів влади;

– створення дійових, у тому числі судових, механізмів захисту конституційних прав людини і основних свобод;

– забезпечення політичної стабільності, громадянського миру та взаєморозуміння в суспільстві, запобігання проявам екстремізму;

– забезпечення прозорості в діяльності державних органів, прийнятті управлінських рішень, інформованості населення, зміцнення на цій основі його довіри до владних інститутів;

– створення повноцінного, ефективно діючого місцевого і регіонального самоврядування;

– формування і вдосконалення політико-правових, соціально-економічних та духовно-культурних засад етнонаціональної стабільності, відпрацювання ефективних механізмів узгодження інтересів етнічних спільнот та розв'язання міжнаціональних суперечностей;

– забезпечення міжконфесійної стабільності та запобігання конфліктним загостренням на релігійній основі, недопущення протистояння різних церков, у тому числі щодо розподілу сфер впливу на території України.

В економічній сфері:

– забезпечення умов для сталого економічного зростання та підвищення конкурентоспроможності національної економіки;

– прискорення прогресивних структурних та інституціональних змін в економіці, поліпшення інвестиційного клімату, підвищення ефективності інвестиційних процесів;

– стимулювання випереджувального розвитку наукоємних високотехнологічних виробництв;

– удосконалення антимонопольної політики; створення ефективного механізму державного регулювання природних монополій;

– подолання "тінізації" економіки через реформування податкової системи, оздоровлення фінансово-кредитної сфери та припинення відпливу капіталів за кордон, зменшення позабанківського обігу грошової маси;

– забезпечення збалансованого розвитку бюджетної сфери, внутрішньої і зовнішньої захищеності національної валюти, її стабільності, захисту інтересів вкладників, фінансового ринку;

– здійснення виваженої політики внутрішніх та зовнішніх запозичень;

– забезпечення енергетичної безпеки на основі сталого функціонування і розвитку паливно-енергетичного комплексу, у тому числі послідовного й активного проведення політики енергозбереження та диверсифікації джерел енергозабезпечення;

– забезпечення продовольчої безпеки;

– захист внутрішнього ринку від недоброякісного імпорту - поставок продукції, яка може завдавати шкоди національним виробникам, здоров'ю людей та навколишньому природному середовищу;

– посилення участі України в міжнародному поділі праці, розвиток експортного потенціалу високотехнологічної продукції, поглиблення інтеграції в європейську й світову економічну систему та активізація участі в міжнародних економічних і фінансових організаціях.

У науково-технологічній сфері:

– посилення державної підтримки розвитку пріоритетних напрямів науки і техніки як основи створення високих технологій та забезпечення переходу економіки на інноваційну модель розвитку, створення ефективної системи інноваційної діяльності в Україні;

– поетапне збільшення обсягів бюджетних видатків на розвиток освіти і науки, створення умов для широкого залучення в науково-технічну сферу позабюджетних асигнувань;

– створення економічних і суспільно-політичних умов для підвищення соціального статусу наукової та технічної інтелігенції;

– забезпечення необхідних умов для реалізації прав інтелектуальної власності;

– забезпечення належного рівня безпеки експлуатації промислових, сільськогосподарських і військових об'єктів, споруд та інженерних мереж.

В екологічній сфері:

– здійснення комплексу заходів, які гарантують екологічну безпеку ядерних об'єктів і надійний радіаційний захист населення та довкілля, зведення до мінімуму впливу наслідків аварії на Чорнобильській АЕС;

– впровадження у виробництво сучасних, екологічно безпечних, ресурсо- та енергозберігаючих технологій, підвищення ефективності використання природних ресурсів, розвиток технологій переробки та утилізації відходів;

– поліпшення екологічного стану річок України, насамперед басейну р. Дніпро, та якості питної води;

– запобігання забрудненню Чорного та Азовського морів та поліпшення їх екологічного стану;

– стабілізація та поліпшення екологічного стану в містах і промислових центрах Донецько-Придніпровського регіону;

– недопущення неконтрольованого ввезення в Україну екологічно небезпечних технологій, речовин і матеріалів, збудників хвороб, небезпечних для людей, тварин, рослин, організмів;

– реалізація заходів щодо зменшення негативного впливу глобальних екологічних проблем на стан екологічної безпеки України, розширення її участі в міжнародному співробітництві з цих питань.

У соціальній та гуманітарній сферах:

– істотне посилення соціальної складової економічної політики, реальне підвищення життєвого рівня населення, передусім на основі збільшення вартості оплати праці, своєчасної виплати заробітної плати та гарантованих законом соціальних виплат, посилення цільової спрямованості матеріальної підтримки, зниження рівня безробіття;

– створення умов для подолання бідності і надмірного майнового розшарування в суспільстві;

– збереження та зміцнення демографічного і трудо-ресурсного потенціалу країни; подолання кризових демографічних процесів;

– створення ефективної системи соціального захисту людини, охорони та відновлення її фізичного та духовного здоров'я, ліквідації алкоголізму, наркоманії, інших негативних явищ;

– ліквідація бездоглядності, безпритульності та бродяжництва серед дітей і підлітків.

1.3. Місце і роль інформаційної безпеки в системі національної безпеки держави

1.3.1. Інформаційна безпека як складова національної безпеки держави

У законі України “Про основи національної безпеки України” [1], як показано на рис. 1.1, окремою сферою визначена інформаційна. Цим же законом визначені такі основні напрями державної політики з питань національної безпеки України в *інформаційній сфері*:

– забезпечення інформаційного суверенітету України;

– вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну;

– активне залучення засобів масової інформації до боротьби з корупцією, зловживаннями службовим становищем, іншими явищами, які загрожують національній безпеці України;

– забезпечення неухильного дотримання конституційного права громадян на свободу слова, доступу до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів

масової інформації, дискримінації в інформаційній сфері й переслідування журналістів за політичні позиції;

– вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України.

За роки незалежності в Україні створено основні елементи системи забезпечення інформаційної безпеки, напрацьовано нормативно-правову базу їх діяльності, визначено основні функції й повноваження державних органів в інформаційній сфері.

Розглянемо основні *елементи системи забезпечення інформаційної безпеки України*, їх функції та повноваження, схему взаємодії, а також чинники, що знижують ефективність діяльності органів державної влади щодо забезпечення інформаційної безпеки України.

Правові засади побудови, поточної діяльності та розвитку системи забезпечення інформаційної безпеки України складають: Конституція України, Закон України "Про основи національної безпеки України", інші законодавчі та нормативні акти, що регулюють відносини в інформаційній сфері. Створене правове підґрунтя має досить розвинутий характер: більшість правових норм відповідають міжнародним стандартам, принципам і нормам забезпечення прав громадян на свободу слова, отримання та поширення інформації. Водночас чинна нормативно-правова база в інформаційній сфері потребує вдосконалення з метою усунення суперечностей і заповнення прогалин у законодавстві [3].

Основні функції системи забезпечення інформаційної безпеки України:

– створення та забезпечення діяльності державних органів – елементів системи забезпечення інформаційної безпеки, що включає:

створення правових засад для побудови, розвитку та функціонування системи;

формування організаційної структури системи та її окремих елементів, визначення та раціональний розподіл їх функцій;

комплексне забезпечення діяльності елементів системи: кадрове, фінансове, матеріальне, технічне, інформаційне та інші;

підготовку елементів системи до виконання покладених на них функцій згідно з призначенням;

– управління діяльністю системи забезпечення інформаційної

безпеки, що включає:

вироблення стратегії і планування конкретних заходів щодо забезпечення інформаційної безпеки;

організацію і безпосереднє керівництво системою та її структурними елементами;

оцінку результативності дій, витрат на проведення заходів щодо забезпечення інформаційної безпеки та їх наслідків;

– здійснення планової та оперативної діяльності щодо забезпечення інформаційної безпеки, що включає:

визначення національних інтересів та їх пріоритетів в інформаційній сфері;

прогнозування, виявлення та оцінку можливих загроз, дестабілізуючих чинників та конфліктів в інформаційній сфері, причин їх виникнення, а також наслідків їх прояву;

запобігання та усунення впливу загроз та дестабілізуючих чинників на національні інтереси в інформаційній сфері;

локалізацію, деескалацію та розв'язання інформаційних конфліктів;

ліквідацію наслідків інформаційних конфліктів або впливу дестабілізуючих чинників;

– міжнародне співробітництво в сфері інформаційної безпеки, що включає:

розроблення нормативно-правової бази, що регулює інформаційні відносини між державами та їх взаємодію в галузі інформаційної безпеки;

входження в існуючі та утворення нових двосторонніх і багатосторонніх структур (організацій), діяльність яких спрямована на спільне вирішення проблем інформаційної безпеки;

участь у роботі керівних, виконавчих та забезпечувальних підрозділів цих структур (організацій), спільне проведення планових та оперативних заходів.

Виконання повного переліку цих функцій є необхідною умовою ефективного функціонування системи забезпечення інформаційної безпеки України.

Аналіз чинних нормативно-правових актів дає можливість сформулювати повноваження та функції суб'єктів інформаційної безпеки наступним чином [3].

Громадяни України – на виборах, референдумах, через інші форми безпосередньої демократії, а також через органи державної влади та місцевого самоврядування висловлюють і реалізують своє бачення національних інтересів України в інформаційній сфері, засобів їх захисту; привертають увагу суспільних і державних інститутів до небезпечних явиш і процесів в інформаційній сфері; захищають власні права та інтереси в інформаційній сфері всіма законними способами та засобами.

Верховна Рада України здійснює законодавче регулювання і контроль за діяльністю органів державної влади та посадових осіб щодо виконання ними функцій і завдань у сфері інформаційної безпеки; ухвалює засади внутрішньої і зовнішньої політики держави в інформаційній сфері; затверджує державний бюджет, в якому передбачає кошти на забезпечення інформаційної безпеки України; схвалює національні програми розвитку інформаційної сфери; проводить парламентські слухання з питань забезпечення свободи слова та інформаційної безпеки України; призначає половину складу (чотири особи) Національної Ради України з питань телебачення і радіомовлення; дає згоду на призначення та звільнення з посади Президентом України голови Державного комітету телебачення і радіомовлення України.

Профільний парламентський Комітет з питань свободи слова та інформації готує законопроекти з питань інформаційної політики й безпеки. *Комітет з питань будівництва, транспорту і зв'язку* вносить законодавчі пропозиції з питань функціонування та розвитку системи зв'язку як одного з ключових елементів інформаційної інфраструктури.

Структурним підрозділом Апарату Верховної Ради є *Інформаційне управління*, у складі якого діє прес-служба Верховної Ради. Зв'язки з громадськістю спікера Парламенту забезпечує прес-секретар Голови Верховної Ради України.

Президент України, в межах своїх повноважень, здійснює керівництво в сфері інформаційної безпеки; створює, реорганізує та ліквідує органи виконавчої влади, визначає їх функції та основні завдання; видає укази і розпорядження, що стосуються функціонування та розвитку інформаційної сфери; звертається з щорічними (позачерговими) посланнями до Верховної Ради про

внутрішнє і зовнішнє становище України, в т.ч. в інформаційній сфері; призначає (за поданням Прем'єр-міністра) та звільняє з посад керівників міністерств, державних комітетів, інших центральних органів виконавчої влади, що здійснюють повноваження в інформаційній сфері: міністра освіти і науки України, голів Державного комітету інформаційної політики, телебачення і радіомовлення, Державного комітету зв'язку та інформатизації. Державного комітету архівів, Державного патентного відомства, Державного комітету статистики; президентів Національної телекомпанії України, Національної радіокомпанії України; призначає (за поданням голови Служби безпеки України) та звільняє з посади керівника Департаменту спеціальних телекомунікаційних систем та захисту інформації; призначає половину складу (чотири особи) Національної Ради України з питань телебачення і радіомовлення.

Секретаріату Президента України підпорядкований *Національний інститут стратегічних досліджень*, який є базовою науково-дослідною установою аналітично-прогнозного супроводу діяльності Президента України. На Інститут покладене завдання координації наукових досліджень з питань інформаційної безпеки.

Інформування про діяльність глави держави здійснюють прес-секретар Президента України та Управління прес-служби Секретаріату Президента України**.**

Рада національної безпеки і оборони (РНБО) України, яку очолює глава держави, координує та контролює діяльність органів виконавчої влади в сфері інформаційної безпеки. На РНБО України покладено виконання наступних функцій: внесення пропозицій Президентові України щодо реалізації засад внутрішньої і зовнішньої політики в сфері національної безпеки і оборони; координація та здійснення контролю за діяльністю органів виконавчої влади у сфері національної безпеки і оборони в мирний час; координація та здійснення контролю за діяльністю органів виконавчої влади в сфері національної безпеки і оборони в умовах воєнного або надзвичайного стану та при виникненні кризових ситуацій, що загрожують національній безпеці України. Очевидно, що ці функції розповсюджуються і на сферу інформаційної безпеки. Відповідно до вказаних функцій, РНБО України подає главі держави пропозиції

щодо: визначення стратегічних національних інтересів України в інформаційній сфері, концептуальних підходів та напрямів забезпечення інформаційної безпеки; утворення, реорганізації та ліквідації органів виконавчої влади в інформаційній сфері; проекту державного бюджету за статтями, пов'язаними із забезпеченням інформаційної безпеки; заходів інформаційного та іншого характеру відповідно до масштабу потенційних та реальних загроз національним інтересам України.

Апарат Ради національної безпеки і оборони України здійснює поточне інформаційно-аналітичне та організаційне забезпечення діяльності Ради національної безпеки і оборони України. Апарат підпорядковується *Секретареві РНБО України*, до повноважень якого, крім іншого, віднесено підготовку пропозицій щодо перспективного й поточного планування діяльності РНБО України.

Кабінет Міністрів України забезпечує державний суверенітет, здійснення внутрішньої та зовнішньої політики, виконання Конституції і законів України, актів Президента України в інформаційній сфері; вживає заходів щодо забезпечення прав і свобод громадян, забезпечення інформаційної безпеки України, боротьби зі злочинністю в інформаційній сфері; під час формування проекту бюджету передбачає виділення необхідних коштів для виконання загальнодержавних програм, спрямованих на забезпечення інформаційної безпеки України.

Урядова комісія з питань інформаційно-аналітичного забезпечення діяльності органів виконавчої влади розробляє пропозиції щодо реформування системи інформаційно-аналітичного забезпечення діяльності органів виконавчої влади.

У складі Секретаріату Кабінету Міністрів України діє *Управління інформаційних технологій.* Інформування про діяльність Прем'єр-міністра України здійснює його прес-секретар – керівник прес-служби.

Міністерства, інші центральні органи виконавчої влади, в межах своїх повноважень, наявних засобів бюджетного і позабюджетного фінансування, забезпечують виконання законів, указів Президента України, постанов Кабінету Міністрів України, інших органів виконавчої влади в інформаційній сфері. У кожному з цих органів діють інформаційно-аналітичні підрозділи та прес-служби.

Міністерство освіти і науки України є головним органом у системі центральних органів виконавчої влади із забезпечення реалізації державної політики в сфері освіти, наукової, науково-технічної, інноваційної діяльності та інтелектуальної власності; сприяє функціонуванню національної системи науково-технічної інформації; видає охоронні документи на об'єкти інтелектуальної власності, забезпечує державну реєстрацію авторського права: координує діяльність щодо трансферу технологій та прав на об'єкти інтелектуальної власності. створені повністю або частково за рахунок коштів державного бюджету.

Державний комітет інформаційної політики, телебачення і радіомовлення України вносить пропозиції щодо формування державної політики в інформаційній та видавничих сферах, забезпечує її реалізацію, здійснює управління в цих сферах, міжгалузеву координацію та функціональне управління з питань, віднесених до його відання; здійснює координацію діяльності державних засобів масової інформації, в т.ч. Національної телекомпанії України, Національної радіокомпанії України, Державної телерадіокомпанії "Крим", обласних і регіональних телерадіокомпаній, видавництв; проводить аналіз і прогнозування тенденцій розвитку інформаційного простору України, здійснює заходи щодо його захисту.

Державний комітет зв'язку та інформатизації України забезпечує проведення державної політики в галузі зв'язку, розподілу й використання радіочастотного ресурсу та в сфері інформатизації, несе відповідальність за їх стан і розвиток; розробляє та здійснює заходи щодо розвитку й удосконалення національної системи зв'язку; формує Національну програму інформатизації та забезпечує її виконання.

Державний комітет архівів України вносить пропозиції щодо формування державної політики в сфері архівної справи і діловодства та забезпечує її реалізацію, здійснює управління в цій сфері, а також міжгалузеву координацію та функціональне регулювання з питань, віднесених до його відання; несе відповідальність за стан в архівній справі і подальший її розвиток.

Департамент спеціальних телекомунікаційних систем та захисту інформації, який діє в складі Служби безпеки України, є

органом державного управління в галузі забезпечення захисту державних інформаційних ресурсів у мережах передачі даних, реалізує державну політику в сфері криптографічного та технічного захисту інформації.

Національна Рада України з питань телебачення і радіомовлення вирішує питання: забезпечення свободи слова та масової інформації; прав телеглядачів і радіослухачів, виробників і розповсюджувачів масової звукової, візуальної та аудіовізуальної інформації; розроблення і здійснення державної політики ліцензування телерадіомовлення; використання радіочастотного ресурсу держави; реалізації та контролю за додержанням законодавства України в сфері телебачення і радіомовлення.

Конституційний Суд України вирішує питання про відповідність законів та інших правових актів в інформаційній сфері Конституції України, дає офіційне тлумачення Конституції та законів України з відповідних питань.

Суди загальної юрисдикції здійснюють правосуддя в сфері інформаційних відносин.

Генеральна прокуратура здійснює нагляд за додержанням і застосуванням законів, що регулюють інформаційні відносини, порушує кримінальні справи.

Рада Міністрів Автономної Республіки Крим, обласні державні адміністрації, Київська та Севастопольська міські державні адміністрації забезпечують: виконання законів, указів Президента України, постанов Кабінету Міністрів України, інших органів виконавчої влади; додержання законних прав і свобод громадян: виконання державних і регіональних програм в інформаційній сфері; реалізацію інших, наданих державою або делегованих відповідними радами, повноважень. У державних адміністраціях діють інформаційно-аналітичні підрозділи та прес-служби.

Органи місцевого самоврядування затверджують регіональні та місцеві програми розвитку інформаційної сфери, бюджети відповідних адміністративно-територіальних одиниць (в яких передбачають кошти на виконання завдань в інформаційній сфері); виконують інші, передбачені законодавством повноваження.

Інші державні органи та організації – Державний комітет статистики України, Державне патентне відомство України,

Українське державне підприємство поштового зв'язку "Укрпошта", Концерн радіомовлення, радіозв'язку і телебачення, ВАТ "Укртелеком" та інші – діють в інформаційній сфері в межах визначених функцій та повноважень.

Засоби масової інформації є важливим елементом системи забезпечення інформаційної безпеки України. ЗМІ інформують громадськість про події в Україні й світі, в т.ч. про діяльність органів державної влади; впливають на формування громадської думки; створюють своєрідні зворотні зв'язки між владою та громадськістю. Незаангажованість, активна діяльність ЗМІ є необхідною передумовою формування в Україні громадянського суспільства. ЗМІ можуть відігравати й негативну роль у системі забезпечення інформаційної безпеки, якщо їх втягують у політичну боротьбу, перетворюють із засобів масової інформації на засоби масової пропаганди. Державні засоби масової інформації, присутність яких в інформаційному просторі України є непомірно високою, мають більші можливості маніпулювати масовою свідомістю.

Політичні партії та рухи, громадські організації, професійні спілки, заклади академічної науки та освіти, неурядові дослідницькі організації, інші організації та установи виконують функції в системі забезпечення інформаційної безпеки України відповідно до мети і завдань їх діяльності.

Загалом, в Україні створена й функціонує структурно-ієрархічно повна система забезпечення інформаційної безпеки. Функції та повноваження відповідних державних органів закріплені в нормативно-правових актах різного рівня – Конституції України, законах України, указах Президента України, постановах Кабінету Міністрів України, інших, у т.ч. відомчих, нормативних актах. Водночас, розподіл функцій між окремими суб'єктами системи та схема їх взаємодії потребують удосконалення.

Отже, інформаційна безпека є однією з основних складових національної безпеки країни. Її забезпечення з використанням грамотно сформульованої національної інформаційної політики значно сприяло б досягненню успіху у виконанні завдань в політичній, воєнно-політичній, воєнній, економічній, соціальній та інших сферах державної діяльності. Зокрема, впровадження вдалої інформаційної політики може істотно впливати на зниження

напруженості та розв'язання зовнішньополітичних і воєнних конфліктів.

1.3.2. Інформаційна безпека як складова інших сфер національної безпеки держави

Слід зазначити, що *інформаційна безпека є не лише самостійною складовою національної безпеки, а й складовою інших сфер національної безпеки держави, спрямованою на забезпечення національних інтересів у цих сферах* [4]. Це обумовлюється:

– прагненням кожної держави реалізувати та захистити власні національні інтереси, що спрямовані на формування та накопичення національного інформаційного потенціалу в умовах глобалізації світових інформаційних процесів;

– необхідністю не лише розвивати й посилювати національний інформаційний потенціал, але й захищати його від широкого спектра існуючих та потенційних інформаційних загроз;

– існуванням реальної потреби в захисті всіх суб'єктів інформаційних стосунків від можливих негативних наслідків упровадження та використання інформаційних технологій;

наявною можливістю інформаційного тиску на Україну, навіть інформаційної агресії з боку розвинутих країн світу з метою одержання односторонніх переваг в політичній, економічній, військовій та інших сферах, а також інформаційного впливу на свідомість і підсвідомість індивідів, на сім'ю, суспільство й державу, що загрожує національній безпеці країни.

Такі складові інформаційного середовища України як інформаційні ресурси, інформаційна інфраструктура та інформаційні технології, які надходять до *національного інформаційного потенціалу*, сьогодні значною мірою визначають рівень і темпи соціально-економічного, науково-технічного й культурного розвитку країни. Нині "інформаційний потенціал" стає одним з найважливіших чинників забезпечення національної безпеки наряду з "економічним потенціалом", "військовим потенціалом" тощо.

У сфері політики ефективність державного управління, обґрунтованість і ефективність політичних рішень та їх реалізації в

умовах інформаційної експансії з боку інших держав обумовлюється головним чином обсягом і якістю інформації та швидкістю й якістю її аналізу, тобто рівнем інформаційного потенціалу держави. Крім того, політичний імідж країни на міжнародній арені та ефективність дипломатичних заходів значною мірою залежать від грамотності й адекватності висвітлення політичної платформи, позицій України в закордонних засобах масової інформації та від спроможності формування країною в міжнародного співтовариства об'єктивного уявлення про Україну. В останньому проявляється активний характер заходів з інформаційної безпеки. Перевага в рівні інформаційного потенціалу на сучасному етапі еквівалентна захопленню ініціативи в зовнішній політиці.

В економічній та виробничій сферах рівень інформаційного потенціалу має вирішальне значення для розвитку нових технологій, поліпшення культури виробництва, розроблення ефективних процедур маркетингу, розв'язання завдань прогнозування й керування виробництвом, економікою та фінансами, підвищення ефективності зовнішньої торгівлі та освоєння нових ринків. Характерним для сьогодення є те, що окремі компоненти інформаційного потенціалу все більше набувають рис товару, простежується навальне зростання інформаційного виробництва, інформаційних технологій, ринку інформаційних продуктів і послуг.

У сфері соціальних стосунків рівень інформаційного потенціалу разом з розвиненими інформаційними стосунками уможливлює досягнення соціального компромісу і тим самим – підтримання стабільності суспільства і держави. Говорячи про компроміс, маємо на увазі баланс інтересів усіх суб'єктів соціальних стосунків.

В екологічній сфері спроможність визначати екологічні проблеми, прогнозувати їх розвиток і керувати ресурсами з метою усунення цих проблем пов'язана, насамперед, з наявністю і відповідним рівнем інформаційного потенціалу, з необхідністю розв'язання інформаційних завдань, включаючи екологічний моніторинг і моделювання процесів, що відбуваються в навколишньому середовищі.

Стосовно науково-технологічної сфери доречним буде вислів В.І.Вернадського: "Той народ, який зуміє найповніше, найшвидше, найдосконаліше опанувати новим, що відкривається в людському

житті, знанням, досконало розвинути і використати його у своєму житті, одержить ту могутність, досягнення якої на загальне благо є основним завданням усякої розумної державної політики". А ефективність наукових досліджень та уречевлення їх результатів у всіх сферах життєдіяльності суспільства і країни перебуває в прямій залежності від стану національного інформаційного потенціалу.

Отже, рівень розвитку та безпека інформаційного середовища, які є найвагомішими факторами у всіх сферах національної безпеки, активно впливають на стан політичної, економічної та інших складових національної безпеки України. У зв'язку з цим *доцільно розглядати інформаційну безпеку як складову інших сфер національної безпеки.*

Не дивно, що в системі національної безпеки розвинених країн передбачено реалізацію національних стратегій (програм) національної безпеки, до яких входять політичні, воєнні, економічні, соціальні й інші стратегії. Особлива роль при цьому відводиться *інформаційним стратегіям*, основне призначення яких полягає в забезпеченні реалізації решти стратегій. *Інформаційні стратегії набувають вирішального значення в разі реалізації політичних стратегій співдружності і своєрідної "зброї" – стратегій суперництва.*

Висновки

Інформаційна безпека є не лише самостійною складовою національної безпеки, а й складовою інших сфер національної безпеки держави, спрямованою на забезпечення національних інтересів у цих сферах.

Такі складові інформаційного середовища України, як інформаційні ресурси, інформаційна інфраструктура та інформаційні технології, які в сукупності можна визначити як національний інформаційний потенціал, нині в значній мірі визначають рівень і темпи соціально-економічного, науково-технічного і культурного розвитку країни. В наш час "інформаційний потенціал" стає однією з найважливіших складових компонент потенціалу держави серед

таких традиційних, як “економічний потенціал”, “військовий потенціал”, “інтелектуальний потенціал”.

В сфері політики ефективність державного управління, обґрунтованість і ефективність прийнятих рішень визначається головним чином обсягом і швидкістю опрацювання інформації в процесі вироблення управляючих дій, тобто рівнем інформаційного потенціалу держави. Перевага в рівні інформаційного потенціалу еквівалентна захопленню ініціативи в зовнішній політиці.

В економічній сфері рівень інформаційного потенціалу має вирішальне значення для розвитку нових технологій, покращання культури виробництва, розроблення ефективних процедур маркетингу, вирішення завдань прогнозування і управління економікою і фінансами, підвищення ефективності зовнішньої торгівлі і освоєння нових ринків. Характерним для сьогодення є те, що окремі компоненти інформаційного потенціалу все більше набувають рис товару, спостерігається навальне зростання інформаційного виробництва, інформаційних технологій, ринку інформаційних продуктів і послуг.

В екологічній сфері спроможність визначати екологічні проблеми, прогнозувати їх розвиток і керувати ресурсами, направленими на їх усунення, пов’язана, в першу чергу, з наявністю і відповідним рівнем інформаційного потенціалу, з необхідністю вирішення інформаційних завдань, включаючи екологічний моніторинг.

В сфері обороноздатності країни рівень інформаційного потенціалу все в більшій мірі визначає оперативність прийняття рішень, структуру і якість озброєнь, оцінку рівня їх необхідної достатності, дієвість пропаганди, ефективність дій союзників і власних збройних сил і, в кінцевому підсумку, результат збройного протистояння.

В сфері соціальних стосунків рівень інформаційного потенціалу разом з розвиненими інформаційними відносинами дає можливість досягнення соціального компромісу і тим самим – підтримання стабільності суспільства і держави. При цьому, говорячи про компроміс, маємо на увазі баланс інтересів всіх суб’єктів соціальних стосунків.

Отже, рівень розвитку та безпека інформаційного середовища, які є системоутворюючим фактором в усіх сферах національної безпеки, активно впливають на стан політичної, економічної, оборонної та

інших складових національної безпеки України. В той самий час забезпечення інформаційної безпеки являє собою важливу самостійну сферу національної безпеки.

По-перше, це пов'язано з прагненням кожної держави реалізувати та захистити власні національні інтереси, що направлені на формування та накопичення національного інформаційного потенціалу в умовах глобалізації світових інформаційних процесів.

По-друге, національний інформаційний потенціал необхідно не тільки розвивати та посилювати, але й захищати від широкого спектру існуючих та потенційних інформаційних загроз.

По-третє, існує реальна потреба захисту всіх суб'єктів інформаційних стосунків від можливих негативних наслідків впровадження та використання інформаційних технологій.

І на врешті-решт, це зумовлено наявною можливістю інформаційного тиску на Україну, навіть інформаційної агресії з боку розвинутих країн світу з метою одержання односторонніх переваг в політичній, економічній, військовій та інших сферах, інформаційного впливу на свідомість і підсвідомість індивідів, сім'ю, суспільство, державу, що загрожує національній безпеці країни.

Тому стійкий, прогресивний розвиток України як суверенної, демократичної, правової і економічно стабільної держави можливий тільки за умови забезпечення інформаційної безпеки всіх суб'єктів інформаційних стосунків країни.

Глосарій до розділу

Воєнна безпека (безпека у воєнній сфері та сфері безпеки державного кордону України) – стан воєнної організації держави, який надає змогу: стримувати і послідовно знижувати рівень воєнної загрози з боку ймовірного агресора; успішно відбити агресію в разі виникнення воєнного конфлікту; виключити або максимально обмежити деструктивні прояви воєнної сили в середині держави.

Державна безпека – захищеність конституційного ладу, суверенітету і територіальної цілісності держави від зовнішніх і внутрішніх загроз.

Економічна безпека (безпека в економічній сфері) – захищеність економіки країни від зовнішніх і внутрішніх загроз, при якій забезпечується можливість і здатність створити достойні соціально-економічні умови стабільного функціонування і розвитку особистості, суспільства і держави.

Загрози національній безпеці – наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України.

Інформаційна безпека – сукупність чинників, умов і факторів, що визначають стан захищеності інформаційного середовища особистості, суспільства та держави від навмисних і ненавмисних загроз і впливів.

Національна безпека – 1) захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам; 2) сукупність зв'язків і відношень, які характеризують такий стан особистості, соціальної групи, суспільства, держави, народу, при якому забезпечуються їх тривале, стабільне існування, задоволення і реалізація життєвих потреб, спроможність до ефективного відбиття внутрішніх і зовнішніх загроз, саморозвитку і прогресу.

Національні інтереси – життєво важливі матеріальні, інтелектуальні і духовні цінності Українського народу як носія суверенітету і єдиного джерела влади в Україні, визначальні потреби суспільства і держави, реалізація яких гарантує державний суверенітет України та її прогресивний розвиток.

Об'єкти національної безпеки:

– людина і громадянин - їхні конституційні права і свободи;

– суспільство – його духовні, морально-етичні, культурні, історичні, інтелектуальні та матеріальні цінності, інформаційне і навколишнє природне середовище і природні ресурси;

– держава – її конституційний лад, суверенітет, територіальна цілісність і недоторканність.

Політична безпека (безпека у зовнішньополітичній та внутрішньополітичній сферах) – захищеність політичної системи

суспільства від зовнішніх і внутрішніх загроз. Передбачає забезпечення стійкого політичного суверенітету в рамках системи міжнародних відносин, можливості нації і створюваних нею державних структур самостійно вирішувати питання державного устрою і незалежно проводити внутрішню і зовнішню політику, а також політичної стабільності, що базується на балансі інтересів особистості, суспільства, держави.

Соціальна безпека – стан державного і суспільного захисту, за якого сукупність державних гарантій забезпечує конституційні права й свободи людини, духовні та матеріальні цінності *суспільства*.

Технологічна безпека (безпека у соціальній та гуманітарній сферах) – захищеність науково-технічного і технологічного потенціалу від вразливості, застою, руйнування, деградації з метою забезпечення підвищення конкурентоспроможності вітчизняної наукоємкої продукції. Рівень технологічної безпеки визначається станом нормативно-правових актів та науково-виробничого потенціалу, який дає змогу: самостійно розробляти і впроваджувати науково-технологічні досягнення; виключити передумови завдання фізичної шкоди й матеріальних збитків населенню через технологічну недосконалість небезпечних виробництв.

Зв'язок ключових термінів і понять

Рис.1.2.

Завдання і запитання для самоперевірки

1. Дайте визначення і назвіть сфери національної безпеки держави.
2. Як співвідносяться поняття «національна безпека» і «національні інтереси»?
3. Сформулюйте основні принципи забезпечення національної безпеки.
4. Сформулюйте основні пріоритети національних інтересів України.
5. Сформулюйте основні напрями державної політики з питань національної безпеки України в інформаційній сфері
6. Дайте загальну характеристику основних функцій системи забезпечення інформаційної безпеки України.
7. Назвіть суб'єктів системи забезпечення інформаційної безпеки та дайте характеристику їхнім повноваженням.
8. Обґрунтуйте положення, що інформаційна безпека є складовою інших сфер національної безпеки держави.

Рекомендована література до розділу

1. Закон України "Про основи національної безпеки України" (19 червня 2003 року, № 964-IV, Орієнтир, 30 липня 2003 року, №139, с.1–6)
2. *Брыжко В.М., Цимбалюк В.С., Орехов А.А., Гальченко О.Н.* Е-будущее и информационное право. –К.: Интеграл, 2002.
3. Информационные вызовы национальной и международной безопасности / Под общей редакцией А.В. Федорова и В.Н. Цыгичко. – М.: ПИР_Центр, 2001.
4. Інформаційна безпека держави у контексті протидії інформаційним війнам: Навчальний посібник /О.В. Варюхін, Я.М. Жарков, І.В. Замаруєва та ін.; За ред. В.Б.Толубка. – К.: МОУ НАОУ, 2004.
5. *Лопатин В.Н.* Информационная безопасность России: Человек. Общество. Государство. – Санкт-Петербург: Фонд "Университет", 2000.

6. Національна безпека України, 1994–1996 рр.: Наук. доп. НІСД / Редкол.: О.Ф. Бєлов (голова) та ін. – К.: НІСД, 1997.
7. Актуальні проблеми інформаційної безпеки України // Національна безпека і оборона. – 2001. – №1.

Використані джерела

1. Закон України “Про основи національної безпеки України” (19 червня 2003 року, № 964-IV, Орієнтир, 30 липня 2003 року, №139, с.1–6)
2. *Манилов В.Л.* Национальная безопасность: ценности, интересы и цели // Военная мысль. – 1995. – № 6.
3. Актуальні проблеми інформаційної безпеки України // Національна безпека і оборона. – 2001. – №1.
4. Інформаційна безпека держави у контексті протидії інформаційним війнам: Навчальний посібник /О.В. Варюхін, Я.М. Жарков, І.В. Замаруєва та ін.; За ред. В.Б.Толубка. – К.: МОУ НАОУ, 2004.

Розділ 2.
ІНФОРМАЦІЙНІ ВІЙНИ ЯК ДЖЕРЕЛО ЗАГРОЗ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ ДЕРЖАВИ

2.1. Сутність поняття “інформаційна війна”

Стосовно правомірності існування терміну “інформаційна війна” існують різні погляди, у тому числі й протилежні. Узагальнене визначення війни, яке відповідає сучасним поглядам, таке: війна – це складне соціально-політичне явище, що охоплює всі сфери життя держави і визначається внутрішньою та зовнішньою політикою, які перебувають у тісній взаємодії та формуються на загальній суспільно-економічній базі; війна являє одну з форм розв’язання суспільно-політичних, ідеологічних, а також національних, територіальних, релігійних та інших суперечностей між державами, народами, націями, класами й соціальними групами шляхом збройного насильства. Разом з цим, небезпідставно зазначається, що у пресі, зокрема військовій, широко застосовуються такі поняття і вирази: холодна, дипломатична, економічна, технічна, комп’ютерна, інформаційна, торговельна, психологічна війна. Очевидно, у повному розумінні слова їх не можна ототожнювати з власне війною у традиційному сенсі цього поняття. Однак за своїми змістом і суттю ці явища дійсно є активними й цілеспрямованими формами протиборства у стосунках між окремими державами, коаліціями чи союзами кількох країн, які всебічно підготовлені, здійснюються за узгодженим та раніше розробленим планом із застосуванням високоефективних технічних, дипломатичних економічних та інших засобів.

Подальше широкомасштабне використання зброї проти армій і народів в сучасних війнах призведе до глобальної катастрофи і загибелі життєвого середовища. Є серйозні підстави стверджувати, що світ вступає в період війн нового покоління, спрямованих не стільки на безпосереднє знищення противника, скільки на досягнення політичних та економічних цілей без битв між масовими арміями. Про те, що наступає епоха “цивілізованих” війн, в яких політичні й економічні цілі досягаються не прямим збройним

втручанням, а використанням нових форм насилля та підриву могутності противника зсередини, свідчить "холодна війна", під час якої воєнна сфера була гострою ділянкою протиборства, але боротьба велась не у вигляді збройних зіткнень, а "небольовим" впливом на збройні сили, підривом зсередини воєнної могутності й воєнної організації СРСР. "Холодна війна" наочно продемонструвала можливості незбройних методів досягнення мети протидіючими сторонами, зокрема, з забезпечення бажаних цілей на інформаційному рівні. Разом з тим, вона підпадає під загальноприйняте визначення війни, оскільки справді була складним соціально-політичним явищем, продовженням політики насильницькими засобами, вона порушувала всі сфери життя й діяльності суспільства і до неї були залучені різною мірою практично всі верстви населення країни. Взагалі багато фахівців схильні розглядати "холодну війну" за її основними ознаками та результатами як третю світову війну. Її кінцевими результатами стали розвал світової системи соціалізму та розпад Організації Варшавського договору як одного зі світових центрів сили [1]. Відбулися великомасштабні геополітичні зрушення, перегрупування сил, коаліцій і союзів, зміна політичних режимів, з'явилося близько 30 нових країн. За наслідками зміни світопорядку ця війна, як вважає ряд зарубіжних фахівців, не лише порівнянна з двома попередніми війнами, але й перевершує їх [2]. Явище "холодної війни" має бути об'єктом майбутніх глибоких досліджень в усіх аспектах, в тому числі й у безпосередньо воєнному.

Як відомо, специфічний зміст війни становить збройна боротьба. Поряд зі збройною боротьбою для досягнення поставлених політичних цілей у війні застосовуються також економічні, дипломатичні, ідеологічні й інші методи та відповідні їм засоби боротьби. Збройна боротьба – основна форма боротьби у війні. Це стосується воєн у традиційному розумінні, в яких домінуючими є методи і прийоми збройної боротьби.

Сучасна епоха побудови інформаційного суспільства, тобто суспільства, в якому за рахунок розвитку продуктивних сил більшість працездатного населення (на відміну від аграрного чи індустріального суспільства) залучена до інформаційної сфери, сприяє розвитку нових форм і методів досягнення країнами політичних, економічних та

інших цілей на інформаційному рівні. Як наслідок, з'явилося поняття "інформаційної війни", яке на відміну від поняття "холодної війни" зафіксоване в ряді таких офіційних документів США, як "Стратегія національної безпеки США" (1994 і 1996 роки) [3,4] , "Національна воєнна стратегія Сполучених Штатів Америки" (1995 рік) [5], "Стратегія національної безпеки США для нового сторіччя"[6], в яких так чи інакше способи й методи інформаційної війни розглядаються як одні з найефективніших засобів забезпечення національних інтересів США в різних регіонах світу, з одного боку, і як джерело загроз власним національним інтересам, з іншого боку.

Сутності і ролі інформаційної війни присвячена досить велика кількість публікацій, у яких вона трактується по-різному. Проаналізуємо визначення інформаційної війни, що містяться в роботах зарубіжних фахівців і в офіційних документах. Їх можна згрупувати так: визначення інформаційної війни у вузькому розумінні, тобто такі, які відбивають суто воєнну спрямованість, і визначення в широкому розумінні, які відбивають спрямованість на забезпечення національних інтересів у будь-якій життєво важливій сфері державної і суспільної діяльності.

У ряді публікацій стверджується, що термін "інформаційна війна" у вузькому розумінні своїм походженням зобов'язаний військовим [7]. Військові експерти, які сформулювали доктрину інформаційної війни, чітко уявляють собі окремі її грані: це штабна війна, електронна війна, психологічні операції і т.д. У цьому контексті показовим є визначення, що вийшло зі стін кабінету директора інформаційних військ міністерства оборони США: "Інформаційна війна являє собою всеосяжну, цілісну стратегію, покликану віддати належне значущості і цінності інформації в питаннях командування, управління та виконання наказів збройними силами й реалізації національної політики. Інформаційна війна націлена на всі можливості і чинники уразливості, що неминуче виникають при зростаючій залежності від інформації, а також на використання інформації у всіляких конфліктах... Інформаційна війна має наступальні й оборонні складові, але починається з цільового проектування та розроблення своєї "архітектури командування, управління, комунікацій, комп'ютерів і розвідки, що забезпечує особам, приймаючим рішення, відчутну інформаційну перевагу у

всіляких конфліктах" [7]. В директиві МО DODD 3600.1 та меморандумі управління голови Об'єднаного штабу комітету начальників штабів (ОШ КНШ) від 1993 року, в яких зафіксовані загальні положення про інформаційну війну, значну увагу приділено також протидії системам управління військами [8].

Слід зазначити, що в досить чисельній кількості публікацій акцент робиться саме на тому, що поява терміну "інформаційна війна" зумовлене стрімким розвитком інформаційних технологій, індустрії інформаційних ресурсів і засобів інформаційного впливу та їх можливостей у разі їх використання як інформаційної зброї для досягнення країнами політичних, економічних та інших цілей шляхом здобуття необхідної переваги на інформаційному рівні, а також на тому, що вона є війною переважно в "кіберпросторі" і має суто технічний характер. Сьогодні поширюються спроби розкласти інформаційну війну на цілком незалежні складові [8]. Одні зводять її до проблем комп'ютерних технологій, тобто до реалізації можливостей технологічних засобів передавання, опрацювання та використання інформації, інші – до психологічної війни, тобто до використання засобів впливу на людину. Операція "Буря в пустелі" наочно продемонструвала, що комплексне та узгоджене використання різнопланових методів інформаційного впливу істотно впливає на ведення безпосередньо воєнних операцій. У цій операції були застосовані майже всі методи й засоби інформаційного впливу: логічні бомби (руйнування інфосфери машинно-технічних систем), дезінформування (введення в оману військового керівництва іракської армії), пропаганда (психологічна підготовка військ об'єднаних сил), інформаційний вплив на формування думки світової громадськості (виставляння Іраку в очах світової громадськості агресором).

На користь комплексного погляду на війну ряд фахівців вважає, що війна в телекомунікаційних мережах належить до поняття інформаційного конфлікту високого рівня між окремими націями або суспільствами [9]. Її мета – зруйнувати або модифікувати в свідомості протилежної нації своє власне розуміння ролі і місця у світових процесах або ж зруйнувати чи змінити уявлення про неї всього навколишнього світу. Основний удар під час ведення такої війни концентрується або на широких прошарках населення, або

спрямований лише проти політико-економічної еліти. Вона може використовувати дипломатичні засоби, пропагандистські й психологічні кампанії, політичну або підривну культурну діяльність, обман чи втручання в діяльність місцевих засобів масової інформації, проникнення в комп'ютерні мережі та бази даних і т.д. Іншими словами, війна в телекомунікаційних мережах являє собою щось нове в усьому спектрі можливих конфліктів, об'єднуючи економічну, політичну і соціальну форми ведення війни. Звичайно, що вона не обмежується рамками лише телекомунікаційних мереж. "Ми наближаємося до такого ступеня розвитку, коли вже ніхто не є солдатом, але всі є учасниками бойових дій, – сказав один з керівників Пентагону. – Завдання тепер полягає не в знищенні живої сили, а в підриві мети, поглядів і світогляду населення, в руйнуванні соціуму" [7]. Зазначимо, що великомасштабне інформаційне протистояння між суспільними групами або державами має за мету змінити розстановку сил в суспільстві. В цьому полягає *сутність інформаційної війни в широкому розумінні.*

З наведеного аналізу випливає, що інформаційна війна в широкому розумінні не є алегоричним образом, вона являє собою суспільно-політичне явище і повністю підпадає під наведене вище визначення війни. На неї повною мірою поширюються всі загальні закони війни. Інформаційна війна має наступальні й оборонні компоненти, може вестись в конфліктах низької інтенсивності і в конфліктах з застосуванням засобів масового ураження, на тактичному, оперативному й стратегічному рівнях. Інформаційна війна характеризується низкою притаманних їй особливостей. На відміну від традиційних воєн, вона значно ширша за своїми цілями, завданнями та сферами впливу. Крім силових структур, у цю війну втягуються політичні, фінансові, промислові та інші структури. Тенденція розширення масштабів інформаційної війни неухильно посилюється від міждержавного характеру до міжблокового.

Нині інформаційну війну розглядають як найбільш ефективний і "цивілізований" або "гуманний" шлях колоніалізації однієї країни іншою.

2.2. Чинники, які обумовлюють неминучість інформаційних воєн

Які витоки виникнення і живучості ідей інформаційної війни? Судячи по різноманітних оцінках, що фігурують в пресі, таких причин декілька [10–13].

По-перше, стаючи цілісною, світова економіка диктує і свої світові закони – все більш гуманні. Головний з них виглядає просто: війна (в традиційному розумінні) економічно не вигідна. Це один з системних чинників, що сприяють розповсюдженню і розвитку гуманістичних тенденцій.

По-друге, економічність інформаційної зброї, що дозволить, з одного боку, скорочувати певною мірою військовий бюджет, а з іншого – створювати високоефективну зброю XXI століття, застосування якої матиме багатообіцяючі результати. Крім того, першочергового розвитку отримує електронна промисловість США, яка зараз ледь витримує конкуренцію з електронними технологіями Японії і Західної Європи.

По-третє, масоване застосування інформаційної зброї, як стверджують західні експерти, дасть можливість порівняно швидко придушувати противника, паралізувати його, примушувати до капітуляції без залучення збройних сил, без звичайних битв, типових для класичних війн, без загибелі людей і руйнування громадянської інфраструктури, і, нарешті, без втрат особового складу американських ЗС, що надто болюче сприймається американським суспільством.

Співробітники Інституту комп'ютерної безпеки США, яким довірено стояти на варті цілісності, конфіденційності і доступності інформаційних систем близько 500 корпорацій, незліченної безлічі державних органів і провідних університетів, впевнені, що інформаційна війна врешті-решт націлена на економіку в світовому масштабі. А тому особливо актуальні інформаційні дії оборонного характеру в сучасній глобальній економіці [7].

Наочним прикладом реалізації таких оборонних дій, що полягають в контролі змісту інформаційних потоків, є Китай. Так, представник агентства Сіньхуа зробив заяву в зв'язку з тим, що за уповноваженням Держради КНР Сіньхуа буде здійснювати єдине

управління розповсюдженням економічної інформації на території Китаю іноземними агентствами і їхніми інформаційними установами. Таке єдине управління, зазначив представник, призначене головним чином для створення нормативів інформаційного ринку в ході формування соціалістичної ринкової економіки в Китаї, для сприяння послідовному розвитку ринку економічної інформації, створення умов рівноправної конкуренції як для китайських, так і для зарубіжних інформаційних установ. Подібні заходи вже прийняті в країнах Азії й інших країнах, що розвиваються. Так що можна назвати її узвичаєною світовою практикою [14].

Панування розвинених держав в сферах інформаційних технологій кардинально поширило можливості найбільш сильних валют шляхом монетарних важелів впливати на розвиток світової економіки. Угорський фахівець з питань світової економіки Поран Каролі вважає, що причина боргової проблеми криється в тому факті, що світовий ринок грошей єдиний, а ринки товарів, праці і капіталу ще роз'єднані. Однак ці ринки знаходяться під впливом інформаційного поля, ключові позиції в якому займають найбільш розвинені держави і потужні транснаціональні кампанії. Як свідчить світова практика, незалежно від того, чи нормально функціонують ці ринки, чи вони дестабілізовані під впливом інформаційних потоків, в кращому положенні виявляються більш інформовані і потужні в фінансовому відношенні суб'єкти, будь то держави або кампанії. Передусім, це стосується володарів твердих валют, особливо США, Німеччини і Японії. Найважливіші компоненти кредитно-грошової політики постійно знаходяться в полі зору розвинених держав, найбільших компаній і міжнародних фінансових організацій. До того ж при багатомільярдному товарообігові володіння відповідною інформацією стає просто життєво необхідним [15].

Показовою в контексті розглядуваних проблем є *стратегія національної безпеки США для нового століття* [6]. Згідно з нею стратегія зміцнення національної безпеки США виходить з того факту, що Сполучені Штати стоять перед обличчям різноманітних загроз, які потребують єдиного підходу в справі захисту країни, створення сприятливої міжнародної обстановки, реагування на кризові ситуації і підготовки до непередбачуваного майбутнього.

Військові фахівці США відіграють важливу роль в створенні коаліції і формуванні такої міжнародної обстановки, яка б захищала і просовувала вперед американські інтереси. Найбільш важливе завдання при цьому полягає в недопущенні агресії чи насильства в будь-який час. В цьому контексті великого значення набувають операції обмеженого масштабу.

Під операціями обмеженого масштабу розуміються всі можливі види операцій, які не охоплюють великі театри воєнних дій, в тому числі здійснення гуманітарної допомоги, миротворча діяльність, забезпечення режиму ембарго і контроль заборонених для польотів зон, евакуація американських громадян, зміцнення сил союзників, завдання обмежених ударів і збройне втручання. "Наші збройні сили мають готуватися не лише до успішного здійснення чисельних операцій обмеженого масштабу по всьому світу, але й до того, щоб робити це перед обличчям таких викликів, як тероризм, інформаційні атаки і використання чи загроза використання зброї масового ураження."

"В силу нашої переваги в сфері звичайних озброєнь противники, які здійснюють виклик Сполученим Штатам, можуть вдатися до таких засобів, як зброя масового ураження, інформаційні операції чи тероризм.

Ми також підвищуємо нашу здатність захищатися від інформаційних операцій, які проводяться нашими противниками і які в майбутньому можуть прийняти форму широкомасштабних стратегічних інформаційних атак на наші життєво важливі елементи інфраструктури, керівництво, економіку і збройні сили. Оскільки інші країни нарощують свої можливості по здійсненню наступальних інформаційних операцій, необхідно забезпечити захист нашої національної і оборонної інформаційної інфраструктури. Ми повинні мати можливість швидко визначити, звідки ведеться інформаційна атака, захиститися від неї і дати негайно відсіч на інформаційний напад.

Наш пріоритет полягає в формуванні такого міжнародного клімату, який би запобігав початку локальних війн на ТВД."

Значна увага в стратегії приділяється підготовці до непередбачуваного майбутнього: "Грядуще XXI століття з його

воєнними викликами і застарілість основних елементів американської силової структури потребують фундаментальних перетворювань наших збройних сил. Хоча майбутні загрози розпливчасті і непередбачувані, американським збройним силам, швидше за все, доведеться мати справу з рядом викликів і цілим спектром можливих конфліктів, в тому числі зі спробами перешкодити доступу наших військ в кризові регіони, з воєнними діями в містах, інформаційними війнами і атаками з використанням хімічної і біологічної зброї. Щоб дати достойну відсіч на ці виклики, ми маємо трансформувати наші збройні сили, використовуючи революцію у військовій справі. Покращання збору і аналізу розвідувальних відомостей, сучасні методи опрацювання інформації, нові методи навігації, управління і контролю – це ключ до того, щоб змінити наші бойові можливості."

"Нам необхідно мати все необхідне для збору і аналізу інформації, щоб попереджати про загрози національній безпеці, забезпечувати аналітичну підтримку політикам і військовим, без затримок надавати розвідувальні дані в кризових ситуаціях. Але в той самий час необхідно тримати в полі зору глобальну перспективу – відшукувати шляхи відстоювання наших національних інтересів і зберігати нашу інформаційну перевагу на міжнародній арені…

Операції в сфері збору інформації, спостереження і розвідки мають бути пов'язаними з більш широким спектром загроз і політичних обставин, ніж будь-коли раніше. В першу чергу ми віддаємо пріоритет збереженню і розширенню розвідувальних можливостей в цій сфері, завдяки яким ми отримуємо відомості про ті країни і групи осіб, які являють собою найбільш серйозну загрозу для нашої безпеки. Особлива увага буде приділятися країнам, які проводять ворожу по відношенню до США політику, країнам та іншим утворенням, які володіють стратегічними ядерними силами або мають ядерну зброю, інші види зброї масового ураження або розщеплювальні матеріали; тероризму, міжнародній злочинності і розповсюдженню наркотиків; потенційним конфліктам в регіонах, які можуть відбитися на інтересах національної безпеки США; посиленню робити з протидії активності іноземних розвідок, що зачіпає американські інтереси, в тому числі економічному і промисловому шпіонажу; загрозам інформаційної війни і загрозам американським збройним силам та громадянам, які знаходяться за кордоном. Розвідувальне

забезпечення потрібне також для вироблення і проведення політики США по сприянню демократії в інших країнах, для визначення загроз нашим інформаційним і космічним системам, стеження за виконанням домовленостей про контроль над озброєнням, підтримки дій в гуманітарній сфері і захисту навколишнього середовища…

Наші можливості в сфері розвідки і збору відомостей включають отримання новин і приймання передач електронних засобів масової інформації, повідомлень інформаторів, що безпосередньо беруть участь в тих чи інших важливих подіях за кордоном, візуальне спостереження і перехоплення сигналів за допомогою супутників і літаків, узагальнення і глибокий аналіз зібраної інформації висококласними фахівцями. Використовуючи свою величезну перевагу, що полягає в постійному і непомітному зборі різного роду відомостей космічними засобами, ми маємо можливість стежити за виконанням умов договорів, пересуванням військових частин, розробленням, випробуванням і розгортанням зброї масового ураження. Використання отриманих при цьому даних для підтримки наших дипломатичних і воєнних кроків робить внесок в забезпечення глобальної безпеки, показуючи, що Сполучені Штати можуть бути або безцінним союзником, або грізним ворогом…

Хоча наші можливості в інформаційній сфері значно зросли завдяки передовим технологіям і багато в чому залежать від них, все ж не існує заміни інформованій людині з її суб'єктивною думкою. Ми маємо продовжувати залучати висококваліфікованих фахівців, що забезпечують збір, передачу і аналіз відомостей в тих чисельних нових сферах, де зробити це за допомогою техніки просто неможливо. Зростаюче співробітництво між установами, що складають розвідувальне співтовариство, і злиття всіх напрямків інформаційної діяльності забезпечують найбільш ефективний збір і аналіз даних, які стосуються найбільш важливих з розвідувальної точки зору проблем…

Ми також маємо віддавати собі звіт, що нам, як і раніше, необхідні ефективні програми в галузі служб безпеки і контррозвідки. Щоб захистити особливо важливу інформацію, яка стосується національної безпеки, ми маємо бути здатні ефективно протидіяти іноземним технічним розвідкам за допомогою енергійних дій контррозвідки, вироблення всеосяжних програм забезпечення

безпеки і постійного стеження за намірами і об'єктами спостереження іноземних розвідувальних центрів. Контррозвідка залишається складовою частиною розвідувального суспільства, що займається збором і опрацюванням відомостей, незалежно від того, чи виходить загроза від традиційного шпіонажу, чи від крадіжки життєво важливої економічної інформації. Протидія іноземним зусиллям по збору технічної, промислової і комерційної інформації потребує тісного співробітництва між урядом і приватним бізнесом. Важливу роль тут відіграють поінформованість про загрози і прихильність додержанню визначених стандартів і правил особистої, інформаційної і фізичної безпеки, основаних на принципах управління в умовах ризику…

В цьому десятиріччі космос набув глобального інформаційного значення, що має серйозні політичні, дипломатичні, воєнні і економічні наслідки для США. Ми переживаємо зараз період все більшого проникнення в космос, оскільки світ докладає всі зусилля, щоб використати стрімке зростання інформаційних технологій. Телекомунікації, міжнародні фінансові операції, трансляція розважальних і освітніх програм та новин по всьому світу, передача повідомлень про погоду і стан навколишнього середовища – все це робить внесок в могутність нашої економіки і все це залежить від наших можливостей в космосі" [6].

2.3. Погляди зарубіжних фахівців на ведення інформаційної війни

Аналіз стану, проведений в попередніх підрозділах свідчить, що концепція тотальної війни в традиційному розумінні, яка є основою стратегічних настанов багатьох країн світу, в кінці XX століття себе зживає. Є серйозні підстави стверджувати, що світ вступає в період війн нового покоління, спрямованих не стільки на безпосереднє знищення противника, скільки на досягнення політичних та економічних цілей без битв між масовими арміями.

За висловом Клаузевіца – "будь-яка епоха має свої власні війни", сучасна епоха – не виняток. Наступає епоха "цивілізованих" війн, в яких політичні й економічні цілі досягаються не прямим збройним

втручанням, а використанням нових форм насилля та підриву могутності противника зсередини.

2.3.1. Погляди військового керівництва США на ведення інформаційної війни

Президент США Джордж Буш, виступаючи перед співробітниками Центрального розвідувального управління в штаб-квартирі ЦРУ в Ленглі, перелічив головні загрози безпеці Сполучених Штатів. На другому місці, після тероризму, у цьому переліку значиться інформаційна війна. І вже за нею – поширення зброї масового ураження і засобів її доставки [16, 17].

Як вважають американські військові фахівці, до порядку денного поставлене питання про перенесення акценту в збройному протиборстві з традиційних його форм ведення (вогонь, удар, маневр) в інформаційно-інтелектуальну й інформаційно-технічну сфери, тобто туди, де ведеться підготовка, відбувається прийняття і реалізація воєнних і політичних рішень. Навіть майбутня війна може бути спровокована в інформаційній сфері, що буде охоплювати всю сукупність завдань у політичній, економічній, технічній і військовій галузях.

Відповідно до документів ОШ КНШ ЗС США, інформаційна війна може вестися як у воєнний, так і в мирний час, як на державному (дипломатичними, економічними, інформаційними, спеціальними й іншими силами і засобами), так і на військовому рівні (силами і засобами боротьби із системами бойового управління).

Хвиля “цифрової революції” створила абсолютно новий економічний сектор, якого раніше просто не було. Це провокує зростання інтенсивності конфліктів з метою захоплення й утримання переваги в даному секторі нової світової економіки. Капіталом, що відіграє чільну роль у “цифровій революції”, є інтелектуальний капітал насамперед у галузі інформаційних технологій.

І, нарешті, основний продукт цього сектора – інформація має унікальні властивості, не притаманні іншим секторам економіки. Інформація на відміну від всіх інших ресурсів придатна для багаторазового використання і для численних користувачів, при цьому чим більше вона використовується, тим більшої вартості

набуває.

Разом з переходом від постіндустріального до інформаційного суспільства нового значення набуває і споконвічна боротьба щита і меча, броні і снаряда. Поле бою в конфліктах XXI століття – це віртуальний кіберпростір, у якому розгортаються дії інформаційних воєн. Без сумніву, процеси глобалізації накладають певний відбиток і на модернізацію основних концепцій воєнної стратегії XXI століття. Це переконливо підтверджує побудова нової національної воєнної стратегії США.

Ряд офіційних документів, таких як доповідь міністерства оборони США "Report of the quadrennial Defense Review", концептуальний документ Комітету начальників штабів "Joint Vision 2010", доповідь комісії з національної оборони "Transforming Defense National Security in the 21st Century, Report of the National Defense Panel", констатують відповідно: "Ми визнали, що світ продовжує швидко мінятися. Ми не в змозі цілком зрозуміти або прогнозувати проблеми, що можуть виникнути у світі за часовими межами, обумовленими традиційним плануванням. Наша стратегія приймає такі невизначеності і готує збройні сили таким чином, щоб справитися з ними". "Прискорення темпу змін робить майбутні умови більш непередбаченими і менш стабільними, висуваючи широкий діапазон вимог до наших сил". "Проблеми XXI століття будуть кількісно і якісно відмінні від тих, котрі були характерні для періоду холодної війни, у зв'язку з чим будуть потрібні корінні зміни інститутів національної безпеки, воєнної стратегії і підходів до питань оборони до 2020 року".

У колах деяких фахівців термін "інформаційна війна" трактується як відкритий і/чи прихований цілеспрямований інформаційний вплив систем одна на одну з метою одержання певного виграшу в матеріальній сфері. Однак інформаційна війна не є простим "впливом систем одна на одну". В основних документах збройних сил США говориться, що інформаційний вплив носить різнобічний характер і змінюється залежно від розв'язуваних завдань і обстановки. Напрямками здійснення інформаційного впливу можуть бути такі:

– інформаційно-розвідувальна діяльність (виявлення воєнного, економічного, політичного і культурного потенціалу);

– протидія будь-яким видам розвідки супротивника (OPSEC);

– спотворення, руйнація, нейтралізація, знищення чи, напроти, захист інформації (CNA, CND);

– комп'ютерне відтворення реальної чи віртуальної обстановки і візуалізації поля бою;

– здійснення інформаційно-психологічного (PSYOP) чи фізичного впливу на особовий склад, об'єкти, бойову техніку, зброю, лінії зв'язку і управління;

– концентрація на демонстративних діях, обмані і введенні в оману (Military Deception);

– радіоелектронне подавлення засобів зв'язку, комп'ютерно-телекомунікаційних мереж, радіоелектронних засобів, які випромінюють, тощо;

– зниження помітності об'єктів, бойової техніки і зброї;

– захист особового складу, об'єктів, бойової техніки, зброї, органів управління і різних радіоелектронних засобів від впливу на них електромагнітного чи інших видів спрямованої енергії;

– відведення самонавідної зброї від найбільш важливих цілей й ін. [17].

В основі такого впливу лежать, насамперед, психологічні і світоглядні фактори, а також комп'ютерні технології. Настільки ж невірно зводити його до класичної спецпропаганди – у поняття "інформаційний вплив" закладений куди більш широкий зміст.

У документах також говориться, що на державному рівні основними завданнями інформаційної війни є:

– забезпечення національної безпеки США;

– добування інформації, необхідної для прийняття військово-політичних рішень.

Так, наприкінці 1996 року на одному із симпозіумів Роберт Банкер представив доповідь, присвячену новій воєнній доктрині збройних сил США XXI сторіччя (концепції "Force XXI"). Ключовим моментом у ній є поділ усього театру воєнних дій на дві складові – традиційний простір і кіберпростір, причому останнє має більш важливе значення. Банкер запропонував доктрину "кіберманевру", що повинна з'явитися природним доповненням до існуючих воєнних концепцій, що переслідують мету нейтралізації чи придушення збройних сил супротивника (концепції "Force XXI").

Отже, у число сфер ведення бойових дій, крім землі, моря, повітря і

космосу тепер включається й інфосфера. Як підкреслюють військові експерти, основними об'єктами ураження в нових війнах будуть інформаційна інфраструктура і психологія супротивника (з'явився навіть термін "human network").

Отже, під *інформаційною війною у вузькому сенсі* (Information Warfare, IW) розуміється комплексний вплив на систему державного і воєнного управління конфронтуючої сторони, на її військово-політичне керівництво. У принципі цей вплив повинний ще в мирний час призводити до прийняття сприятливих для країни-ініціатора інформаційного тиску рішень, а в ході конфлікту цілком паралізувати функціонування інфраструктури управління супротивника.

Здатність не тільки реагувати, але і передбачати проблеми до того, як вони досягнуть кризової точки, – та здатність, яку прагнуть набути США в найближчому майбутньому. При цьому вони віддають пріоритет системам і засобам, що дозволяють різко знизити в початковій стадії конфлікту (чи до його початку) функціональні можливості протидії держави-супротивника за рахунок проведення наступальних інформаційних операцій.

Концепція інформаційної війни передбачає:

– придушення (у воєнний час) елементів інфраструктури державного й військового управління (ураження центрів управління);

– електромагнітний вплив на елементи інформаційних і телекомунікаційних систем (радіоелектронна боротьба);

– одержання розвідувальних даних у результаті перехоплення і дешифрування інформаційних потоків, переданих по каналах зв'язку і по побічних випромінюваннях, а також шляхом впровадження спеціальних технічних засобів перехоплення інформації;

– здійснення несанкціонованого доступу до інформаційних ресурсів (завдяки використанню програмно-апаратних засобів прориву систем захисту інформаційних і телекомунікаційних систем супротивника) з подальшим їх перекручуванням, знищенням чи викраданням, або порушенням нормального функціонування цих систем;

– формування і масове поширення по інформаційних каналах чи глобальних мережах протидіючої сторони дезінформації або тенденційної інформації для впливу на оцінки, наміри й орієнтацію населення та осіб, що приймають рішення;

– одержання необхідної інформації шляхом перехоплення й опрацювання відкритої інформації, переданої по незахищених каналах зв'язку, циркулюючої в інформаційних системах, а також друкованої у відкритому порядку і ЗМІ.

Як основні об'єкти впливу в інформаційній війні виступають:

– особовий склад;

– мережі зв'язку й інформаційно-обчислювальні мережі, використовувані державними організаціями при виконанні своїх управлінських функцій;

– військова інформаційна інфраструктура, що вирішує завдання управління військами;

– інформаційні і управляючі структури банків, транспортних і промислових підприємств;

– засоби масової інформації (у першу чергу – електронні).

У принципі про будь-яку систему, здатну по вхідних даних відпрацьовувати той чи інший алгоритм, можна говорити як про інформаційну систему – об'єкт інформаційної війни.

Відповідно до статутів американських ЗС на збройні сили США покладені такі завдання інформаційної війни:

– примушувати військово-політичне керівництво ворожих держав приймати рішення, що забезпечують створення вигідних для ЗС США умов;

– завоювати й утримувати "інформаційну перевагу" над супротивником;

– досягати цілей і рішення завдань кампаній і операцій;

– добувати і вчасно оновлювати інформацію для прийняття рішень.

Залежно від театру війни, оперативної обстановки і розв'язуваних завдань будь-яка складова цих сил може зіграти вирішальну роль.

Нова *проблема* полягає в *інтеграції інформаційних воєн у загальну стратегію національної безпеки*. Експертами США відзначається необхідність розроблення єдиної концепції інформаційної війни, що включає як воєнний, так і фінансовий, торговий, психологічний, юридичний й інші аспекти.

При цьому головна стратегічна мета наступальних інформаційних дій з активного впливу на автоматичні системи і засоби озброєнь зміщується на особистість, тобто на людину, що приймає рішення. На

думку експертів, такі дії можуть бути найбільш ефективними в мирний час і на початкових етапах зародження конфлікту, що добре узгоджується з основними цілями національної політики безпеки США.

На основі прогнозу стратегічних умов до 2020 року американські військові експерти виявили і зафіксували в офіційних документах ряд основних тенденцій світового розвитку, що ставлять перед США потенційні проблеми. При цьому уточнюється, що висновки, базовані на прогнозі тенденцій розвитку, можуть бути відносно точними тільки для найближчого часу (від одного року до трьох років), але точність їхня губиться в міру віддалення в майбутнє. Цілком зрозуміло, що деякі тенденції (наприклад, демографічні) можуть бути відстежені з високим ступенем точності. Інші ж (типу геополітичних) менш передбачувані. Вони піддані значно більш швидким змінам під впливом різних подій.

Воєнні аналітики США роблять загальний висновок: держави хоча і залишаються домінантними одиницями міжнародної системи, але в зростаючій мірі будуть підпадати під вплив могутності багатонаціональних корпорацій і міжнародних організацій. Розвиток технологій, геополітична трансформація, демографічний "тиск", а також посилення економічних і соціальних тенденцій можуть радикально змінити реалії сьогоднішнього часу. Діапазон можливих сценаріїв широкий і їх складно (чи неможливо) пророчити. Отже, центральною проблемою для оборонної структури є розвиток у тому напрямку, що дозволить їй ефективно реагувати на будь-який варіант подій. Це визначає необхідність постійної адаптації сил до існуючих тенденцій.

2.3.2. Інформаційна війна за поглядами китайських військових аналітиків

Інформаційне протиборство у збройній боротьбі. Майбутня війна, виникнення якої, як вважають китайські військові аналітики, може бути спровоковане збоєм у комп'ютерних мережах промислового сектора світової економіки, буде являти собою, власне кажучи, безкомпромісну боротьбу в інформаційній сфері. Така війна охопить

усю сукупність воєнних, політичних і економічних аспектів життєдіяльності людей. На першому плані в ній будуть інформаційні системи.

Люди, що беруть участь в інформаційній війні, за своїм положенням аж ніяк не солдати (не носять військову форму, не стріляють). Однак вони можуть приймати стратегічні рішення як персонал так званих мозкових центрів, основа яких – фахівці найвищої кваліфікації в галузі інформаційних технологій (ІТ). Якнайшвидша мобілізація особового складу збройних сил у період розвитку конфліктів утрачає свою актуальність. Замість цього передбачається "мобілізація" інформаційних центрів і вступ їх у війну першими.

Вплив на супротивника може здійснюватися непрямим шляхом, наприклад через Інтернет. У цьому випадку протиборчій стороні не завжди удасться визначити, що це – несанкціонований доступ в інформаційну мережу комп'ютерного хакера чи підступ ворога. Такий характер дій передбачає наявність у кожного "комп'ютерного солдата" високого рівня незалежності й ініціативи. Він спроможний працювати самостійно, без взаємодії з ким-небудь і, діючи поодинці, вводити в інформаційні мережі супротивника таку величезну кількість непотрібних відомостей, що через перевантаження каналів зв'язку блокується нормальна робота інформаційних систем останнього, знижується імовірність відповідних дій. Таким чином, активно сполучаючи людський і штучний інтелект, використовуючи вмілу організацію, можна ввести протидіючу сторону в стан інформаційного хаосу.

Крім того, передбачається корінна зміна традиційних форм і способів збройної боротьби, затвердження пріоритету концепції інформаційної війни і т.д. Інформаційні технології – це ключ до оволодіння всіма іншими технологіями світу, який стрімко розвивається, і оскільки вони поступально соціалізуються, а сфери зіткнення інтересів людей усе більше розширюються, то *ведення інформаційного протиборства перестало бути завданням винятково збройних сил.*

В даний час нові концепції ведення операцій швидко завойовують собі право на життя. Інформація вже сама по собі не тільки своєрідна зброя, але і цінний трофей. Якість, кількість і швидкість її передачі

являють собою ключові елементи інформаційної переваги. За своїм впливом на об'єкт вона порівнянна з високоточною зброєю і засобами ведення електронної війни. Інформаційна зброя може використовуватися для завдання втрат як активним, так і пасивним системам впізнання супротивника, з найбільшою ефективністю виводити з ладу його бойові засоби, приводитися в дію після певного періоду "інкубації". Тому надійний захист інформації, своєчасне прийняття контрзаходів щодо нейтралізації негативного впливу є основними пунктами підготовки і ведення інформаційної війни.

Отже, в інформаційне століття засоби і методи, концепції ведення війни докорінно змінюються. Протиборство воюючих сторін може мало вплинути на зовнішній матеріальний світ, викликавши руйнування інформаційних мереж. Шантаж й інші ефективні заходи активного характеру, застосовувані за допомогою інформаційного впливу, дозволяють істотно послабити супротивника чи завдати йому поразки. Кривавий характер війни змінюється безкровною конфронтацією інформаційних систем. Ігнорування питань інформаційної війни в даний час неприпустимо, інакше легко опинитися на задвірках історичного процесу.

Незважаючи на відсутність загальноприйнятого, офіційного визначення поняття "інформаційна війна", китайські військові експерти вже давно оперують ним. У даному питанні вони широко використовують напрацювання іноземних, зокрема американських, військових фахівців і виділяють *такі аспекти* у змісті цього поняття:

– розвідка воєнного, економічного, політичного і культурного потенціалу супротивника і блокування аналогічних дій з його боку;

– руйнування (подавлення) інформаційної складової його систем бойового управління і зв'язку і захист своєї;

– забезпечення безперешкодного доступу до глобальних інформаційних систем і недопущення до них супротивника;

– широке використання АСУ як засобу інформаційного забезпечення будь-яких видів бойової діяльності;

– створення гнучкої і мобільної бази даних; комп'ютерне відтворення реального поля бою.

Вважається, що інформаційна війна включає також бойові дії за участю сучасних, інформаційно насичених засобів ведення бою. Передбачається створення спеціальних бойових формувань,

призначених для захоплення і контролю інформації, застосування усіх видів інформаційної зброї, подавлення (нейтралізації) інформаційних систем супротивника, уведення його в оману і протидії йому.

Військові аналітики КНР, формулюючи термін "інформаційна війна", трактують його у вузькому і широкому сенсі [18]. У *вузькому сенсі інформаційна війна – це польова інформаційна війна, тобто бойові дії в сфері управління військами.* Сюди входять активне використання засобів розвідки, заходи щодо введення супротивника в оману й оперативного маскування, психологічні операції, послідовне ураження його інформаційних систем, систем бойового управління і зв'язку, а також захист своїх аналогічних систем.

У широкому сенсі інформаційна війна — це великомасштабні бойові дії з перевагою інформаційної складової, які характеризуються застосуванням спеціально призначених для її ведення військових формувань, оснащених високоточною зброєю. Якщо основним засобом досягнення успіху на полі бою в XX столітті були танки, то в майбутньому ним стане комп'ютер. Це, у свою чергу, передбачає застосування комп'ютерних вірусів, здатних руйнувати програмне забезпечення технічних засобів органів бойового управління і зв'язку, ініціювати збої в системах управління і наведення високоточної зброї і тим самим значно знижувати бойовий потенціал супротивника. Війна із широким використанням високоточної зброї зажадає істотного збільшення швидкості добування розвідданих, часу попередження про удари супротивника, поліпшення взаємодії командирів усіх ступенів, підвищення маневреності військ, а тобто, і ефективності усіх видів інформаційного забезпечення. Літаки, танки, кораблі і ракети, виготовлені із застосуванням технології "Стелс", стануть основною бойовою технікою військ. Бойові дії з їхньою участю, швидше за все, будуть нагадувати змагання у швидкості виявлення і знищення і характеризуватися високою інтенсивністю і швидкоплинністю.

Китайські військові експерти пильну увагу приділяють закордонним розробкам в сфері ведення інформаційної війни. Як і західні військові фахівці, вони вважають, що інформаційна війна не є в буквальному значенні війна на полі бою, підготовкою до якої служать численні навчання і маневри військ. Збройні конфлікти

останнього часу спонукали їх виділити *кілька характерних рис, властивих інформаційній війні.*

По-перше, *"прозорість" полю бою.* Звична "гарячка бою" поступається місцем "хірургічним" методам роботи підрозділів інформаційної війни. Оператор комп'ютера може здійснювати безупинний контроль за ситуацією, спостерігати відображуване на дисплеї розташування своїх військ і військ супротивника, його об'єкти, концентрацію і переміщення його сил.

По-друге, *загальна координація дій військ* за допомогою створення єдиного каналу управління для всіх бойових підрозділів і підрозділів тилового забезпечення. Всі оперативні функції зазначених формувань (розвідка, управління, зв'язок) у цьому випадку зводяться в єдину систему. Наприклад, оператор інформаційного центру, маючи дані про кількість, склад і координати виявлених цілей супротивника, робить розрахунки для їх розподілу за засобами ураження, визначає кількість необхідних боєприпасів і т.д.

По-третє, *ведення бойових дій у реальному масштабі часу,* тобто негайне реагування на зміну бойової обстановки.

По-четверте, *точність ударів,* що відрізняються своєрідною чистотою й акуратністю, подібно до роботи скальпеля хірурга.

Для перемоги в інформаційній війні необхідне оснащення збройних сил передовими інформаційними технологіями.

Такі збройні сили являють собою нову категорію військ із самостійною теорією ведення бойових дій, особливою організаційно-штатною структурою, високим рівнем підготовки особового складу й озброєнням, що цілком відповідають вимогам інформаційної війни. Китайські військові експерти скрупульозно переймають досвід закордонних колег у даній сфері. Особливо пильну увагу вони приділяють дослідженням у США – єдиній країні, де план створення армії нового типу вже існує на папері і поступово втілюється в життя.

Бойові формування, призначені для ведення інформаційної війни, будуть використовувати технології цифрового зв'язку, цілісну систему розвідки і бойового управління, високоточну зброю. Їхній арсенал поповнять радари нового покоління, системи впізнання типу "свій–чужий", елементи глобальних навігаційних систем. Досвід навчань, проведених армією США, свідчить, що сучасні ІТ забезпечують, наприклад, скорочення середнього часу підльоту

бойових вертольотів і підготовки їх до атаки цілі з 26 до 18 хвилин, збільшення відсотка цілей, що уражаються, з 55 до 90. Опрацювання і передача повідомлень у вищестоящі штаби в ланці рота – батальйон скорочується з 9 до 5 хвилин.

З метою пристосування до потреб інформаційної війни організаційно-штатна структура збройних сил набуде змін:

– чисельність сухопутних військ буде скорочуватися, а ВМС і ВПС зростатиме;

– можливо, з'являться нові види збройних сил, такі як космічні сили й інформаційно-комп'ютерні війська. Збільшиться кількість офіцерів-професіоналів, особливо з інженерною освітою. Організація частин і підрозділів буде ґрунтуватися на оптимальній комбінації високоосвіченого особового складу і високотехнологічної техніки; управління повинне стати ще більш гнучким.

За поглядами керівництва КНР, її збройні сили спроможні адекватно реагувати на зміни, що відбуваються в сфері світового військового будівництва. Поки ще за розробками й оснащенням сучасним озброєнням вони відстають від розвинених країн Заходу. Однак китайські військові експерти вважають, що у світлі прийдешніх збройних конфліктів, зокрема із застосуванням інформаційних технологій, їхня армія здатна відповідним чином відповісти супротивнику, адже принцип максимального використання внутрішніх сил у протидії зовнішнім – у національних традиціях Китаю. За рівнем інформаційних технологій та інформаційної зброї Китай у майбутній війні навряд чи зможе перевершити потенційного супротивника, тому його стратегічна лінія буде спрямована на активну оборону своїх рубежів з максимальним залученням внутрішніх ресурсів. У контексті інформаційної війни це означає посилення заходів з маскування своїх військ, підвищення активності протиповітряної оборони, атаки і перехоплення бойових засобів, що застосовують високоточну зброю, у момент, коли супротивник цього не очікує, і т.д.

Китайські військові аналітики припускають, що успішне ведення інформаційної війни зажадає від збройних сил:

– повного використання переваг території країни і засобів розвідки з метою раннього виявлення намірів супротивника, його підготовки до наступальних дій;

– розроблення, удосконалювання і застосування наявних на озброєнні ефективних інформаційних технологій;

– посилення акценту на ведення мобільних бойових дій;

– організації операцій по деморалізації військ ворога;

– формування спеціальних сил ведення інформаційної війни, їх оснащення сучасною зброєю, розробленою на базі нових інформаційних технологій.

Вони упевнені, що розвиток інформаційних технологій неминуче викликає революцію у військовій справі і ця революція вже почалася. Ті, хто першими візьмуть у ній участь, виявляться на гребені процесу розвитку людського суспільства. Зазначена революція – це насамперед *революція концепцій*, а потім уже прогрес у науці і техніці, стратегії і тактиці, навчанні військової справи. Тому найважливішою проблемою, що вимагає ретельного пророблення, є підготовка і ведення інформаційної війни.

Значення психологічних операцій в інформаційній війні. Пропагандистське розкладання військ і населення супротивника має таку саму давню історію, як і воєнне мистецтво. Протилежні сторони і сотні, і тисячі років тому знали, що боротися з ворогом можна не тільки за допомогою зброї, але і шляхом цілеспрямованого психологічного впливу, намагалися використовувати засоби духовного впливу для ослаблення морального духу і бойової могутності ворога.

Уже приблизно в V столітті до н.е. китайський полководець, воєнний теоретик і філософ Сунь Цзи у своєму трактаті “Мистецтво війни” писав, що найкраща політика зводиться до захоплення держави цілісною, зруйнувати її значно легше. Взяти в полон армію супротивника краще, ніж її знищити. Одержати сотню перемог у сотні боїв – це ще не межа мистецтва. Скорити супротивника без бою – от вінець мистецтва.

Саме в цій широко відомій праці підкреслюється, що найвигідніша з усіх воєнних стратегій – маніпулювання ворогом таким чином, щоб домогтися легкої перемоги над ним без бою. Сунь Цзи першим узагальнив досвід, накопичений давнім Китаєм в галузі психологічних операцій. Він стверджував, що найгірше – напад на ворожі укріплені міста. У Китайській Народній Республіці дану концепцію перефразували так: “Краще атакувати розум супротивника, аніж його

укріплені міста”.

Теоретичні побудови основоположника психологічної війни зводяться до наступного:

– розкладайте все хороше, що є в стані вашого супротивника;

– втягуйте його видних представників у злочинні підприємства, підривайте їхній престиж, виставляйте їх у потрібний момент на ганьбу громадськості;

– використовуйте співробітництво найпідліших і мерзенних людей;

– розпалюйте сварки і зіткнення серед громадян ворожої країни;

– перешкоджайте всіма способами оснащенню, забезпеченню і наведенню порядку в збройних силах ворога;

– будьте щедрі на пропозиції і подарунки для покупки інформації і підкупу спільників;

– взагалі не заощаджуйте ні на грошах, ні на обіцянках, тому що вони приносять багаті дивіденди.

Подальший розвиток воєнного мистецтва незмінно супроводжувався удосконалюванням форм морального впливу на супротивника. До II століття н.е. належить поява самостійної теми пропаганди – проголошення справедливого чи несправедливого характеру війни. Ні чим іншим, як прагненням підірвати бойовий дух воїнів ворога, можна пояснити звичай, коли одна з воюючих сторін виступає з тим чи іншим обвинуваченням на адресу свого суперника і закликає своїх союзників і однодумців у конфронтуючому стані примкнути до “боротьби за праведну справу”. Цей прийом широко використовувався правителями давнього Китаю впродовж значного періоду часу. Висунуте до початку чи на самому початку збройного зіткнення обвинувачення служило в ході всієї війни надійним обґрунтуванням законності дій, спрямованих на розтрощення ворога.

Здавна в Китаї вважали одним із найбільш надійних засобів для цього обман (дезінформацію) – пряме маніпулювання поглядами супротивника на реальність з метою спонукати його вживати заходів у напрямку, який відповідає власним інтересам. Знову звернемося до Сунь Цзи. Він писав: “Війна – гра обману. Тому:

– прикидайся немічним, коли сильний;

– прикидайся млявим, коли готовий завдати удару;

– здавайся далеким, коли насправді знаходишся поруч, і навпаки;
– коли ворог жадає наживи, підмани його наживкою;
– коли ворог в безладді, нападі і перекинь його;
– коли ворог хвалиться значними силами, будь подвійно готовий діяти проти нього;
– коли ворог страшний, обходь його;
– якщо ворог податливий гніву, провокуй його;
– якщо ворог боязкий і обережний, заохочуй його марнославство;
– якщо сили ворога свіжі, вимотай їх;
– якщо ворог єдиний, розділи його;
– атакуй ворога, коли він найменше готовий;
– дій, коли ворог найменше тебе очікує.

У цьому полягає тонкість командування стратега, що неможливо заздалегідь передати чітко визначеними правилами, готовими для негайного застосування".

Китайські військові аналітики вважають, що сьогодні нездатність протистояти іноземному інформаційно-психологічному вторгненню більш небезпечна, чим відсталість в інших галузях. Розвиток технологій у наші дні, на їхню думку, дав можливість активно впливати на всіх людей – від звичайних громадян до глав держав. Імітація промов, вимовлених нібито лідерами країн, фальсифікація фото- і кіноматеріалів з подальшою демонстрацією непідготовленій аудиторії – усе це здатне серйозно вплинути на населення і військовослужбовців протиборчої сторони.

Можна сміливо стверджувати, що тактика і стратегія ведення психологічної війни активно розробляється провідними воєнними теоретиками НВАК. Деякі роботи з даної тематики дають підстави говорити про наявність в них свого роду "китайської специфіки". Звертає на себе увагу широке використання історичного матеріалу й основних принципів китайського воєнного мистецтва, що має тисячолітні традиції. Крім того, робиться упор на проведення психологічних операцій у мирних умовах, вони розглядаються як підготовчий етап повномасштабної інформаційної війни в умовах відкритого збройного протиборства.

Інтенсифікація розробок щодо організації і ведення подібних операцій дає всі підстави думати, що незабаром вони одержать у КНР найбільше поширення [19].

2.3.3. Погляди російських військових фахівців на роль інформаційної компоненти у війнах майбутнього

Особливості бойового застосування високоточної зброї призвели до необхідності інтеграції різних засобів збройної боротьби в єдині системи високоточної зброї – розвідувально-ударні комплекси. Ці комплекси будуть являти собою складні системи функціонально взаємопов'язаних засобів розвідки, управління, забезпечення і ураження. Складність таких систем не стане перешкодою для їх використання в умовах війни. Вони будуть абсолютно надійні, стійкі до радіоелектронної протидії і не вимагатимуть особливої підготовки обслуговуючих їх операторів.

Існуючі і розроблювані у провідних країнах світу високоточні крилаті й інші ракети звичайного типу наземного, повітряного і морського базування можуть застосовуватися лише в умовах інформаційної переваги. З допомогою засобів інформатики, розвідки і зв'язку можна швидко одержати точну, своєчасну і захищену інформацію, що дозволить правильно реагувати на будь-який конфлікт із метою негайного оволодіння ситуацією і прийняття необхідних рішень. Для цього, очевидно, доведеться розробити зовсім інші, чим зараз, глобальні воєнні системи командування, управління, розвідки і зв'язку. Знадобиться мати комунікацію інформаційних мереж, що перекриватимуть усі сфери збройної боротьби практично по всій земній кулі. Одночасно буде потрібно перешкоджати супротивнику в одержанні інформації для управління його військами і зброєю. Інформаційна перевага повинна бути реалізована через перевагу в мобільності, у швидкості реакції, у точному впливі на супротивника й у мінімально можливому ризику для своїх сил і засобів. Інформаційна перевага повинна бути реалізована: через панування в маневрі силами, засобами і вогнем; через масоване і тривале за часом застосування високоточної зброї; через адресне всебічне матеріально-технічне забезпечення; через надійний захист сил і засобів на всіх рівнях.

За думкою академіка Академії воєнних наук Російської Федерації В.Сліпченка, інформаційна складова високоточної зброї буде мати повний набір програмних засобів і заходів як активного і пасивного захисту від атак на його інформаційні системи, так і впливу на всі існуючі і перспективні системи ППО і ПРО супротивника і буде діяти разом з космічними засобами розвідки цілей і об'єднаною радіолокаційною системою виявлення і наведення. Засоби розвідки також одержать великий розвиток, тому що на них будуть покладені завдання пошуку, виявлення, ідентифікації і виміру необхідних параметрів стаціонарних об'єктів економіки, що повинні бути знищені високоточними крилатими чи міжконтинентальними ракетами. Використовуватимуться командні пункти космічного і повітряного базування для спрямування ударів по найбільш важливих стаціонарних і рухомих цілях.

Для виявлення наземних цілей, що підлягають ураженню в глибині території супротивника, очевидно буде потрібно створити більш дешеві чим космічні, але високоефективні безпілотні літальні засоби стратегічної розвідки. Розвідувальний потенціал держав може істотно підвищитися саме за рахунок безпілотних літальних апаратів з великою тривалістю польоту.

Слід зазначити, що в ряді найбільш розвинених країн у різних видах їхніх збройних сил, родах військ уже зараз є велика кількість різнотипних сил і засобів розвідки, однак усі вони значною мірою роз'єднані. У війнах і воєнних конфліктах майбутнього буде потрібна висока інтеграція численних розвідувальних систем для їхнього автоматизованого розподілу в глобальній інформаційній мережі по всій земній кулі. Виникне необхідність серйозного об'єднання систем розвідки космічного і повітряного базування. Неминуче підвищення гнучкості застосування й універсалізації засобів розвідки.

Необхідна кількість повітряно-космічних сил і засобів розвідки у війнах нового покоління буде заповнюватися, головним чином, безпілотними літальними апаратами, кількість яких на рубежі сторіч в західних країнах досягне 30 тис. Один з таких літаків уже був продемонстрований в середині лютого 1997 року в Сан Дієго (штат Каліфорнія, США). Цей літак має розрахункову дальність польоту до 25 тис. км і здатний знаходитися в повітрі впродовж 42 годин на висоті 22 км. На борті безпілотного літака є оптичні й інфрачервоні

телекамери, радіолокаційна станція, а також станції радіо і радіотехнічної розвідки. Бортова апаратура дозволяє робити детальну зйомку місцевості і безупинно передавати розвіддані по супутникових каналах зв'язку безпосередньо на центральний командний пункт збройних сил США. Є відомості, що інший літак-розвідник подібного типу також розробляється в США. Правда, його характеристики трохи нижчі – тривалість польоту 12 годин на висоті 15 тис. км. Однак цей літак розробляється за програмою "Стелс", тобто він буде невидимкою для засобів виявлення. США сподіваються мати на початку нового століття і тисячоліття 120–150 стратегічних літаків-розвідників, а подальша їх кількість може досягати 500-600 одиниць. Не виключено, що частина таких літаків буде виготовлена і для інших країн – Великобританії, Франції, Німеччини, Китаю, Тайваню.

У цей перехідний період будуть діяти спільно стратегічні неядерні засоби, повітряні, морські й сухопутні сили, засоби доставки високоточної зброї і зброї на нових фізичних принципах. Значною мірою цьому сприятимуть також триваюче розроблення (крім високоточних засобів і інших типів озброєнь, і в першу чергу – зброї спрямованої передачі енергії), автоматичних і автоматизованих систем наведення високоточної зброї, нових вибухових речовин підвищеної могутності, засобів опрацювання даних надвисокої швидкодії, а також засобів радіоелектронної боротьби.

Після завершення перехідного періоду у війнах шостого покоління знайдуть широке застосування засоби ураження, дія яких по об'єктах (цілях) буде заснована на використанні фізичних форм енергії, а також відповідних засобів захисту від їхнього впливу. Можна стверджувати, що й у збройній боротьбі майбутнього головною залишиться фізична боротьба. Однак зовсім не виключено, що в цій боротьбі знайдуть застосування й інші засоби ураження.

В арсеналах деяких, головним чином, відсталих країн у перехідний період збережеться на озброєнні хімічна зброя (так звана, ядерна зброя бідних), яку вони цілком ймовірно можуть застосувати, не боячись за наслідки. У разі застосування таких засобів ураження буде потрібно мати і застосовувати відповідні засоби захисту від їхнього впливу. Такий вид збройної боротьби буде належати до хімічної боротьби. Здається, що після закінчення перехідного періоду будуть

вжиті всі заходи, спрямовані на повну ліквідацію цієї зброї на нашій планеті.

Не виключено, що в перехідний період може одержати розвиток і біологічна зброя. Вона також найбільше ймовірно може бути на озброєнні ряду економічно відсталих, але екстремістських країн. Вид збройної боротьби, у якому ураження буде здійснюватися біологічним впливом і будуть застосовуватися відповідні засоби захисту, можна назвати біологічною боротьбою. Є підстави думати, що за допомогою Ради Безпеки ООН ця зброя буде поставлена поза законом і у разі її розроблення в окремих країнах до них будуть вжиті усі, в тому числі і силові, заходи для припинення виробництва і ліквідації наявних запасів.

У війні і збройній боротьбі майбутнього для виведення з ладу обслуговуючого персоналу об'єктів економіки може знайти застосування і зброя на нових фізичних принципах (НФП) – акустичне ураження. Вона може доставлятися у великих кількостях за допомогою високоточних крилатих і балістичних ракет, викидатися на парашутах, скидатися на землю в районі об'єктів і проникати усередину об'єктів, що підлягають ураженню. У цьому виді уражального впливу буде використовуватися енергія акустичних випромінювань певної частоти й енергія, яка генерується акустичною зброєю. Таке ураження може викликати деморалізацію і навіть загибель усього живого, порушувати роботу чи виводити з ладу ті радіоелектронні засоби, що працюють на принципі приймання і перетворення акустичних хвиль, руйнувати окремі елементи деяких видів зброї, військової техніки й об'єктів. Носіями такої зброї можуть бути наземні, морські, повітряні і космічні засоби.

Значний розвиток одержить зброя НФП електромагнітного ураження. Вона буде являти собою вид уразливого впливу на об'єкти, цілі з використанням енергії електромагнітних випромінювань різної довжини хвилі і рівня потужності, генерованих радіочастотною і лазерною зброєю, засобами радіоелектронної протидії (РЕП) чи висотними ядерними вибухами. Така зброя буде здатна подавляти практично всі класичні радіоелектронні засоби (РЕЗ), що працюють на принципі приймання і перетворення електромагнітних хвиль; викликати розплавлювання чи випар металу озброєння і військової техніки або викликати структурні зміни електронних елементів

військової техніки; впливати на поведінку людини; руйнувати живі клітини, порушувати біологічні і фізіологічні процеси у функціях живих організмів. Носіями такої зброї можуть бути ракетні системи наземного, морського і повітряного базування, застосовувані по настильних траєкторіях, безпілотні засоби великої дальності дії.

Ефективне ураження і захист у війнах і збройній боротьбі майбутнього потребують кардинального розвитку засобів розвідки. Розвідка в збройній боротьбі майбутнього також змінить свій статус і стане невід'ємним елементом і змістом будь-якого удару, бою, операції, а не їх забезпеченням, як прийнято в даний час. Єдність розвідки і ураження, як один з головних ознак збройної боротьби майбутнього, особливо наочно видні на прикладах функціонування розвідувально-ударних бойових систем (РУБС) і розвідувально-вогневих комплексів (РВК).

Аналогічні міркування стосуються і визначення місця маскування у війнах і збройній боротьбі майбутнього. Засоби і прийоми маскування, застосовувані узгоджено з діями великої кількості високоточних засобів і зброї на нових фізичних принципах у сполученні з ураженням засобів розвідки, будуть вводити в оману супротивника не зважаючи на те, що вони безпосередньо не уражають цілей, але знижують чи навіть виключають його можливості по радіоелектронному придушенню і вогневому ураженню військ і об'єктів. Тому в збройній боротьбі майбутнього маскування також цілком очевидно виключать з видів забезпечення на всіх рівнях і віднесуть до змісту бойових дій, зокрема, до заходів щодо захисту військ від ураження.

Що стосується терміна "забезпечення бойових дій", то у війнах і збройній боротьбі майбутнього до нього будуть віднесені тільки ті специфічні заходи, що створюють умови для дій по ураженню супротивника чи захисту від його ураження. Тут термін "забезпечення" буде повною мірою відповідати його змісту: постачання всім необхідним, недопущення нестачі будь-чого і т.п. Виходячи з цього, забезпеченням бойових дій у збройній боротьбі майбутнього можна буде вважати лише тиловий і технічний види забезпечення.

Особлива роль у збройній боротьбі майбутнього буде приділятися *інформаційному ресурсу.* Високоточна зброя і зброя на нових

фізичних принципах, на які будуть покладені ті завдання, що завжди вирішували в основному лише великі угруповання живої сили, зажадає мати необхідну розвідувальну інформацію. Виникне гостра потреба в різних інформаційних комплексах, реалізованих у засобах розвідки й управління, а також у силах і засобах РЕБ. Для ведення розвідки будуть широко застосовуватися космічні, морські і наземні сили і засоби розвідки. Буде потрібно безупинно і детально спостерігати за всією територією супротивника, за станом його стратегічних ударних і стратегічних оборонних сил, за всіма пересуваннями його військ (сил) у межах театру воєнних дій.

Управління військами (якщо вони в деякій мірі збережуться в нинішньому розумінні), силами і засобами буде здійснюватися головним чином з командних пунктів, піднятих у космос і повітря, чи з захищених командних пунктів на землі, але через повітряно-космічні засоби. Значно збільшиться кількість літаків управління і далекого радіолокаційного виявлення. Інформаційний обмін буде здійснюватися між усіма ланками і рівнями командування за допомогою автоматичних чи автоматизованих систем, розміщених на повітряних і космічних засобах.

Стає цілком очевидним, що одним із атрибутів війни майбутнього стане "інформаційна боротьба". Ясно, що цей вид боротьби також, як й інші її різновиди, має дві складові – оборонну і наступальну чи ударну. Оборонна – захист своєї інформації від впливу супротивника. Ударна – дезорганізація чи руйнація інформаційної інфраструктури супротивника, порушення процесу оперативного управління його силами і засобами. Очевидно, для ударної складової інформаційного протиборства можна використовувати і поняття "інформаційна інтервенція" чи "інформаційна агресія". У зв'язку з тим, що зараз чітко позначене прямування у бік воєн нового покоління, роль інформаційної боротьби різко зростає в таких напрямках: у боротьбі з системами управління; у нав'язуванні супротивнику своїх правил ведення воєнних дій; у ставці на військово-технічну перевагу. Інформаційна боротьба набула могутнього розвитку після створення сучасних методів воєнної системології. Використовуючи ці методи, можна швидко знайти уразливі місця системи управління, зв'язку, комп'ютерного забезпечення і розвідки супротивника і, виводячи їх з ладу, різко підвищити ефективність своїх дій в інших видах

протиборства. Критичними ланками системи управління супротивника є інформаційні засоби, руйнування або знищення яких призводить до негайного зниження його можливостей по управлінню військами і силами. Вершиною розвитку систем і засобів інформаційної боротьби очевидно стане створення *глобальної бойової інформаційно-ударної системи країни і збройних сил,* здатної контролювати стан і функціонування збройних сил і угруповань супротивника і знижувати ефективність їхнього застосування.

Прояв великого інтересу до інформаційного протиборства не випадковий. Це пов'язано з тим, що інформація стає такою самою зброєю, як ракети, бомби, торпеди і т.п. Зараз уже ясно, що інформаційне протиборство є тим фактором, що впливає на саму війну майбутнього.

Однак інформаційна боротьба ніколи не припинялася, йде вона і зараз, тому що сторони завжди прагнули контролювати інформацію супротивника не тільки у воєнний, але й у мирний час. Володіння інформаційними ресурсами у війнах майбутнього стає таким самим неодмінним атрибутом, як у минулих війнах розгром збройних сил супротивника, оволодіння його територією, руйнування його економічного потенціалу і зміни політичного строю. Цілі і завдання інформаційної боротьби є основою побудови її змісту, а отже і структури її наукової теорії.

У найзагальнішому вигляді головною метою інформаційної боротьби, як уже було показано, є збереження необхідного рівня своєї інформаційної безпеки і зниження рівня цієї безпеки в супротивника. Поставлена мета може бути досягнута вирішенням ряду взаємопов'язаних завдань, найважливішими з яких будуть руйнування інформаційного поля супротивника і збереження свого інформаційного поля.

Зараз інформаційна боротьба вже стала найважливішим змістом війни, але через застосовувані в ній сили і засоби, а також специфічні цілі і завдання набуває як значної самостійності, так і є невід'ємним елементом всіх інших форм боротьби.

Висновки

Поняття “інформаційна війна” – це не алегоричний образ, воно відбиває різновид війни, формою ведення якої є інформаційна боротьба. Висока ефективність її ведення підтверджена як масштабами і результатами холодної війни, яка була найбільш вражаючою у порівнянні з попередніми світовими війнами, хоча і велася без розв’язання збройної боротьби, так і досвідом локальних війн і збройних конфліктів сучасності.

Сутності і ролі інформаційної війни присвячена досить велика кількість публікацій, у яких вона трактується по-різному. Визначення інформаційної війни, що містяться в роботах зарубіжних фахівців і в офіційних документах, можна згрупувати так: визначення інформаційної війни у вузькому розумінні, тобто такі, які відбивають суто воєнну спрямованість, і визначення в широкому розумінні, які відбивають спрямованість на забезпечення національних інтересів в будь-якій життєво важливій сфері державної і суспільної діяльності.

Чинниками виникнення і живучості ідей інформаційної війни, судячи по різноманітних оцінках, що фігурують в пресі, є такі:

– світова економіка диктує і свої світові закони – все більш гуманні. Головний з них виглядає просто: війна (в традиційному розумінні) економічно не вигідна. Це один з системних чинників, що сприяють розповсюдженню і розвитку гуманістичних тенденцій;

– економічність інформаційної зброї, що дозволить, з одного боку, скорочувати певною мірою військовий бюджет, а з іншого – створювати високоефективну зброю XXI століття, застосування якої матиме багатообіцяючі результати;

– масоване застосування інформаційної зброї, як стверджують західні експерти, дасть можливість порівняно швидко придушувати противника, паралізувати його, примушувати до капітуляції без залучення збройних сил, без звичайних битв, типових для класичних війн, без загибелі людей і руйнування громадянської інфраструктури, і, нарешті, без втрат особового складу.

В низці таких офіційних документів США, як “Стратегія національної безпеки США” (1994 і 1996 роки), “Національна воєнна стратегія Сполучених Штатів Америки” (1995 рік), “Стратегія національної безпеки США для нового сторіччя” способи й методи інформаційної війни розглядаються як одні з найефективніших засобів забезпечення національних інтересів США в різних регіонах

світу, з одного боку, і як джерело загроз власним національним інтересам, з іншого боку. За поглядами воєнних фахівців провідних країн світу роль інформаційних воєн у забезпеченні національних інтересів буде неухильно зростати, набуватимуть інтенсивного розвитку технології їх ведення.

Глосарій до розділу

Інформаційна агресія – розв'язання інформаційної війни однією державою (групою держав) проти іншої. Інформаційна агресія спрямована на нанесення збитків інформаційній інфраструктурі держави-жертви, фактичного захоплення її інформаційного простору.

Інформаційна **війна** (в широкому розумінні) – 1) форма розв'язання суспільно-політичних, ідеологічних, а також національних, територіальних, релігійних та інших суперечностей між державами, народами, націями, класами й соціальними групами шляхом широкомасштабної реалізації способів і методів інформаційного насильства;

2) великомасштабне інформаційне протистояння між суспільними групами або державами, яке має за мету змінити розстановку сил в суспільстві;

3) між- або внутрішньодержавне інформаційне протиборство з використанням методів нанесення шкоди або повного знищення інформаційного середовища протидіючої сторони;

4) інформаційний вплив на різноманітні сфери діяльності суспільства та країни, система заходів з оволодіння інформаційними ресурсами держави та ключовими позиціями в сфері інформатизації.

Інформаційна війна *(у вузькому розумінні)* – 1) явні і приховані цілеспрямовані інформаційні впливи систем один на одного з метою одержання визначеного виграшу в матеріальній сфері;

2) комплекс заходів і операцій, що провадяться в конфліктних ситуаціях, в яких інформація є водночас зброєю, ресурсом і метою;

3) крупномасштабні бойові дії з переважною участю інформаційної складової, які характеризуються застосуванням спеціально

призначених для її ведення військових формувань і високоточної зброї;

4) інформаційна війна являє собою всеосяжну, цілісну стратегію, покликану віддати належне значущості і цінності інформації в питаннях командування, керування та виконання наказів збройними силами й реалізації національної політики. Інформаційна війна націлена на всі можливості і чинники уразливості, що неминуче виникають при зростаючій залежності від інформації, а також на використання інформації у всіляких конфліктах.... Інформаційна війна має наступальні і оборонні складові, але починається з цільового проектування та розроблення своєї "архітектури командування, керування, комунікацій, комп'ютерів і розвідки", що забезпечує особам, приймаючим рішення, відчутну інформаційну перевагу у всіляких конфліктах.

Інформаційна експансія – встановлення й розширення сфер впливу в інформаційному просторі з використовуванням для цього сукупного інформаційного потенціалу і засобів силової інформаційної дії. В агресивному виразі інформаційна експансія виявляється в досягненні інформаційного домінування над протидіючою стороною.

«Холодна війна» – стан воєнної, економічної, політичної й ідеологічної конфронтації (1946 – кінець 1980-х років) між колишнім СРСР і його союзниками, з одного боку, і США та їх союзниками, з іншого, без застосування засобів воєнного насилля.

Зв'язок ключових термінів і понять

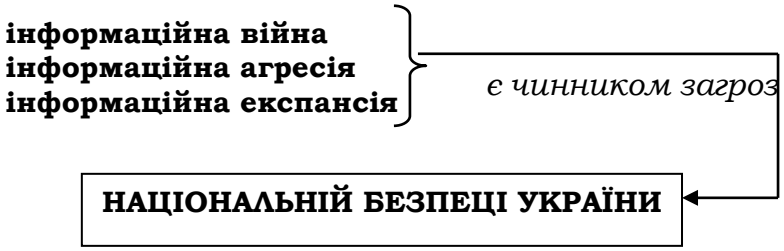


Рис.2.1.

Завдання і запитання для самоперевірки

1. Розкрийте сутність інформаційної війни в широкому розумінні.
2. Розкрийте сутність інформаційної війни у вузькому розумінні.
3. Дайте загальну характеристику чинникам, які обумовлюють неминучість інформаційних воєн.
4. Дайте загальну характеристику поглядів військового керівництва США на ведення інформаційної війни.
5. Дайте загальну характеристику поглядів на інформаційну війну китайських військових аналітиків.
6. Дайте загальну характеристику поглядів російських військових фахівців на роль інформаційної компоненти у війнах майбутнього.

Рекомендована література до розділу

1. *Гриняев С.* Концепция ведения информационной войны в некоторых странах мира // Зарубежное военное обозрение. – 2002. – № 2.

2. *Конопатов С.Н., Юдин В.В.* Традиционный смысл понятия “война” устарел // Военная мысль. – 2001. – № 1.

3. *Красноступ Н., Кругленко В.* Информационная война – миф или реальность? // Бизнес и безопасность. – 1998. – № 5.

4. *Лисичкин В.А., Шелепин Л.А.* Третья мировая информационно-психологическая война. – М.: ИСПИ АСН, 2000.

5. *Почепцов Г.Г.* Информационные войны. – М.: Рефл-бук, К.: Ваклер. – 2000.

6. *Фомін В.О., Рось А.О.* Сутність і співвідношення понять “інформаційна безпека”, “інформаційна війна” та “інформаційна боротьба” // Наука і оборона. – 1999. – № 4.

Використані джерела

1. *Жуков В.* Взгляды военного руководства США на ведение информационной войны // Зарубежное военное обозрение. – 2001. – № 1.

2. *Гулин В.П.* О новой концепции войны // Военная мысль. – 1997. – № 2.

3. Стратегия национальной безопасности США // Зарубежное военное обозрение. – 1994. – № 11.

4. *Барановский А.* Стратегии национальной безопасности США на 1996 год // Финансовая Украина. – 2 июля 1996г.

5. Национальная военная стратегия Соединенных Штатов Америки. – Комитет начальников штабов, 1995.

6. Стратегия национальной безопасности США для нового столетия // Независимое военное обозрение. – 1999. – № 5.

7. *Завадский И.И.* Информационная война – что это такое? // Конфидент. – 1996. – № 4.

8. *Попов М.О., Лук'янець А.Г.* До забезпечення воєнної безпеки в умовах загрози інформаційної війни // Наука і оборона. – 1999. – № 2.

9. *Викторов С.* Накануне 3-й мировой информационной войны // Финансовая Украина. – 18 февраля 1997 г. – № 5.

10. *Гуревич А.* Комплекс ГТО в эпоху информатики // Финансовая Украина. – 17 апреля 1996 г. – № 16.
11. *Ничипоренко В.* Прибыльная философия // Финансовая Украина. – 17 сентября 1996 г. – № 37.
12. *Рэндов А.* Глобальная стратегия США в современном мире // Финансовая Украина. – 6 августа 1996 г.
13. *Сибирский Б.* Фактор внезапности // Новости разведки и контрразведки. – 1996. – № 23.
14. Распространение иностранной экономической информации в КНР теперь будет управляться централизовано // Финансовая Украина. – 30 января 1996 г. – № 5.
15. *Кулицкий С.* Экспансия информационная и экспансия экономическая. – Финансовая Украина. – 27 февраля 1996 г. – № 9.
16. *Гриняев С.Г.* Война в четвертой сфере. Превосходство в киберпространстве будет определять победу в конфликтах XXI века // Независимое военное обозрение. – 2000. – №42.
17. *Горбачев Ю., Тюрин В.* К вопросу о “войне в четвертой сфере” // Независимое военное обозрение. – 2000. – №42.
18. *Дежин Е.Н.* Информационная война по взглядам китайских военных аналитиков // Военная мысль. – 1999. – № 6.
19. *Дежин Е.* Атака на разум противника. Китайские психологические операции в свете национальных традиций // Независимое военное обозрение. – 2001. – № 1.

Розділ 3.
ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ

3.1. Сутність та зміст основних понять предметної галузі "інформаційна безпека"

У законі України "Про основи національної безпеки України" [1] визначені основні напрямки забезпечення безпеки в інформаційній сфері, під якою часто розуміють інформаційну безпеку як складову національної безпеки України. Слід зазначити, що ці поняття не є тотожними за змістом. Під *інформаційною сферою* на змістовому рівні розуміється безпосередньо інформація та сфера її обігу. Тобто *безпека інформаційної сфери* – це стан захищеності інформації та сфер її створення, накопичення, зберігання, оброблення, розповсюдження й використання.

Запропоновані такі визначення *інформаційної безпеки* на основі аналізу робіт [1–5], а також досвіду роботи авторів над проектом Концепції інформаційної безпеки України:

– такий стан інформаційної озброєності особистості, суспільства, держави, тобто озброєності їх знаннями, при якому досягається захищеність і реалізація їх життєво важливих інтересів і гармонічний розвиток незалежно від наявності внутрішніх і зовнішніх загроз;

– такий стан інформаційного забезпечення завдань національної безпеки, при якому досягається захищеність і реалізація життєво важливих інтересів, гармонічного розвитку і потреб в інформації особистості, суспільства, держави незалежно від наявності внутрішніх і зовнішніх загроз;

– стан інформаційного середовища, при якому гарантується його розвиток і використання в інтересах особистості, суспільства і держави;

– захищеність від різного роду зовнішніх і внутрішніх загроз системи формування і поширення автоматизованих інформаційних ресурсів, яка забезпечує їхнє ефективне використання в інтересах громадян, суспільства і держави.

Безпека в інформаційній сфері – стан захищеності національних інтересів країни в сфері обертання *інформації*.

Інформаційна безпека суспільства, держави характеризується ступенем їхньої захищеності й, отже, усталеністю основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи, суспільної свідомості і т.д.) стосовно небезпечних (дестабілізуючих, деструктивних, які зачіпають інтереси країни й ін.) інформаційних впливів, причому як до впровадження, так і до викрадення інформації. Визначається спроможністю нейтралізувати такі впливи [2].

Інформаційна безпека особистості характеризується захищеністю психіки й свідомості від небезпечних інформаційних впливів: маніпулювання, дезінформування, спонукування до самогубства, образ й ін.

Необхідно зазначити, що інформаційні впливи небезпечні (або корисні) не стільки самі по собі, скільки тим, що "запускають" потужні матеріально-енергетичні процеси, управляють ними. Сутність впливу інформації саме і полягає в її спроможності "запускати" і контролювати матеріально-енергетичні процеси, параметри яких на багато порядків вище самої інформації.

Варто звернути увагу на принципову відмінність в змісті понять "інформаційна безпека" і "безпека інформації".

Безпека інформації – захищеність інформації в організації або технічній системі від несанкціонованого доступ*у* (ознайомлення, крадіжки, змін, знищення). Держстандартом України прийняте наступне визначення терміна *безпека інформації*: "стан, що забезпечує захист інформації від загроз для неї" *[Держстандарт України. Технічний захист інформації. Терміни і визначення]*. Безпека інформації забезпечується шляхом захисту інформації від випадкового або навмисного доступу осіб, що не мають на це права, її отримання, розкриття, модифікації або руйнування. Реалізація вимог і правил щодо захисту інформації, підтримка інформаційних систем в захищеному стані, експлуатація спеціальних технічних і програмно-математичних засобів захисту та забезпечення організаційних і інженерно-технічних заходів захисту інформаційних систем, що оброблюють інформацію з обмеженим доступом в недержавних структурах, здійснюється відповідними службами.

Інформаційно-енергетичний вплив – один із різновидів *психофізичного впливу*, вплив на біосистеми і, перш за все на людину, фізичних полів різної природи, модульованих семантичними (смисловими) сигналами, які сприймаються біологічними організмами в формі сигналів, повідомлень, відомостей, образів (тобто у вигляді *інформації*).

*Інформаційно-психологічний вплив****Ошибка! Закладка не определена.*** – вплив на психіку (свідомість і підсвідомість) людини сигналами вербальної (семантичної) *інформації*. Каналами розповсюдження сигналів виступають *засоби масової інформації*, окремі особи.

Системний підхід до інформаційної безпеки потребує визначення її суб'єктів, засобів і об'єктів, інформаційних загроз, джерел небезпеки, спрямованості небезпечних інформаційних потоків. Наведемо такі визначення *інформаційної загрози*:

– такий інформаційний вплив (внутрішній або зовнішній), при якому створюється потенційна або актуальна (реальна) небезпека зміни напрямку або темпів прогресивного розвитку держави, суспільства, індивідів;

– небезпека заподіяння шкоди життєво важливим інтересам особистості, суспільства, держави шляхом інформаційного впливу на свідомість, інформаційні ресурси та інфосферу машинно-технічних систем;

– сукупність чинників, що перешкоджають розвитку і використанню інформаційного середовища в інтересах особистості, суспільства і держави.

Особливістю інформаційних загроз є те, що вони, з одного боку, являють собою самостійний клас загроз, а з іншого – є реалізаційною основою інших видів загроз на інформаційному рівні, а часто і їх першопричиною.

Так у законі України "Про основи національної безпеки України" [1] як основні реальні та потенційні загрози національній безпеці України, стабільності в суспільстві в інформаційній сфері визначені такі:

– прояви обмеження свободи слова та доступу громадян до інформації;

– поширення засобами масової інформації культу насильства, жорстокості, порнографії;

– комп'ютерна злочинність та комп'ютерний тероризм;

– розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;

– намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

Разом з цим значна кількість основних реальних та потенційних загроз національній безпеці України, стабільності в суспільстві та інших сферах, визначених у Законі, тією чи іншою мірою реалізовуються через інформаційну сферу. Наведемо деякі з них:

У зовнішньополітичній сфері:

– посягання на державний суверенітет України та її територіальну цілісність, територіальні претензії з боку інших держав;

– спроби втручання у внутрішні справи України з боку інших держав;

– воєнно-політична нестабільність, регіональні та локальні війни (конфлікти) у різних регіонах світу, насамперед поблизу кордонів України.

У сфері державної безпеки:

– розвідувально-підривна діяльність іноземних спеціальних служб;

– загроза посягань з боку окремих груп та осіб на державний суверенітет, територіальну цілісність, економічний, науково-технічний й оборонний потенціал України, права та свободи громадян;

– злочинна діяльність проти миру і безпеки людства, насамперед поширення міжнародного тероризму;

– прояви сепаратизму, вимоги автономізації за етнічною ознакою окремих регіонів України.

У воєнній сфері та сфері безпеки державного кордону України:

– недостатня ефективність існуючих структур і механізмів забезпечення міжнародної безпеки та глобальної стабільності;

– можливість втягування України в регіональні збройні конфлікти чи у протистояння з іншими державами.

У внутрішньополітичній сфері:

– порушення з боку органів державної влади та органів місцевого самоврядування Конституції і законів України, прав і свобод людини і громадянина, у тому числі при проведенні виборчих компаній, недостатня ефективність контролю за дотриманням вимог Конституції і виконанням законів України;

– можливість виникнення конфліктів у сфері міжетнічних і міжконфесійних відносин, радикалізації та проявів сепаратизму в діяльності деяких об'єднань національних меншин та релігійних громад;

– загроза прояву сепаратизму в окремих регіонах України.

У соціальній та гуманітарній сферах:

– зниження можливостей здобуття якісної освіти представниками бідних прошарків суспільства;

– прояви моральної та духовної деградації суспільства.

У науково-технологічній сфері:

– наростаюче науково-технологічне відставання України від розвинутих країн;

– низька конкурентоспроможність продукції;

– відплив учених, фахівців, кваліфікованої робочої сили за межі України.

З наведених загроз можна зробити висновок, що інформаційні загрози проявляються не лише в інформаційній сфері, але й в інших сферах. Таким чином, можна дати наступне визначення поняттю інформаційної загрози. *Інформаційна загроза* – це сукупність умов і чинників, що створюють небезпеку нанесення шкоди інформації, інформаційній інфраструктурі, реалізації правового статусу людини і громадянина в інформаційній діяльності, а також шкоди діяльності по реалізації національних інтересів, пов'язаних з цими об'єктами.

Джерела інформаційних небезпек можуть бути природними (об’єктивними) і навмисними. Перші виникають у результаті непередбачених помилок і несправностей, випадкових чинників, стихійних лих й ін [2].

Одна з найбільш поширених причин, які призводять до перекручування інформації в автоматизованих інформаційних системах, і, як наслідок, до її втрати – участь спеціаліста в попередньому або підготовчому опрацюванні текстів – реферуванні,

анотуванні, індексуванні, класифікації, кодуванні й в інших операціях, які стосуються змісту оброблюваної інформації. У цьому випадку через суб'єктивізм і розходження у "тезаурусах" цих спеціалістів неможливо домогтися повної однаковості при опрацюванні семантики близьких документів, у зв'язку з чим перекручування змісту і втрата інформації при пошуку – неминучі.

Джерелами навмисних загроз особистості, суспільству, державі, у тому числі й інформаційних, є конфліктні ситуації, викликані протиріччями, обумовленими розбіжністю відповідних інтересів (системи цінностей, цілей) суб'єктів або наявністю в однієї зі сторін стосовно іншої домагань, претензій або інших спонукувань до конфлікту. За характером інтереси суб'єктів можна поділити на чотири класи:

Конфронтаційні інтереси. До цієї групи належать протилежні, взаємовиключні інтереси, що є джерелом антагонізмів між індивідуумами, соціальними групами, державами.

Розбіжні інтереси. Такими вважаються інтереси суб'єктів, які не збігаються між собою, але не є взаємовиключними і не зіштовхуються безпосередньо.

Паралельні інтереси. Для даної групи характерна відсутність антагонізмів. Навпаки – сторони переслідують по суті близькі, однорідні інтереси. Проте при цьому кожна сторона намагається реалізувати їх самостійно, без координації своїх дій з іншою стороною. У цій ситуації момент зіткнення цілком відсутній, але і кооперації немає. Паралельні інтереси можуть розвиватися як у бік розбіжності, так і в бік співробітництва.

Спільні інтереси. Під цим припускається спільність підходів обох сторін, високий рівень ідентичності уявлень двох держав про мету і методи досягнення таких інтересів. Самостійно, поодинці їх реалізувати неможливо. Спільні інтереси припускають максимальний ступінь співробітництва сторін у досягненні загальних цілей.

Основним джерелом навмисних загроз є об'єктивні і суб'єктивні протиріччя духовних, інтелектуальних і матеріальних інтересів (системи цінностей, цілей) суб'єктів взаємовідносин, а також шляхів, форм і методів їх задоволення, які й породжують конфліктні ситуації. Прагнення усунення конфліктних ситуацій та інших протиріч засобами інформаційного впливу ініціює *інформаційну боротьбу*.

Успіху досягає та сторона, яка в боротьбі за досягнення своїх цілей більш ефективно використовує інформацію й канали інформаційного впливу. Це спостерігається на всіх рівнях: окремих особистостей, їхніх співтовариств, суспільства, держави й цивілізації в цілому.

Навмисні інформаційні впливи здійснюються свідомо й цілеспрямовано. При цьому часто використовуються засоби масової інформації, засоби радіоелектронного впливу, спеціальні програмні засоби для комп'ютерів тощо.

Об'єктами небезпечного інформаційного впливу і, отже, *інформаційної безпеки* можуть бути: свідомість, підсвідомість, психіка людей; інформаційно-технічні системи різного масштабу та призначення. Якщо ж говорити про соціальні об'єкти інформаційної безпеки, то до них можна віднести особистість, колектив, суспільство, державу, світове співтовариство.

Суб'єктами інформаційної безпеки варто вважати ті органи і структури, що займаються її забезпеченням. Це можуть бути органи не тільки виконавчої, але і законодавчої, судової влади тощо.

Небезпечні інформаційні впливи доцільно поділити на два види [6,7]. Перший пов'язаний із втратою цінної інформації, що або знижує ефективність власної діяльності, або підвищує ефективність діяльності противника, конкурента. Якщо об'єктом такого впливу є свідомість людей, то йдеться про розголошення державних таємниць, вербування агентів, спеціальні заходи і засоби для підслуховування, використання детекторів брехні, медикаментозні, хімічні й інші впливи на психіку людини з метою змусити її заговорити або забути що-небудь. Безпеку від інформаційного впливу даного виду забезпечують органи цензури, контррозвідки й інші суб'єкти інформаційної безпеки. Якщо ж джерелом інформації є технічні системи, то йдеться вже про технічну розвідку або шпигунство (перехоплення телефонних розмов, радіограм, сигналів інших систем комунікації), проникнення в комп'ютерні мережі, банки даних. Діяльністю подібного роду займається, наприклад, агентство національної безпеки США, витрачаючи на це близько 15 млрд доларів на рік. Протидіють технічній розвідці органи контррозвідки, а також структури, які володіють теорією та практикою захисту комп'ютерних засобів, систем зв'язку.

Другий вид інформаційного впливу пов'язаний із впровадженням негативної інформації, що може не тільки призвести до небезпечних помилкових рішень, але і змусити діяти на шкоду, навіть підвести до самогубства, а суспільство – до катастрофи. Прикладом наслідків інформаційних впливів такого виду може бути достатньо великий клас таких інформаційно-психологічних небезпек:

– спроби узурпації влади через оволодіння інформаційними ресурсами;

– маніпулювання суспільною свідомістю з боку неконтрольованих засобів масової інформації;

– селективне поширення інформації (створення "інформаційного дефіциту" в окремих прошарках суспільства);

– виникнення елітарних прошарків суспільства (розподіл суспільства на поінформованих і непоінформованих);

– руйнація національної культури через виникнення і розвиток нової "комп'ютерної культури";

– психічні розлади ("інформофілія", "інформофобія");

– розмивання почуття колективізму, розвиток індивідуалізму, відрив від суспільства.

Інформаційну безпеку цього виду повинні забезпечувати спеціальні структури інформаційної (інформаційно-психологічної, інформаційно-технічної) боротьби, завданням яких є нейтралізація акцій дезінформації, припинення маніпулювання суспільною думкою, протидія різноманітним видам радіоелектронного впливу, попередження й ліквідація наслідків комп'ютерних атак тощо.

Розгляд інформаційної безпеки з позицій системного підходу дозволяє побачити відмінність наукового розуміння цієї проблеми від повсякденного, розкрити її сутність. У повсякденному житті інформаційна безпека розуміється лише як необхідність боротьби з витоком інформації, у тому числі і закритої (секретної), а також поширенням хибних відомостей і таких, які можуть бути джерелом деструктивного впливу. Осмислення нових інформаційних небезпек, особливо технічного плану, у суспільстві ще не відбулося.

3.2. Інформаційна боротьба як інструмент забезпечення інформаційної безпеки держави

Інформаційна революція і пов'язані з нею організаційні новації вносять зміни в природу конфліктів, структуру збройних сил, військові доктрини і стратегії, які будуть потрібні в найближчому майбутньому, а також припускають можливість ведення "інформаційної війни", для досягнення результатів в якій не вимагається ані масовості, ані мобільності – перемога дістанеться стороні, яка володіє більшими знаннями і здатна передбачити дії протиборчої сторони.

У сучасних умовах перемога у війні, на думку зарубіжних фахівців, не обов'язково полягає в повному розгромі збройних сил протидіючої сторони, в їх фактичному знищенні або полоні, окупації або встановленні тотального контролю над територією противника. Тому гіпотетична перемога, яка переслідує надто значні політичні цілі, може полягати в дезінтеграції військового організму іншої сторони, руйнуванні основних елементів системи державної влади, виведенні з ладу передусім найважливіших вузлів громадянського і військового управління.

Пошук альтернативних шляхів досягнення перемоги у війні призведе до того, що боротьба набуватиме принципово іншої форми, а з урахуванням тенденцій скорочення Збройних Сил, систем і засобів озброєння все з більшим ступенем буде здійснюватися перехід від можливої відкритої збройної боротьби до прихованої боротьби в різноманітних сферах.

Виходячи із сутності інформаційних воєн, розглянемо основні поняття інформаційної боротьби.

Триєдина сутність інформаційної боротьби в широкому розумінні відображена в таких її взаємопов'язаних визначеннях:

– це об'єктивно існуюча форма прояву стосунків між суб'єктами під час досягнення певних цілей і розв'язання конфліктних ситуацій чи інших суперечностей на інформаційному рівні;

– це наука, що акумулює всі вироблені людством знання про закономірності, принципи, форми, методи й засоби завоювання

інформаційної переваги над протидіючою стороною, тобто наука про механізми інформаційного протиборства;

– це комплекс заходів, спрямованих на досягнення певних цілей і розв'язання конфліктних ситуацій на інформаційному рівні, здійснюваних за єдиним задумом і планом та узгоджених за часом, місцем, залученими силами й засобами.

Об'єктивність існування інформаційної боротьби зумовлена об'єктивністю існування самої інформації й природністю використання інформації та її властивостей для розв'язання конфліктних ситуацій, що виникають при неузгодженості інтересів і цілей сторін. Із сутності інформаційної боротьби випливає, що вона, на відміну від інформаційної війни, не має агресивної основи. До її методів і засобів удаються, наприклад, для обґрунтування доцільності впровадження у виробництво певних технологічних рішень.

Посилення ролі інформаційної боротьби при вирішенні завдань у будь-якій сфері суспільно-політичної і державної діяльності зумовлено рядом факторів. Один із них – це створення умов для більш інтенсивного виявлення і включення в процес розвитку суспільства й країни індивідуального та групового інтелекту водночас з безумовними достоїнствами демократії, що надала ці умови, з'явилась необхідність боротьби за "уми", за їх орієнтацію в інтересах вирішення тих чи інших завдань, за формування бажаного "усвідомленого" відношення до вирішення життєво важливих проблем, бажаної системи поглядів і цінностей окремих особистостей або соціальних груп. Найефективнішим способом цієї боротьби є цілеспрямоване і методологічно грамотне формування інформаційних потоків, "збалансованих" за змістом і обсягом та орієнтованих на особливості тих чи інших соціальних прошарків суспільства.

Як об'єктивно існуючий феномен, інформаційна боротьба має свої мету, завдання, закономірності, способи, методи й засоби ведення. Урахування та грамотне використання об'єктивно існуючих закономірностей інформаційної боротьби дозволить усунути або знизити рівень прояву загроз національній безпеці України.

Метою інформаційної боротьби в широкому розумінні є, перш за все, забезпечення воєнно-політичних, економічних і воєнних інтересів країни за рахунок досягнення й утримання інформаційної переваги на найбільш значущих (чуттєвих, уразливих) в конкретних умовах

напрямках. Інформаційна перевага не є самоціллю, тому що надає перевагу тільки у разі її ефективного перетворення в перевагу в царині поінформованості і прийняття рішень та управління поведінкою протидіючої сторони. Інформаційна перевага є фактором забезпечення мети інформаційної боротьби. Вона не може бути досягнута на всіх напрямках інформаційної боротьби. Навіть найбільш розвинена в інформаційному плані країна, якою сьогодні є США, не спроможна забезпечити абсолютну перевагу в інформаційній боротьбі. Тому мистецтвом є пошук і виявлення найбільш уразливих, з точки зору інформаційного впливу, місць, важливих для досягнення мети як у себе, так і у протидіючої сторони, і концентрація зусиль (сил і засобів інформаційної боротьби) з метою інформаційного захисту своїх військ і населення та інформаційного впливу на війська і населення протидіючої сторони.

Метою інформаційної боротьби у вузькому розумінні є створення сприятливих умов для успішного проведення операцій і бойових дій, ефективного застосування своїх військ (сил), озброєння і військової техніки, а також зниження ефективності застосування військ (сил) і зброї противника шляхом захоплення й утримання інформаційної переваги над противником під час підготовки й в ході воєнних (бойових) дій опосередкованим введенням протидіючої сторони в контур свого управління на інформаційному рівні. Цієї мети можна досягти, забезпечуючи перевагу над протидіючою стороною в розв'язанні *таких взаємопов'язаних комплексів завдань*:

1) цілеспрямоване добування інформації про поточну ситуацію з жорсткими вимогами до її своєчасності, якості, обсягу й темпу відновлення та оцінка на основі цієї інформації політичної (воєнно-політичної, воєнної, економічної, соціальної, екологічної тощо) ситуації. Виконання цього комплексу завдань ускладнене тим, що воно в загальному випадку здійснюється в умовах інформаційної протидії. При цьому інформація, що підлягає аналізу, характеризується невизначеністю об'єктивного й суб'єктивного походження, неповнотою за одними аспектами і надмірністю за іншими, суперечливістю, наявністю частково зруйнованої або перекрученої інформації, у тому числі і дезінформації;

2) цілеспрямований і комплексний вплив на свідомість і підсвідомість населення й особового складу, на інформаційні ресурси

на всіх фазах їх виробництва, розповсюдження й використання, а також на інші складові інформаційного середовища протидіючої (конкуруючої) сторони в інтересах нав'язування їй бажаних рішень і керування її поведінкою. Особливої ваги набуває не так руйнівний, як цілеспрямований вплив саме на зміст інформації для забезпечення своїх інтересів у різних сферах діяльності особистості, суспільства, країни. Ця проблема обумовлює потребу в дослідженні механізмів формування дезінформації, розробленні науково-методичних засад її виявлення та створення автоматизованих систем аналізу поточних ситуацій в умовах інформаційної протидії, зокрема за наявності дезінформації. У цьому комплексі завдань особливого значення набуває можливість використання інформації (інформаційних потоків) як ефективного засобу формування позитивного іміджу України на міжнародній арені, а також можливість усунення політичної, воєнно-політичної, економічної й, особливо, воєнної напруженості у відносинах з іншими країнами та в різних регіонах країни;

3) захист власних інформаційних ресурсів та інших складових інформаційного середовища, у тому числі на рівні свідомості і підсвідомості людини**,** від впливу на них протидіючої сторони. Не зменшуючи важливості виконання завдань технічного захисту інформації, спрямованого в основному на забезпечення її конфіденційності, слід підкреслити особливу значущість завдань захисту власне змісту інформації від навмисного його спотворення чи перекручення, у тому числі й завдань виявлення дезінформації. До цього комплексу входять також завдання відновлення цілісності змісту частково зруйнованої чи спотвореної інформації, у тому числі й природно-мовної текстової інформації.

Взаємопов'язаність наведених комплексів завдань інформаційної боротьби виявляється так:

– грамотне вирішення завдань першого й третього комплексів неможливе без знань про те, яким чином протидіюча сторона вирішує завдання другого комплексу;

– ефективне вирішення завдань другого комплексу неможливе без знань про сили, засоби, методи, алгоритми вирішення протидіючою стороною завдань першого і третього комплексів, а також про її знання (інформаційне уявлення) про проблемну ситуацію.

Як випливає із сформульованих завдань, *соціальними об'єктами інформаційної боротьби* є індивід (особистість), соціальні групи, суспільство та країни. *Об'єктами інформаційної боротьби* є свідомість і підсвідомість індивіда, насамперед колективна свідомість, а також інформаційні ресурси та інші складові інформаційного середовища (системи інформаційного та інформаційно-аналітичного забезпечення органів державного і відомчого управління, автоматизовані системи управління військами й озброєнням, телекомунікаційні мережі, радіо- та телестудії, компоненти інформаційного та програмного забезпечення систем озброєння й військової техніки тощо).

На рис. 3.1 наведена схема взаємозв'язку вирішення завдань інформаційної боротьби, на якій для сторони C_1 завдання формування адекватного інформаційного представлення про поточну ситуацію подані блоками 1, 2, 5–10, впливу на інформаційне представлення протидіючої сторони шляхом інформаційного впливу на складові її інформаційного середовища – блоками 11–13, захисту власного інформаційного представлення в умовах інформаційного впливу – блоками 3, 4, 6. Для сторони C_2 вирішення цих завдань має дзеркальне відображення, тому вони подані суттєвими для нашого розгляду блоками в узагальненому вигляді.

Як випливає з наведеної схеми, при вирішенні завдань першого класу особливого значення набувають завдання виявлення дезінформації і управління каналами і засобами отримання інформації з метою усунення невизначеності, неповноти і змістової несуперечливості інформації. В контексті інформаційної боротьби сутність завдання оцінки ситуації полягає в боротьбі за якісну, своєчасну, повну і достовірну інформацію, яка спрямована на формування адекватного інформаційного представлення про поточну ситуацію. При цьому інформація, що добувається, в загальному випадку характеризується невизначеністю об'єктивного і суб'єктивного походження, неповнотою за одними аспектами і надмірністю за іншими, суперечливістю, наявністю частково зруйнованої або перекрученої інформації, у тому числі і дезінформації. Остання є одним з найбільш ефективних способів нав'язування "бажаних" рішень протидіючій стороні та "управління" її

поведінкою. Адже фахівцями з оцінки ситуацій грамотно побудована дезінформація частіше сприймається за правдиву і використовується

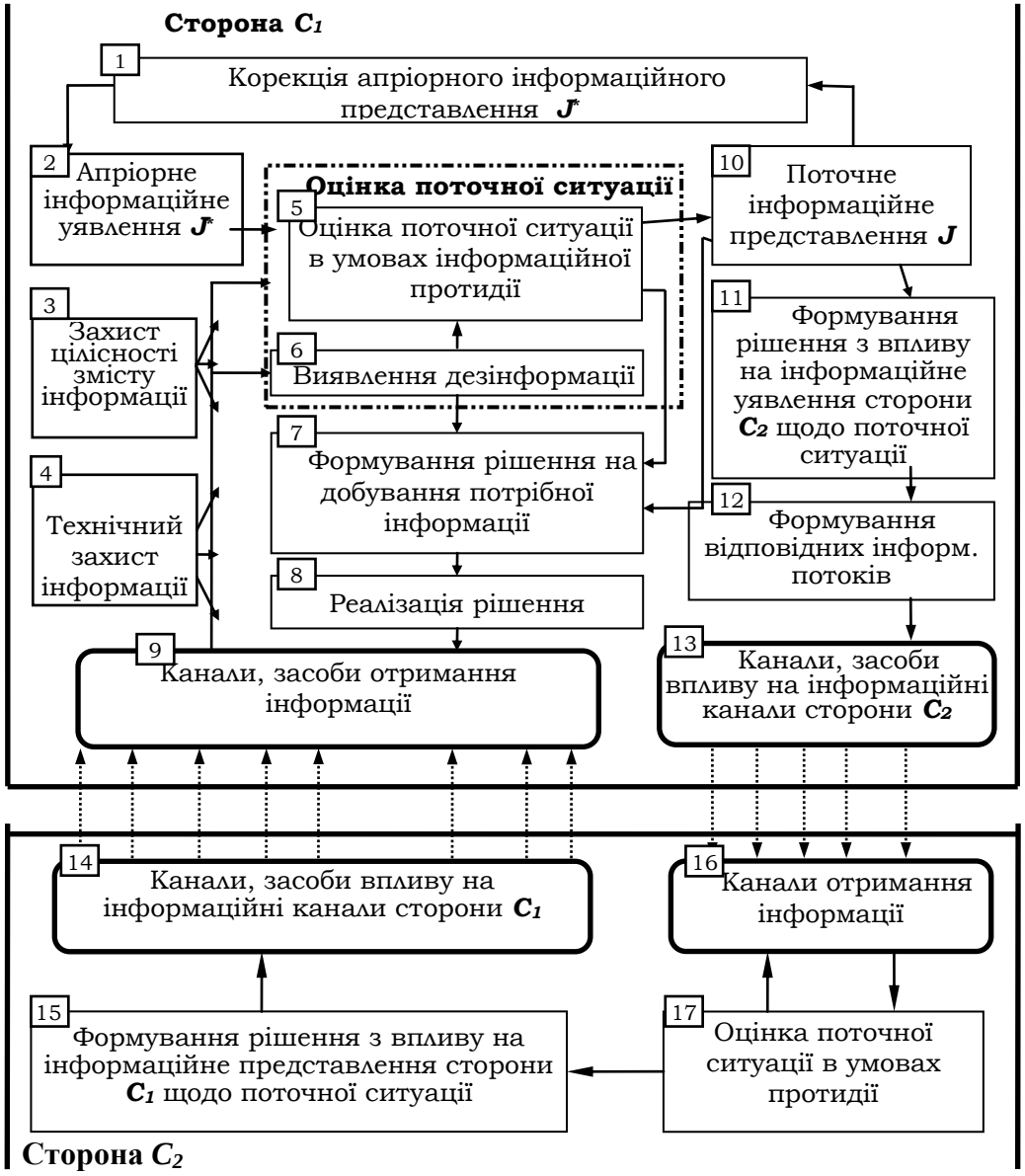

Сторона C_1
1
Корекція апріорного інформаційного представлення J^*
2
Апріорне інформаційне уявлення J^*
Оцінка поточної ситуації
5
Оцінка поточної ситуації в умовах інформаційної протидії
10
Поточне інформаційне представлення J
3
Захист цілісності змісту інформації
6
Виявлення дезінформації
11
Формування рішення з впливу на інформаційне уявлення сторони C_2 щодо поточної ситуації
4
Технічний захист інформації
7
Формування рішення на добування потрібної інформації
12
Формування відповідних інформ. потоків
8
Реалізація рішення
9
Канали, засоби отримання інформації
13
Канали, засоби впливу на інформаційні канали сторони C_2
14
Канали, засоби впливу на інформаційні канали сторони C_1
16
Канали отримання інформації
15
Формування рішення з впливу на інформаційне представлення сторони C_1 щодо поточної ситуації
17
Оцінка поточної ситуації в умовах протидії
Сторона C_2

Рис. 3.1.

При вирішенні завдань другого класу блоками 11, 12 передбачається підпорядковане єдиній цілі інформаційної боротьби формування за змістом і обсягом інформаційних потоків і їх розподілення між каналами і засобами впливу. При вирішенні завдань третього класу особливого значення набувають завдання захисту саме змісту інформації, при цьому методи виявлення дезінформації розглядаються як специфічні методи захисту інформаційного представлення про поточну ситуацію, спрямовані на забезпечення його адекватності реальному стану справ.

Особливу увагу слід звернути на інформаційну замкненість контуру "оцінка ситуації стороною C_1" $\rightarrow$ "вплив з боку сторони C_1 на інформаційне представлення сторони C_2" $\rightarrow$ "оцінка ситуації стороною C_2" $\rightarrow$ "вплив з боку сторони C_2 на інформаційне представлення сторони C_1" $\rightarrow$ "оцінка ситуації стороною C_1". Наявність цього контуру обумовлена замкненістю інформаційного процесу, в якому інформація виступає зв'язною компонентою між протидіючими сторонами, що дає підстави розглядати їх як одну систему.

Особливого значення сьогодні набуває інформаційна боротьба, яка реалізується на рівні систем управління протидіючих сторін. Основними специфічними завданнями інформаційної боротьби при цьому є:

– при забезпеченні інформаційного маскування – захисні семантичні перетворення інформації (необоротні – на основі застосування спецапаратури і оборотні – кодування і шифрування); організація маскованого інформаційного обміну в інформаційно-розподілених мережах (радіо-, провідних й ін.) систем управління; застосування широкосмугових інформаційних сигналів тощо;

– при забезпеченні інформаційного прикриття: радіоелектронний захист; блокування цінної інформації; обмеження доступу до засобів й інформаційно-програмних ресурсів систем управління; контроль потенційних загроз і каналів витоку інформації; організація технологічних процесів захищеної (вірогідної і конфіденційної) переробки інформації в системах управління; контроль і управління доступом до ресурсів систем управління;

– при забезпеченні інформаційного збору – розвідка; контррозвідка; верифікація інформації з різноманітних джерел; тестування системи управління протидіючою системою;

– при забезпеченні інформаційної протидії – радіоелектронне подавлення; інфільтрація дезінформації, включаючи інформацію для впливу на психіку персоналу протидіючої системи (інформацію психологічної боротьби) й інформацію для здійснення дезорганізації функціонування системи управління протидіючої сторони; інфільтрація комп'ютерних вірусів у систему управління протидіючої сторони; блокування інформаційних процесів в системі управління протидіючої сторони; руйнування інформаційно-програмного забезпечення АСУ протидіючої сторони.

Особливістю сучасних умов інформаційної боротьби є те, що інколи в конфліктні взаємовідносини втягуються не окремі країни, а їх коаліції або складні цілісні соціотехнічні системи, що вирішують узгоджену низку завдань в інтересах досягнення загальної цілі. Окремі елементи таких систем не є взаємно незалежними, а доповнюють і "допомагають" один одному. У цьому випадку конфліктна взаємодія протидіючих сторін набуває всіх характерних рис складного коаліційного конфлікту – зіткнення інтересів двох коаліцій, кожна з яких представлена сукупністю засобів і систем, які прагнуть до випереджувального вирішення своїх завдань, у тому числі й шляхом втручання в процес функціонування протидіючої сторони.

Аналіз сучасних поглядів дозволяє вважати, що інформаційна боротьба в цілому є комплекс взаємопов'язаних і узгоджених за цілями, місцем і часом заходів, орієнтованих на досягнення інформаційної переваги. У самому загальному формулюванні *інформаційна перевага* – це сукупність факторів, що включають можливість зміни уявлення протидіючої сторони про реальну ситуацію, можливість прогнозування наступних подій і впливу на них у своїх інтересах в умовах перешкоджаючих дій з боку іншої сторони. У цьому зв'язку *конфлікт в інформаційній боротьбі* слід розглядати як процес суперництва (і не лише антагоністичного) перешкоджаючих одна одній сторін з випереджувального досягнення інформаційної переваги. Очевидно, що результат такого суперництва багато в чому (за деякими оцінками на 60–80%) буде визначатись

спроможністю тієї чи іншої сторони до випереджувального добування відомостей про свого суперника і введення його в оману стосовно власних намірів, надійністю прогнозу обстановки, можливістю пристосування своїх дій до ситуації, що складається, в умовах реально існуючої і навмисно посиленої невизначеності.

Зважаючи на виключну важливість результатів вирішення наведених завдань, для досягнення цілей інформаційної боротьби процес протиборства протидіючих сторін, який включає сукупність їх зустрічних дій щодо випереджувального інформаційного забезпечення своїх сил і засобів та їх пристосування до поточної обстановки, доцільно виділити в самостійну складову частину конфлікту в інформаційній боротьбі, а саме в *інформаційний конфлікт*. Інформаційний конфлікт в умовах інформаційної боротьби не лише не виключає можливості активного втручання в процес добування інформації, але й багато в чому є проявом "боротьби" за формування адекватного інформаційного уявлення про обстановку (поточну ситуацію) зі свого боку і "боротьби" за нав'язування (формування) бажаного інформаційного уявлення про обстановку протидіючій стороні, а також "боротьби" за нейтралізацію протипоставлених засобів інформаційної протидії.

Перевага в інформаційній боротьбі – це один із істотних факторів позитивного результату застосування збройних сил в операціях та бойових діях. Значною мірою її можна забезпечити за рахунок повнішої автоматизації всіх аспектів і засобів інформаційної боротьби, лише підвищивши рівень "інтелектуалізації" процесів аналізу обстановки та скоротивши час прийняття рішень з оцінки поточної ситуації. Дослідження, урахування та реалізація об'єктивно існуючих закономірностей інформаційної боротьби дадуть змогу в умовах паритету активних засобів озброєння в межах оборонного характеру військової політики нашої країни отримати переваги щодо ступеня обґрунтованості рішень, які приймаються стосовно оцінки протидіючої сторони, та забезпечити випереджувальні впливи на канали добування інформації (у тому числі й нетехнічні) та інформаційні канали управління для своєчасної дезорганізації дій протидіючої сторони і нав'язування своєї волі формуванням у неї бажаного інформаційного уявлення, а також захищатися від аналогічних дій з її боку.

Наріжними поняттями інформаційної боротьби є поняття “інформаційний ресурс” та “інформаційна зброя”.

3.3. Сутність і класифікація інформаційних ресурсів

Останнім часом в наукових виданнях і офіційних джерелах все частіше зустрічається поняття “інформаційний ресурс”. Однак є різночитання цього поняття, і особливо в офіційних документах, де його семантичне значення часто звужується.

Сутність поняття *“інформаційний ресурс”* полягає в наступному. Народжується нове постіндустріальне інформаційне суспільство, в якому знання (наука) стає безпосередньою соціальною (виробничою) силою. Це досягається завдяки інформаційному, точніше інформдинамічному механізму перетворення знання в інформаційний ресурс і останнього в матеріальну силу.

“*Інформаційне суспільство* – це суспільство, структура, технічна база, людський потенціал якого пристосований для оптимального перетворення знань в інформаційний ресурс і переробки його з метою переведення із пасивних форм (книжки, статті, патенти тощо) в активні (моделі, алгоритми, програми, проекти тощо)”. Але особливе значення для активізації інформаційного потенціалу суспільства має створення сучасних баз знань. (На відміну від *баз даних*, що містять відомості про кількісні і якісні характеристики конкретних об’єктів, *бази знань* містять концептуальні, поняттєві знання, що виражені природною мовою в термінах предметної області, – знання про відповідні цим термінам класи об’єктів, їх властивості й логічні зв’язки). При переході від індустріального до інформаційного суспільства основну роль в соціальній динаміці починають відігравати соціальні чинники і сфера інформаційного виробництва в цілому, тобто *інформаційна динаміка* (перехід знань в силу починає визначати весь процес соціального розвитку). Наука (нові знання) стають соціальною силою, втілюючись у практичний досвід широких мас, а також матеріалізуючись у новій техніці, технологіях, організаційних системах, продуктах і послугах.

Ідеться про інформаційне коректувальне супроводження матеріально-енергетичних (трудових) процесів у суспільстві. Саме на

ції стадії інформаційного циклу зароджуються основні потоки евристичної інформації, яка потребує обробки й використання. Що стосується неповних інформаційних циклів, які охоплюють лише стадії зв'язку, збирання даних, діагностики, інформування, то вони стають дійсно зрозумілими лише при співвідношенні з повним інформдинамічним процесом (циклом). *Інформація* як повідомлення деяких відомостей не має самостійної цінності. Її значення для одержувача визначається приростом його знань, співвіднесених з певною метою, або, якщо говорити про кінцевий інформаційний результат, величиною зниження ентропії об'єкта, що розглядається. У новому інформаційному суспільстві наука виступає й безпосередньою виробничою силою. Формою безпосередньої участі знань, що виробляються наукою, у виробничому процесі є інформація, точніше інформаційний ресурс (ІР), а механізмом ефективної взаємодії науки і виробництва – інформаційний механізм. Тобто, інформаційний ресурс – це необхідна і суттєва проміжна ланка між знанням (наукою) і дією (матеріальним результатом), яку не можна залишити поза бортом теорії відтворення.

Інформаційний ресурс – інтелектуальний ресурс, фактор колективної творчості, і основна складність в розумінні його природи і функцій полягає в розкритті механізму переходу "знань в силу", способів його впливу на матеріальні фактори прогресу.

Поняття інформаційного ресурсу зароджується на шляхах об'єднання формально-логічного і когнітивного підходів. Інформаційний ресурс у своєму визначенні має дві нерозривні складові: формально-логічну (інформаційну) і семантичну (когнітивну). Перший аспект цього фундаментального поняття (формально-логічна сторона) формується в результаті узагальнення практики комп'ютеризації і розвитку інженерії знань. В основі методів використання представлення знань (перший аспект поняття ІР) лежать головним чином математична формалізація і логічна повнота. Навпаки, когнітивний підхід базується на розумінні процесу усвідомлення чого-небудь людиною, тому представленню знань у даному випадку притаманна швидше виразність, аніж математична витонченість і строгість. Отже, інформаційний ресурс можна розглядати як "симбіоз" знання й інформації (інформації у вигляді

поняттєвого знання). Розглянемо визначення понять “інформація” та “знання”.

У контексті інформаційної боротьби видається за корисне таке визначення сутності поняття інформації.

Інформація – втілені в деякій формі відомості, які відбивають з будь-яким ступенем приближення сутності об’єктів та явищ абстрактного або реального світу.

Інформація являє собою нерозривну єдність сутності й форми (in form) і не існує без носія інформації. На прикладі природно-мовного тексту сутність інформації – це зміст тексту, форма інформації – це природно-мовне подання тексту, носій інформації – це може бути папір. Той, хто передає інформацію, втілює її сутність (зміст) в певну форму (природно-мовне подання, шифроване подання тощо) і усе це фіксує на певному носії (на папері, магнітному носії, в електронній формі в ЕОМ тощо). Той, хто приймає інформацію, отримує її на носії, вилучає сутність інформації з її форми і потім працює з вилученою сутністю, втіливши її, в загальному випадку, в найбільш зручну для оперування форму (наприклад, переклавши її на мову, якою звик мислити).

Слід відрізняти поняття “зміст інформації” і “смисл інформації”. Зміст інформації – це те, про що йде мова, смисл інформації – це те, що вкладається в цю інформацію (значення, інтерпретація інформації).

Інформація має троїсту сутність: вона об’єктивно існує незалежно від нас; вона є моделлю відповідних об’єктів і процесів; вона здатна породжувати певні матеріально-енергетичні процеси.

Разом з цим розумінням інформації наведемо й інші її визначення:

1) відомості про оточуючий світ і процеси, що в ньому відбуваються, які сприймаються людиною або спеціальним обладнанням;

2) повідомлення, що інформують про положення справ, про стан чого-небудь;

3) відомості або повідомлення про оточуючий або абстрактний світ та процеси, що в ньому відбуваються.

Зупинимося на цих визначеннях інформації, звернувши увагу на те, що в першому визначенні поняття інформації ототожнюється лише з її змістом і не має значення форми подання цього змісту. При

цьому під інформацією розуміється деяка смислова одиниця, названа "відомостями". Це важливо, адже, наприклад, слово "книга" саме по собі не є інформацією незалежно від того, в якому вигляді воно подано. Фраза "Книга лежить на столі" вже являє собою певний квант інформації, який можна назвати відомістю. Причому, ця відомість може бути сформованою у свідомості однієї людини і нікому більше не бути відомою. Навпаки, друге визначення під інформацією розуміє єдність форми і змісту (повідомлення містить відомість). Слід звернути увагу ще на один момент: якщо повідомлення (наприклад про вищезгадану книгу) буде викладено японською мовою, а одержувач повідомлення цієї мови не знає, то відповідно з другим визначенням воно для цієї людини не є інформацією, бо ні про що її не "інформує". Третє визначення, з одного боку, узагальнює перші два визначення поняття інформації, а з іншого – поширює це поняття на абстрактні світи. Адже відомості про певні положення теорії відносності також є інформацією. Надалі за необхідності будемо використовувати всі три поняття. Знання, в його філософському трактуванні, – це вірне відображення дійсності в мисленні людей. Але насправді ми у своєму житті оперуємо моделлю знань про світ, рівень адекватності якої істинним (вірним) знанням є різним. Крім того, ця модель часто має суб'єктивну природу. У цьому зв'язку будемо користуватись такими визначеннями поняття "*знання*":

1) сукупність відомостей, що утворюють цілісний опис, який відповідає деякому рівню інформування про питання, предмет, проблему тощо, які описуються;

2) сукупність відомостей про закономірності проблемного середовища і змістовну інтерпретацію виразів мови і процедур ЕОМ;

3) взаємозв'язана сукупність відомостей, що утворюють цілісний опис реального чи абстрактного світу (його фрагментів) і процесів, що в ньому відбуваються;

4) інформаційне подання, що містить взаємопов'язану сукупність відомостей, які утворюють цілісний опис реального чи абстрактного світу або його фрагментів.

Визначення 3) і 4) введені із міркувань, аналогічних міркуванням, згідно з якими введене третє визначення інформації. Крім того, визначення 4) відображає те, що під знаннями можна також розуміти єдність форми й змісту знань (інформаційне подання містить

сукупність відомостей...). Але на відміну від інформаційного повідомлення, інформаційне подання може бути сформованим як у свідомості людини і не бути відомим більше нікому, так і в будь-якій іншій формі (декларативно, наприклад, в текстовій формі або у вигляді бази знань, схематично тощо).

Введемо ще одне визначення, яке буде корисне в подальшому. *Дані* – це відомості про предмети чи окремі факти і про значення їх атрибутів або характеристик.

Враховуючи введені визначення можна говорити, що *інформаційний ресурс (ІР)* – це доступні для безпосереднього використання дані і знання, відмінною і невід'ємною характеристикою яких є їх прагматична цінність, що визначається практичними потребами в їх матеріально-енергетичному уречевленні в інтересах вирішення певних практичних завдань. Інформаційний ресурс є інтелектуальним ресурсом, результатом колективної творчості, і головна складність в розумінні його природи і функцій полягає в розкритті механізму переходу "знань у силу", способів його впливу на фактори розвитку людства [8].

Поняття інформаційного ресурсу зводиться до того, що це знання з усіма атрибутами поняття "інформація" в "шеннонівському" смислі і, навпаки, це інформація з усіма атрибутами поняття "знання" в традиційно-філософському смислі слова. Можна сказати і так: інформаційний ресурс – це семантична інформація, тобто інформація у вигляді понятєвого знання. Основна особливість інформаційних процесів полягає в обов'язковій взаємодії трьох елементів: джерела, каналу зв'язку, одержувача повідомлень. Заслуга Шеннона в тому, що він перший пов'язав інформацію, точніше, інформаційну ємність сигналу із середовищем зв'язку, поставив "вагу" повідомлення в залежність від характеристик джерела, каналу і одержувача. Інформацію не можна виділити із середовища зв'язку, як сік із яблука. Якість повідомлення, його інформаційна ємність цілком визначаються середовищем. Саме по собі воно ніякої інформаційної субстанції не містить, як наприклад, дрова не містять тепла.

Щоб уникнути непорозумінь стосовно цінності інформації, важливо відзначити, що в рамках теорії Шеннона також виникає якоюсь мірою і знаходить своє вирішення проблема цінності повідомлень. Але це вирішення не в смислі визначення значущості того чи іншого

знання, важливості змісту повідомлення для конкретної людини (користувача), а в смислі цінності кодової посилки – її достовірності, релевантності, своєчасності. Важливо вийти за рамки теорії інформації Шеннона – статистичної теорії зв'язку і поставити в центр змістовий аналіз машинно-інформаційних процесів.

Основні особливості інформаційного ресурсу. На відміну від інших (матеріальних) ресурсів він практично невичерпний. При розвитку суспільства й інтенсифікації процесу використання знань їх запаси не зменшуються, а, навпаки, зростають; при використанні він не зникає, а зберігається і навіть збільшується (за рахунок конструктивної трансформації отриманих повідомлень з урахуванням досвіду, місцевих умов тощо); він не самостійний і сам по собі має лише потенційне значення, лише з'єднуючись з іншими ресурсами, він проявляється "кінетично" як рушійна сила; ефективність його використання пов'язана з ефектом похідного (повторного) виробництва знань, інформаційна взаємодія дозволяє отримати нове знання ціною значно менших витрат порівняно з витратами праці, енергії, часу на його пряме генерування; він виступає формою безпосереднього включення науки, в тому числі теоретичних досліджень, до складу виробничих сил; він виникає в результаті не просто розумової праці, а її творчої частини (а не рутинної) [3].

Особливо слід відзначити, що не всі повідомлені знання, зокрема завдяки книгам, газетам, радіопередачам, патентним описам тощо, виступають як інформаційний ресурс. Випливає нова проблема – інформативність повідомлень. Книги, патентні описи й інші повідомлення мають ще знайти своїх споживачів. Із них ще має бути вилучена інформація. Перед людством стоїть велетенська за своєю важливістю і складністю проблема: вилучити максимум інформації із накопичених за всю історію повідомлень і перетворити її в активно функціонуючий ресурс. Йдеться про перетворення книжкових описів й інших "розсіяних" знань в діючі програми й алгоритми. Це частина робіт з формування інформаційного ресурсу.

Перетворення знань в інформаційний ресурс залежить від можливостей їх кодування, розподілення й передачі. Комунікаційна система суспільства – важливіший фактор формування, накопичення і використання інформаційного ресурсу в базі знань. Може

виникнути й така парадоксальна ситуація, коли при надмірності знань суспільство буде відчувати дефіцит інформаційних ресурсів.

Можливість ураження ІР сучасної країни з використанням засобів спеціального програмно-математичного впливу (СПМВ) потребує окремого розгляду специфіки цього ресурсу й оцінки його як елемента збройної боротьби. Фахівці виділяють ряд основних якостей ІР: відновлюваність, мобільність, подільність, замінність, здатність до розвитку. Цією чи іншою мірою вони забезпечують можливість СПМВ на ІР протидіючої сторони. Разом з цим ці якості забезпечують не меншу можливість захисту від подібного впливу з боку іншої сторони. Так, практично, всі вони сприяють досягненню відомої стійкості ІР у випадку, коли його об'єкти піддадуться спеціальному впливу з боку протидіючої сторони, оскільки забезпечується можливість відновлення уражених об'єктів інформаційного ресурсу, завчасного їх резервування і, кінець кінцем, непогане виживання цих об'єктів, не дивлячись на їх досить високу уразливість, що розуміємо як сприйнятливість до будь-якого впливу, в результаті чого порушується їх функціонування.

Найвагомішими, а тому й найбільш захищеними та важкодоступними вважаються ті елементи ІР країни, які за своїм функціональним призначенням мають зберігати безперервну працездатність і (або) діяти в реальному масштабі часу. Більш уразливі електронні інформаційні системи, що відповідають вимогам звичайного життя і діяльності військ, підприємств і закладів цивільного сектора. І хоча результати впливу на них не такі радикальні, кумулятивний ефект від постійно накопичуваних наслідків приховано здійснюваного СПМВ може виражатись у великих прямих й опосередкованих втратах матеріальних та інтелектуальних ресурсів, необоротно втраченого часу.

Саме цьому захищеність ІР активними чи пасивними контрзаходами, відсутність здебільшого необоротності наслідків спеціального впливу протидіючої сторони на ІР і можливість його відновлення не знижують актуальності проблеми його захисту. Гострота цієї проблеми вважається тим більш очевидною, якщо врахувати, що деякі якості ІР сприяють розробленню й використанню засобів СПМВ. Так, наприклад, мобільність забезпечує свободу просторово-часового маневру цими засобами, а здатність до розвитку

означає збільшення їх різновиду і може викликати важко передбачувані, а тому й найнебезпечніші наслідки їх використання. Основними об'єктами СПМВ, на думку закордонних фахівців, можуть бути не лише воєнні, але й цивільні цілі, розміщені в адміністративно-промислових об'єктах. В їх числі електронні засоби безготівкових фінансових операцій, системи передачі даних, центри управління польотами цивільної авіації і навіть засоби автоматизації процедури голосування на виборчих пунктах. Важливо відзначити, що одним із можливих опосередкованих об'єктів нападу з використанням засобів СПМВ може бути і сама людина, життя якої в ряді випадків прямо пов'язане з надійним функціонуванням засобів автоматизованого управління.

Можна так *класифікувати інформаційні ресурси*.

За рівнем готовності до використання інформаційного ресурсу будемо розрізняти такі його види:

– *актуальний інформаційний ресурс* – це таке подання інформації чи знань, яке підготовлене до ефективного його використання в конкретній сфері державної, виробничої чи суспільної діяльності;

– *потенційний інформаційний ресурс* – сукупність інформації або знань, що потребують попередніх ресурсних (часу, аналізу, наукових досліджень й ін.) витрат на їх перетворення в актуальний інформаційний ресурс. Так можна стверджувати, що національні бібліотечні науково-технічні фонди містять величезний обсяг інформаційного ресурсу, який можна використати у виробничій сфері (інформаційний ресурс виробництва), науковій та освітянській сферах тощо. Однак це – потенційний ресурс, тому що в ряді випадків потрібне проведення ще достатньо значного обсягу інформаційно-аналітичної роботи, спрямованої на систематизацію, узагальнення інформації, розосередженої по чисельних, у тому числі різномовних джерелах, і приведення її до вигляду, зручного для вирішення конкретного соціального чи інженерного завдання, створення підручника чи навчального посібника (особливо з нової навчальної дисципліни) або для формування аналітичного огляду стану робіт в тій чи іншій предметній галузі, тобто роботи з формування інформаційного ресурсу у вигляді, готовому для його актуалізації. Аналогічне відбувається і в галузі прийняття рішень, в

тому числі в сфері державного управління. Наприклад, нехай для прийняття політичного рішення про позицію України щодо подій в Югославії на основі оцінки поточної воєнно-політичної ситуації в цьому регіоні і прогнозування її розвитку є вся необхідна інформація, але вона розосереджена по різноманітних інформаційних джерелах, в тому числі і закордонних. Однак для прийняття такого рішення необхідно цю інформацію зібрати докупи, систематизувати, узагальнити, структурувати, розібратися в природі суперечливості інформації про одні і ті самі події, але отриманої з різних джерел (якщо вона є), співвіднести поточну інформацію з передісторією, виявити й проаналізувати тенденції розвитку подій, викрити глибинні причинно-наслідкові, тимчасові, просторові та інші залежності в їх розвитку, нарешті привести всю доступну й наявну в розпорядженні інформацію до подання, що дозволить ефективно вирішити завдання адекватної оцінки поточної ситуації та прийняти грамотне рішення. Тобто необхідно провести аналогічну інформаційно-аналітичну роботу з формування інформаційного ресурсу конкретного завдання прийняття рішення. Слід відзначити, що інформаційний ресурс може бути потенційним для одних завдань і актуальним для інших. Але важливим є та невід'ємна якість, що характеризує інформаційний ресурс і визначає його саме як ресурс, – це його споживча цінність або корисність.

Враховуючи бурхливий темп процесу комп'ютеризації й інформатизації всіх сфер діяльності, особливо виділимо *електронні інформаційні ресурси*, під якими пропонується розуміти інформаційні ресурси, які надані в електронній формі чи в будь-якому іншому вигляді, готовому для оперування ними в машинно-технічних системах, засобах і приладах. Так програмне й інформаційне забезпечення ЕОМ, циркулюючі в АСУ й формовані за результатами обробки РЛС дані та інша інформація, що існує в електронному вигляді й використовується для вирішення конкретних завдань, є електронним інформаційним ресурсом, причому актуальним. За цим визначенням електронним інформаційним ресурсом є і сукупність сигналів, випромінюваних радіоелектронними засобами протидіючої сторони й утворюючих конкретний стан радіоелектронної обстановки. Але це потенційний електронний інформаційний ресурс, адже він, з одного боку, доступний засобам радіоелектронної розвідки

(потенційно доступний), а з іншого – його ще потрібно перетворити в актуальний інформаційний ресурс, наприклад, вирішенням завдань розпізнавання сигналів, об'єктів випромінювання тощо. Слід відзначити, що під це визначення підпадають також аудіо- і відеозаписи на будь-якому носії, а також сукупність сигналів радіо- і телеефіру. Доречно відзначити, що інформаційні ресурси можуть перетворюватися з електронного в неелектронний вигляд і навпаки.

За значущістю інформаційні ресурси поділяються на стратегічні, тактичні й оперативні.

Стратегічні інформаційні ресурси – ресурси, що забезпечують перманентний процес формування менталітету нації як найбільш значущого чинника сталого прогресивного розвитку країни. При цьому під менталітетом розуміється інтегральна характеристика свідомості й підсвідомості соціальних суб'єктів, яка визначає їх образ мислення та дій. До складу стратегічних інформаційних ресурсів мають надходити численним користувачам перетворені в легкодоступну, в тому числі і в електронну форму світоглядні, культурологічні, історичні, правові та інші розділи гуманітарних та фундаментально-природничих знань. У військовій сфері до стратегічних ІР можна віднести воєнну доктрину, закони, що регламентують воєнну діяльність, фундаментальні положення воєнної безпеки, тощо. Іншими словами, до стратегічних інформаційних ресурсів належать ресурси, що створюються і використовуються для забезпечення стратегічних цілей.

Тактичні інформаційні ресурси включають прикладні науково-технічні, економічні, екологічні, демографічні й інші знання, перетворені в ресурс і необхідні для забезпечення розв'язання в поточному періоді проблем, наприклад, поточних проблем інформаційної чи воєнної безпеки. У військовій сфері – це сукупність основних положень оперативного мистецтва і тактики родів військ, це воєнно-прикладні знання, що одержуються курсантами і слухачами військових навчальних закладів, статути і настанови тощо. Це також математичне та програмне забезпечення АСУ й інформаційних систем військового призначення.

Оперативні інформаційні ресурси – це поточна ділова, комерційна й інша довідкова інформація, що орієнтована на задоволення щоденних потреб в різних сферах діяльності. Для військової сфери –

це відомості військового характеру, що добуваються (отримуються) чи створюються під час розвідки, збору інформації, інформаційної роботи штабів та іншої інформаційної діяльності, а також інформація, що циркулює в АСУ військового призначення, по каналах взаємодії, в інформаційних системах різного рівня, в тому числі і в системах технічної розвідки, оперативні директиви, доповіді, довідки, донесення тощо.

За належністю інформаційні ресурси можуть бути: *загальнонаціональні* (фонд бібліотеки НАН України ім. Вернадського); *галузеві* (інформаційні ресурси Міністерства оборони України); *виду військ* (інформаційні ресурси Військово-Повітряних Сил); *роду військ* (інформаційні ресурси ППО Сухопутних військ); інформаційні ресурси *оперативного об'єднання* (інформаційні ресурси радіотехнічної бригади) тощо.

Інформаційні ресурси у військовій сфері включають: законодавчі, нормативні акти, настанови, статути, директиви і накази керівників різних рівнів; відомості військового характеру, які здобуваються (одержуються) або створюються в ході збору інформації, інформаційної роботи штабів й іншої інформаційної діяльності; програмне забезпечення інформаційних та інформаційно-управляючих систем тощо.

За предметною приналежністю (за призначенням) інформаційні ресурси поділяють залежно від того, для вирішення яких завдань вони залучаються. Наприклад, можна виділити *інформаційні ресурси завдань управління економікою, ІР завдань управління Збройними Силами України, ін.*.

Особливим видом інформаційного ресурсу є *інформаційні технології (ІТ)*. Інформаційні технології – це комп'ютеризовані засоби вироблення, зберігання, передачі, використання інформації у вигляді знань. "На відміну від виробничих енергостворюючих інформаційні технології (як об'єкт інформатики) належать до соціальних, знання-утворюючих технологій. Інформаційні технології й виступили новим засобом перетворення знань в інформаційний ресурс суспільства, його новий рушійний чинник, стали засобом ефективного його використання. Інформаційний ресурс став основним ресурсом людства, головною цінністю сучасної цивілізації. Але постали й складні проблеми, що стосуються ролі, механізму функціонування,

соціальних наслідків використання інформаційного ресурсу". Залежно від ступеня розвитку, можливостей і призначення інформаційні технології можна поділити на три рівні, які умовно можна назвати: зберігаючі, раціоналізуючі й утворюючі (творчі).

Зберігаючі ІТ економлять працю, матеріальні, фінансові ресурси і час, але помітно не змінюють стан і рівень функціонування самого об'єкта – підприємства, установи або окремого робітника.

Раціоналізуючі ІТ відрізняються більшою складністю й різноманітністю функцій та охоплюють не тільки стадію зв'язку, але й певною мірою стадії використання повідомлень в системі користувача.

Утворюючі технології відрізняються двома найбільш істотними особливостями комп'ютеризованих систем, що реалізують творчі ІТ:

– ці технології переробляють і використовують семантичну, змістовну інформацію;

– охоплюють весь інформаційний цикл – від матеріально-енергетичних і трудових витрат на створення інформаційних ресурсів до завершення їх використання для переведення об'єкта в новий цільовий стан.

Наведена класифікація, звичайно, неповна, потребує уточнення і розвитку, але необхідна для систематизації інформаційних ресурсів, вивчення властивостей ІР певного класу в інтересах підвищення ефективності оперування ними на всіх етапах їх життєвого циклу – створення (відновлення), безпосереднього оперування (зберігання, накопичення, розповсюдження, інтегрування, логіко-семантичної обробки тощо) й уречевлення (впровадження у всі сфери державної, соціальної і виробничої діяльності, перетворення їх в рушійну матеріально-енергетичну силу).

3.4. Інформаційна зброя – сутність механізмів дії та можливі наслідки для системи державного управління, суспільства, особистості

У результаті застосування нових інформаційних технологій набули змін не тільки засоби збройної боротьби, але й стратегія, і тактика ведення сучасних воєн, з'явилися нові концепції ведення бойових дій

в “інформаційному столітті”, що враховують нові фактори уразливості сторін. Ці нові концепції безпосередньо узгоджуються з тим, що стрімка еволюція кіберпростору може не тільки відкрити додаткові можливості якісного удосконалювання озброєння та військової техніки, але й обумовити виникнення нових проблем уразливості протиборчих сторін: у сучасних умовах більш уразлива та з воюючих сторін, що має менше інформації про поле бою, повільніше обробляє інформацію і приймає рішення з меншою оперативністю. Сьогодні конфлікт у стадію відкритого збройного зіткнення може і не перейти, а завершитися вже після етапу “інформаційного протиборства”, результатом якого стане усвідомлення однією з протиборчих сторін, що вона не може більше розраховувати на ефективне застосування своїх засобів збройної боротьби. У будь-якому випадку сторона, що краще володіє стратегією і тактикою ведення воєнних дій в інформаційному просторі (інформаційної війни), буде в сучасних умовах мати істотні переваги.

3.4.1. Інформаційна зброя – продукт нових інформаційних технологій

Розвиток інформаційних технологій істотно змінює технічні можливості систем управління військами (силами), що спричиняє активізацію досліджень в галузі практичної реалізації концепції “інформаційна війна” і розширить спектр науково-дослідних та дослідно-конструкторських робіт (НДДКР) в галузі інформаційної зброї. За оцінками американських фахівців, істотною загрозою є розширення можливості доступу ряду країн до засобів космічної розвідки (цифрових карт), що забезпечують розрізнювальну здатність п’ять метрів і менше. При такому рівні розрізнення з’являється можливість розпізнати ключові елементи інфраструктури противника і наводити на них крилаті й балістичні ракети, особливо якщо при цьому використовується глобальна навігаційна система.

Високошвидкісна передача великих масивів інформації стає найважливішим завданням при створенні сучасних систем управління, рішення якого зв’язується з розвитком космічних систем

зв'язку й широким використанням волоконно-оптичних ліній. При цьому подібні елементи інформаційної інфраструктури стають найбільш уразливими з погляду інформаційної наступальної операції.

Концентрація ресурсів у рамках обмеженої кількості елементів глобальної (локальної) інформаційної інфраструктури веде, з одного боку, до уразливості всієї системи в цілому за наявності відповідних засобів ураження. З іншого боку, можливості інформаційної інфраструктури такі, що навіть виведення з ладу великої кількості її елементів може знизити ефективність виконання критично важливих інформаційних процесів, тобто значне виведення з ладу інформаційної інфраструктури або перешкода доступу до неї можливі тільки на нетривалий проміжок часу. Цілеспрямована організація подібних ситуацій і є пріоритетним завданням при застосуванні інформаційної зброї в ході ведення наступальної інформаційної війни і досягнення інформаційної переваги над противником. Ефективна протидія такого роду діям противника визначає мету оборонної інформаційної війни.

3.4.2. Трансформація поглядів на інформаційну зброю та її використання

Засоби тиску, що отримують політики в результаті удосконалення інформаційної зброї, у майбутньому можуть досягти рівня потужності та ефективності найновіших видів зброї масового знищення.

Деякі засоби, які зараз прийнято зараховувати до інформаційної зброї, наприклад спеціальні психологічні операції, існують та активно застосовуються досить давно, інші, зокрема специфічні комп'ютерні засоби боротьби, з'явилися лише кілька років тому. Але всі ці засоби мають дещо спільне – засновані на ідеї опосередкованого впливу на матеріальний світ через світ інформаційний. А, як вважає, наприклад, О. Поздняков, "інформаційні загрози небезпечні не так самі по собі, а як каталізатор могутніх процесів у реальному світі" [2].

Відомі фахівці у цій сфері інформаційну зброю визначають як

сукупність технічних, організаційних, політичних і подібних засобів, за допомогою яких реалізуються інформаційні загрози.

Комплексно цю проблему вперше почали вивчати в США на початку 90-х років. До того часу існували досить міцні наукові традиції в галузі досліджень пропаганди, систем та засобів захисту та отримання інформації, зокрема, за допомогою технічних приладів. Але тільки в результаті остаточного утвердження системного підходу та поширення кібернетично-інформаційних методів досліджень вчені довели доцільність та необхідність комплексного розв'язання проблем застосування засобів інформаційної боротьби. Вже в 1995 році Пентагон прийняв так звану "доктрину інформаційних воєн", що разом із доктринами "ядерної", "біологічної" та інших воєн визначає сучасний погляд Міністерства оборони США на військову справу.

В основу доктрини було покладено положення футурологічної концепції А.Тофлера про третю (інформаційну) хвилю у розвитку суспільства. Стисло, але дещо спрощено, сенс цієї концепції можна сформулювати так: "головним ресурсом сучасного суспільства є інформація".

Американські фахівці вважають, що існує дев'ять основних видів інформаційної зброї, які можна об'єднати у чотири типи:

– засоби впливу на інформаційну інфраструктуру;

– засоби розвідки, отримання інформації з інформаційних, телекомунікаційних і подібних систем;

– засоби впливу на інформацію, яка обробляється в інформаційних системах, наприклад, на програмно-математичне забезпечення цих систем;

– засоби впливу на суспільну свідомість.

Відомо, що на початок 1996 року дослідження з цієї проблематики проводилися більш ніж у 30 країнах світу. У провідних державах існують спеціальні служби, основним призначенням яких є використання засобів інформаційної боротьби: у США – Агентство національної безпеки (NSA), у Великобританії – Штаб-квартира урядового зв'язку (HGC),у Німеччині – Німецька служба інформаційної безпеки (BSI) та Агентство національної безпеки Бундесверу, у Канаді – Управління безпеки зв'язку (ASC), у Росії – Федеральне агентство урядового зв'язку та інформації при Президентові РФ (ФАУЗІ).

Яскравими прикладами використання інформаційної зброї можуть бути:

– військові дії в Перській затоці;
– діяльність електронних розвідок провідних держав;
– комп'ютерна злочинність;
– останні події на Балканах, у країнах СНД та в Африці, антитерористична операція в Афганістані.

Проблема використання інформаційної зброї у Перській затоці найбільше досліджена. Нагадаємо лише те, що в цій війні вперше одну з вирішальних ролей відіграло програмно-математичне забезпечення військової техніки (РЛС, французького концерну Tompson).

Проблема комп'ютерної злочинності активно і ретельно досліджувалася в останні роки.

Звернемося, наприклад, до менш дослідженої, але не менш цікавої тематики: подій 1996–1997 р.р. у деяких європейських та африканських країнах. Ефект від використання нових методів політичної пропаганди, які були тут застосовані, дозволяє говорити про якісну трансформацію цих засобів і перетворення їх на інформаційну зброю. Це, по-перше, так звана ідея захоплення керівних висот: для здійснення контролю над усією пресою в країні треба контролювати лише 5–7 видань та 1–2 канали телебачення. Підґрунтя цього спостереження у соціологічній теорії "лідерів думок". Звичайно, тотальний контроль над ЗМІ більш бажаний, але в умовах ворожого середовища достатньо контролювати тільки найбільш відомі розважальні і аж ніяк не політичні ЗМІ. До речі, це демонструє принципово "демократичний" характер впливу, оскільки основна орієнтація в короткострокових операціях – саме на столичну молодь. Поряд з цим – спостереження про важливість контролю FM радіостанцій.

Цікавий тип інформаційної війни демонструють події в Африці та Албанії. Геноцид проти народності тутсі було спровоковано діями радіостанції, яка посідала монопольне становище в ефірі. У результаті: циклопічні масштаби подій (мільйони жертв), практична відсутність об'єктивної інформації.

Інформаційна операція в Албанії забезпечила те, що абсолютно засекречені події навколо збройного повстання жертв албанських

“МММ” фактично не викликали здивування світової громадськості. Повна поразка, якої зазнала сучасна армія в результаті наступу озброєного населення та банд, які за офіційною версією не мали централізованого керівництва, це диво з див. Але з приводу цього у світовій пресі не виникло жодних дискусій. Повна відсутність у засобах масової інформації критичного осмислення подій наводить на досить сумні висновки.

3.4.3. Засоби інформаційного впливу на соціо-технічні та технічні системи

Особливе місце в реалізації інформаційного впливу на соціальні і технічні об’єкти сьогодні посідає ЕОМ. Адже в ній здійснюються такі етапи інформаційних процесів, як прийом інформації від людини або технічних засобів, її обробка, зберігання, формування нової інформації і видача її людині або іншим технічним засобам. І в цьому плані програмно-математичне забезпечення ЕОМ можна розглядати як аналог (модель) морально-семантичного фільтра людини, якісність і розвиненість якого залежить від рівня моделювання його складових. Це дає підстави для використання розглянутого вище підходу до аналізу механізмів інформаційного вербального впливу на соціальні об’єкти стосовно впливу на програмно-математичне та інформаційне забезпечення ЕОМ, що дозволить більш коректно і виважено сформулювати вимоги до програмно-математичного та інформаційного забезпечення ЕОМ в інтересах забезпечення інформаційної безпеки задач, що на них покладені.

Сьогодні відомий широкий *клас засобів програмно-математичного впливу* на функціонування ЕОМ, що здатні порушити й паралізувати інформаційні системи та мережі й інші автоматизовані системи, які забезпечують функціонування органів управління державних і військових об’єктів, промисловості, транспорту, зв’язку, енергетики, банків й інших установ. До цього класу ЗПМВ належать “комп’ютерні віруси”, логічні бомби й інші засоби.

Крім засобів впливу на функціонування безпосередньо програмно-математичного забезпечення, існують методи та *засоби впровадження “потрібної” для іншої сторони інформації*, на основі якої формується

рішення людиною або програмно-математичним забезпеченням ЕОМ. Ефективність застосування таких засобів залежить від того, наскільки впроваджена інформація "правдоподібна" з точки зору людини або програмно-математичного забезпечення ЕОМ.

У недалекому майбутньому слід очікувати інтенсивного розвитку так званих "*семантичних вірусів*" – програм, здатних цілеспрямовано, "осмислено" модифікувати зміст природно-мовної текстової інформації. Сутність такої модифікації може полягати, наприклад, у перерозподілі на основі лінгвістичної обробки текстової інформації розділових знаків (стратити, не можна помилувати), підміні суб'єкта певного відношення на об'єкт і навпаки (вираз "сторона C_1 впливає на сторону C_2" досить модифікувати так: "сторона C_2 впливає на сторону C_1"), в заміні понять того ж класу ("південь" на "захід" або на "північ") тощо. При цьому можуть бути досить складні в змістовому плані модифікації семантики тексту. Ефективність семантичних вірусів залежить від рівня моделювання процесу розуміння людиною текстової природно-мовної інформації. Цей рівень може бути настільки високим, що дозволить наскільки якісно автоматизувати процес модифікації змісту текстів, що результат такої модифікації буде порівняним з грамотно продуманою дезінформацією.

Крім засобів впливу на програмно-математичне та інформаційне забезпечення, сьогодні існують засоби програмно-математичного впливу (ЗПМВ), що впливають безпосередньо на стан людини. Уже є повідомлення про так званий "вірус №666", що наділений спроможністю згубно впливати на психофізіологічний стан оператора ЕОМ. Цей "*вірус-убивця*" формує на екрані монітора особливу кольорову комбінацію, що занурює людину у своєрідний гіпнотичний транс і викликає у неї таке підсвідоме сприймання, яке різко змінює функціонування серцево-судинної системи аж до блокування судин головного мозку.

У зарубіжній літературі *засоби програмно-математичного впливу класифікуються за такими показниками*:

– можливість управління ними суб'єктом впливу (засоби, що управляються і неконтрольовані);

– походження (самостійні, спеціально створені або модифіковані програмні засоби, існуючі в противника);

– конкретний об'єкт впливу (вражають системні або прикладні програми, інформаційні масиви в оперативній пам'яті або на зовнішніх носіях, дезорганізують роботу технічних засобів);

– час дії (разової або тривалої дії);

– спосіб введення в дію (негайної або уповільненої дії);

– спроможність до самовідновлення ("віруси" й інші);

– цільове призначення, тобто для поразки інформаційного ресурсу або його перерозподілу.

Значний клас засобів інформаційного впливу на соціотехнічні й технічні системи складають *засоби, що засновані на випромінюванні енергії тієї чи іншої природи.* До цього класу належать засоби радіоелектронної боротьби (РЕБ), застосування яких показало їх високу ефективність.

Іншим представником цього класу є *електромагнітна зброя.* Американські експерти вважають, що вже сьогодні надто серйозну загрозу становить цей різновид інформаційної зброї. Розроблення такої зброї почалося в 80-х роках в рамках реалізації програми "Зоряні війни", що завершилася створенням гармати, яка дозволить здійснювати направлений викид високоенергетичного пучка в радіочастотному діапазоні. Така зброя серед фахівців носить назву HERF – High Energy Radio Frequency gun. Іншим типом такої зброї є EMPT – Electromagnetic Pulse Transformer bombs.

За повідомленнями засобів масової інформації, діючою і випробуваною під час реальних бойових дій в Перській затоці зброєю такого типу володіють тільки США. Але однією з її особливостей є те, що для її створення не потрібно багатомільярдних асигнувань або наявності суперсучасних технологій. Так для виготовлення найпростішого зразка такої зброї потрібно приблизно три тижні і 500 доларів (звичайно, потрібні певні знання і досвід, але в сучасному світі це не проблема). Потужність такої зброї може досягати 5–7 мегават, а далекість дії – до 8 км.

Експерти в області інформації застерігають, що завдяки малим габаритам оволодіння такою зброєю терористами або її самостійне виготовлення – лише питання часу, а збитки від виведення з ладу будь-якого великого обчислювального центру, наприклад, служби управління повітряним рухом або великого банку, незрівнянно вищі, ніж при використанні бомб або захопленні заручників.

Найстрашнішим є те, що така зброя може використовуватися для масованих атак, причому здійснювати це може терорист-одинак.

Серед перспективних напрямків створення засобів інформаційного впливу можна виділити так звану *акустичну зброю*. Випромінювання енергії певної частоти дозволяє завдавати ураження живій силі і радіоелектронним засобам противника. Бойові генератори можуть встановлюватися на морських, повітряних і космічних носіях. Перспективне їх використання на аеростатах. Випромінювання енергії безпосередньо на об'єкт ураження або створення фону "здатні перетворити дивізію противника в череду переляканих ідіотів. Люди будуть зазнавати безпричинного страху, сильного головного болю, їх дії стануть не передбачуваними". Можливе повне необоротне руйнування психіки. Акустична зброя активно розробляється і вже існує в лабораторних варіантах. Вона може бути прийнята на озброєння в ряді країн вже через 10–15 років.

Отже, інформація може бути використана як найефективніший (не силовий в традиційному смислі) засіб забезпечення національних інтересів і цілей, розв'язання проблем або протиріч у різних областях державної і суспільної діяльності.

3.4.4. Визначення, класифікація і властивості інформаційної зброї

Теоретики зараховують до цього виду зброї широкий клас прийомів і засобів інформаційного впливу на противника – від дезінформації і пропаганди до засобів радіоелектронної боротьби. Наведемо деякі найчастіше вживані в публікаціях визначення.

Інформаційна зброя: 1) це комплекс специфічних програмно-інформаційних засобів, створених для ураження інформаційного ресурсу противника;

2) це – засоби знищення, викривлення або викрадення інформаційних масивів; засоби подолання систем захисту; засоби обмеження доступу законних користувачів; засоби дезорганізації роботи технічних засобів, комп'ютерних систем;

3) це – засоби знищення, викривлення або викрадення інформаційних масивів, добування з них необхідної інформації після

подолання систем захисту, обмеження або заборони доступу до них незаконних користувачів, дезорганізації роботи технічних засобів, виведення з ладу телекомунікаційних мереж, комп'ютерних систем, усього високотехнологічного забезпечення життєдіяльності суспільства і функціонування держави;

4) під термін "інформаційна зброя" підпадають технічні або програмні засоби для забезпечення несанкціонованого доступу або, навпаки, обмеження доступу до інформаційних баз даних; порушення штатного режиму функціонування технічних засобів і програмного забезпечення, а також виведення з ладу ключових елементів інформаційної інфраструктури окремої держави або навіть регіону.

У деяких джерелах відзначається, що сутність інформаційної зброї полягає в розвитку інформаційних технологій, що забезпечують можливість системам (індивідам, суспільним або політичним угрупованням, державам) з більш високим рівнем інформатизації управляти системами з відносно низьким рівнем інформатизації, спрямовуючи їх діяльність у своїх інтересах під постійним інформаційним контролем. В інших джерелах відзначається, що сутність "інформаційної зброї" полягає у впливові на інформаційні потоки систем управління не тільки військового, але і державного призначення з метою порушення сталості управління.

Наведені визначення сутності інформаційної зброї відбивають окремі (часткові), хоча і суттєві, характерні для неї сфери застосування і завдання, що вирішуються за її допомогою. Наведемо наступне визначення зброї (в традиційному розумінні): це – "прилади і засоби, що призначені для поразки противника у збройній боротьбі. Як правило, складаються із засобів ураження і засобів їх доставки до цілі". Із цього визначення випливає призначення та склад певних засобів, що дають підстави кваліфікувати їх як зброю. Спробуємо підійти до визначення поняття "інформаційна зброя", виходячи із системних позицій.

Численні публікації результатів воєнно-теоретичних досліджень і воєнна практика показують, що до основних реальних об'єктів деструктивного інформаційного впливу, які в сукупності складають у даний час інформаційно-стратегічний ресурс, можна зарахувати такі:

– людино-машинні системи управління (ергатичні системи) різного державного (воєнного) рівня, включаючи канали інформаційного обміну і телекомунікації;

– середовище обміну інформацією;

– засоби збору (одержання), обробки, збереження і доставки інформації, основу яких складають електронно-обчислювальні і радіотехнічні системи з відповідними видами забезпечення (інформаційним, програмним, лінгвістичним тощо);

– інформація обмеженого поширення (ІОП), тобто інформація, що становить державну, комерційну й особисту таємницю, включаючи її носії, системи і засоби захисту;

– суспільство, персонал ергасистем і людину як "інформаційного діяча" (носія певного світогляду, політичних поглядів і моральних цінностей; творця і користувача інформаційної бази ергасистем, елемента прийняття управлінських рішень і т.д.).

У загальнотеоретичному значенні під *"інформаційною зброєю"* розуміється сукупність засобів, призначених для враження і знищення інформаційних систем (ергасистем, інформаційних діячів, інформаційних технологій тощо) у ході інформаційної боротьби (війни).

У цьому контексті *інформаційною* називається *система*, у якій утворюючі її елементи й їх відношення (зв'язки) є інформаційними. Така система може розглядатися як ансамбль трьох системно-інформаційних компонентів: структури (способу внутрішньої організації елементів і зв'язків), алгоритмів (які реалізують функції опрацювання інформації – рецепції, інтерпретації і комунікації) і мови подання елементів та їх взаємодії. Тоді засоби для ураження і знищення інформаційної системи шляхом деструктивних впливів на виділені компоненти, як пропонується в [9], можна об'єднати в три відповідні групи, які являють собою три роди "інформаційної зброї", а саме:

– "організаційна (протиорганізаційна) зброя" (засоби і способи дезорганізації, ураження і знищення структури інформаційних систем, деструктивні технології оргуправління й ін.);

– "алгоритмічна (протиалгоритмічна) зброя" (засоби і способи дезорієнтації інформаційних діячів, ураження і знищення технологій і

алгоритмів функціонування систем, алгоритми деструктивних дій й ін.);

– “лінгвістична (протилінгвістична) зброя” (засоби і способи дезінформації і дезорієнтації інформаційних діячів, ураження і знищення алгоритмів, неоднозначні мовні одиниці, суперечливі літеро-цифрові алфавіти й ін.).

Зважаючи на велике розмаїття засобів інформаційного впливу, реалізованих ними механізмів, методів, способів впливу не ставиться завдання повної і детальної класифікації існуючої інформаційної зброї. Наведені вище її класи можна розглядати як ілюстративні приклади, що відбивають лише частку існуючого парку інформаційної зброї. Тим більше, що в наукових виданнях з’являються все нові і нові види інформаційної зброї, наприклад, з такими екзотичними назвами, як “організаційна зброя”, “інтелектуальна зброя” тощо. Незважаючи на те, що під цим розуміється реалізація інформаційного впливу того чи іншого характеру, інколи виникає сумнів у правомірності подібного найменування зброї. Частіше такі назви інформаційної зброї відбивають не її сутність, а данину моді. Тому, виходячи з аналізу існуючих засобів інформаційного впливу та природи інформаційних процесів, що застосовуються в якості зброї, пропонується така *класифікаційна основа інформаційної зброї* [6, 7]:

1) за метою застосування – зброя для цілеспрямованого формування складових морально-семантичного фільтра соціальних об’єктів (системи цінностей, пріоритетів, системи інтересів тощо); зброя для нав’язування протидіючій стороні бажаних рішень і поведінки; зброя для ускладнення умов прийняття рішень протидіючою стороною; зброя для зриву функціонування технічних та соціотехнічних систем (автоматизованих систем управління; інформаційних та інформаційно-керуючих систем тощо); зброя для добування інформації про протидіючу сторону тощо;

2) за об’єктами впливу – зброя впливу на соціосистеми (людина, соціальні групи, суспільство, країни); зброя впливу на соціотехнічні системи (інформаційні та інформаційно-керуючі системи, автоматизовані системи управління, Internet тощо); зброя впливу на технічні системи (системи управління технологічними лініями, загальносистемне програмне забезпечення, перехоплення управління

безпілотними засобами ураження тощо); зброя впливу на інші об'єкти інформаційної інфраструктури;

3) за призначенням – наступальна, оборонна;

4) за масштабом впливу – зброя індивідуального, групового і масового ураження; зброя одно- і багатоцільова, універсальна;

5) за типом носіїв – інформаційно-духовна зброя (ідеології, релігії, культури); інформаційно-психологічна зброя (пропаганда, наклеп, засоби зомбування); інформаційно-фізична зброя (фармакологічні, електронні, енергетичні засоби); інформаційно-ментальна зброя (слово-, мисле-, числоформи);

6) за механізмами реалізації впливу – зброя, що базується на реалізації механізмів вербального впливу на людину та соціосистеми; зброя, що базується на реалізації механізмів невербального впливу на людину та соціосистеми; зброя, що базується на реалізації механізмів впливу на функціонування математично-програмного забезпечення ЕОМ; зброя, що базується на реалізації механізмів випромінювання енергії різної природи;

7) за реалізованими методами впливу – зброя, що базується на реалізації методів інтелектуального характеру (методи дезінформування, нейролінгвістичного програмування, рефлексивного управління, ін.); зброя, що базується на реалізації методів психологічного впливу на людину, суспільство; зброя, що базується на реалізації методів психофізіологічного впливу на людину, суспільство; зброя, що заснована на реалізації методів технічного характеру;

8) за характером впливу на інформацію та інформаційні процеси – зброя руйнуючого характеру; зброя спотворюючого характеру; зброя модифікуючого характеру;

9) за масштабом вирішуваних бойових завдань – стратегічна зброя; оперативно-тактична зброя; тактична зброя;

10) за терміном дії – зброя короткострокової і довгострокової дії;

11) за радіусом дії – зброя ближньої і дальньої дії.

Запропонована класифікаційна основа інформаційної зброї не може претендувати на вичерпність, але її корисність полягає уже в тому, що вона може бути використаною для вирішення, наприклад, таких завдань:

– вибір засобів і методів інформаційного впливу за певними метою, об'єктом впливу, масштабністю, часовими характеристиками тощо;

– вибір методів і засобів забезпечення інформаційної безпеки об'єктів та завдань, що покладені на них.

Перше завдання може вирішуватися як в інтересах, наприклад, забезпечення операцій і бойових дій, так і з метою прогнозування дій противника, спрямованих на протидію реалізації наших планів на інформаційному рівні. Друге завдання полягає у визначенні методів і засобів захисту об'єктів (відповідно – завдань, що на них покладені) від негативних наслідків інформаційного впливу з боку протидіючої сторони і вирішується на основі прогнозування дій противника, спрямованих на інформаційну протидію реалізації наших планів.

Для визначення можливих видів "інформаційної зброї", які мають прикладне значення, скористаємося (з урахуванням розглянутих загальнотеоретичних уявлень) відомою феноменологічною моделлю людини як інформаційного діяча, поширивши її і на ергатичні системи. Відповідна модель найпростішої ергатичної системи включає п'ять основних підсистем-компонентів: духовний, психічний, фізичний, а також ментально-свідомий ("*Его*") і ментально-несвідомий ("*Ід*"). Тоді до видів "інформаційної зброї" можна умовно зарахувати п'ять відповідних сукупностей чи груп засобів, застосовуваних для деструктивних (дезорієнтуючих, дезінформуючих, дезорганізуючих, дестабілізуючих, руйнуючих, гнітючих й ін.) інформаційних впливів на змістові компоненти реальних ергасистем, що відповідають виділеним компонентам моделі, а саме:

– засоби масової інформації (радіо, преса, телебачення) і агітаційно-пропагандистські засоби (відеокасети, електронні підручники, енциклопедії й ін.);

– психотронні засоби (спеціальні генератори, спеціальна відеографічна і телевізійна інформація, відеозасоби типу "Віртуальна реальність" й ін.);

– електронні засоби (оптико- та радіоелектронні засоби, спеціальні передавальні пристрої і випромінювачі електромагнітних хвиль та імпульсів тощо);

– засоби СПМВ ("комп'ютерні віруси", руйнуючі програмні закладки "хробаки" й ін.);

– лінгвістичні засоби (мовні одиниці, “спеціальна” термінологія, звороти мови, що мають семантичну неоднозначність при перекладі на інші мови й ін.);

– психотропні засоби (спеціально структуровані ліки, транквілізатори, антидепресанти, галюциногени, наркотики, алкоголь тощо).

ЗМІ й агітаційно-пропагандистські засоби як вид “інформаційної зброї” масового ураження призначені для цілеспрямованого завдання інформаційного збитку, головним чином, духовно-моральному життю населення (включаючи військовослужбовців) конфронтуючої сторони і, у першу чергу, його історичній пам’яті, світогляду, моральним ідеалам з метою можливого управління її поведінкою, а також для створення перешкоди аналогічним впливам противника.

Психотропні засоби призначені для впливу на психіку людини на генному чи хромосомному рівнях: транквілізатори розривають зв’язок між інформаційно-психічними і фізичними процесами в організмі людини, галюциногени викликають психічні розлади й ін.

Розглянуті групи засобів (види) “інформаційної зброї” можуть одночасно здійснювати побічний деструктивний вплив і на інші компоненти ергасистем. Зокрема, ЗМІ впливають на психічну (наприклад, у формі “електронно-психічної атаки” на основі застосування спеціальної телевізійної інформації) і на свідому (у формі “лінгвістичної агресії” на основі застосування ненормативної лексики, сленгу, “американізмів” й ін.) компоненти свідомості.

Наведена класифікація (стосовно основного об’єкта впливу) можливих видів *“інформаційної зброї”* дозволяє визначити її (з урахуванням ієрархії рівнів у системі державного управління) як сукупність спеціальних засобів, технологій, інформації і дезінформації, застосовуваних для деструктивних впливів на менталітет населення (персоналу ергасистем, військовослужбовців) й інформаційно-технічну інфраструктуру держави.

Узагальнюючи вищенаведене, сформулюємо визначення *інформаційної зброї* – це різновид зброї, головними елементами якої є інформація, інформаційні технології (у тому числі, технології інформаційного впливу) та/або інформаційні процеси, що застосовуються в інформаційній боротьбі. Під це визначення підпадають усі засоби, що реалізують розглянуті вище механізми і

методи інформаційного впливу в інтересах забезпечення протидіючими сторонами досягнення цілей в інформаційній війні або в операціях і бойових діях при веденні традиційних війн.

Аналіз різновидів інформаційної зброї показав як надзвичайну небезпечність і різноманітність її видів, так і небезпечність і різноманітність каналів її впливу – від засобів масової інформації до методів та засобів впливу на свідомість і підсвідомість людей, що вкрай небезпечно у зв'язку з практичною відсутністю засобів контролю цих процесів. Правомірність терміну "інформаційна зброя" зумовлена властивостями інформації та можливостями її використання для досягнення успіху країнами при вирішенні своїх завдань у тій чи іншій сфері державної діяльності.

Інформаційна зброя може характеризуватись такими показниками як цілеспрямованість, вибірковість, розосередженість, масштабність впливу, досяжність, швидкість доставки, комплексність впливу на людей, технічні засоби й системи, можливість регулювання (дозування) "потужності" впливу тощо, що визначає її як зброю масового ураження.

*Інформаційній зброї притаманні такі особливості***:** атакуючий характер, універсальність, прихованість, багатоваріантність форм реалізації, радикальність впливу, псевдовибірковість, свобода просторово-часового маневру, нарешті – економічність роблять інформаційну зброю надзвичайно привабливою і небезпечною. Сутність цих особливостей проілюструємо на прикладі засобів програмно-математичного впливу:

– *універсальність* досягається як фізичним вторгненням в інформаційне поле противника, так і його блокадою ззовні. Крім того, вона зумовлена різноманітністю цілей (військових і суто цивільних), за якими можуть бути використані засоби ЗПМВ. Універсальність, нарешті, проявляється і в тому, що ці засоби поділяються на наступальні (для ураження об'єктів інформаційного ресурсу противника) й оборонні (для захисту власного інформаційного ресурсу від програмної атаки);

– *прихованість* забезпечується, наприклад, схожістю природних помилок програмування і навмисного викривлення програм. Крім того, існують різноманітні прийоми підвищення прихованості засобів СМПВ, своєрідна тактика застосування його засобів. Програмний

вірус, наприклад, має так званий “інкубаційний період”, призначений для того, щоб не можна було визначити звідки і коли він потрапив до програми. Деякі засоби ЗПМВ наділені спроможністю до самознищення. Одним з найважливіших результатів прихованості дії є можливість досягнення раптовості;

– *багатоваріантність* проявляється в широкій різноманітності форм програмної реалізації засобів спеціального впливу. Так для кожного типу програм створюється свій тип “програмного вірусу”, який може мати різноманітні модифікації;

– *радикальність дії* полягає в тому, що безпосередніми об’єктами впливу можуть бути засоби програмного й інформаційного забезпечення автоматизованих систем управління військами і зброєю найбільш високого рівня, що може фактично вивести з ладу всю сукупність керованих ними елементів;

– *псевдовибірковість* означає, що при видимому цілеспрямованому впливі засобів ЗПМВ на окремі об’єкти інформаційного ресурсу противника віддалені глобальні наслідки подібного втручання через зростаючу взаємозалежність будуть негативно відбиватися й на інформаційному ресурсі країни в цілому – суб’єкта насильства;

– *свобода просторово-часового маневру* розуміється як можливість приведення засобів ЗПМВ в дію в будь-яких умовах: за будь-яким варіантом зосередження сил і засобів впливу в той або інший момент протягом необхідного часу і по найвіддаленіших, але практично доступних об’єктах;

– *економічність* розкривається через вигідне для атакуючої сторони співвідношення витрат, необхідних на розроблення засобів програмного впливу, й одержуваний при цьому ефект, порівняний з очікуваною катастрофою для країни – об’єкта насильства.

Існуючі в даний час проблеми “інформаційної зброї” полягають, на наш погляд, по-перше, у відсутності обґрунтованих способів і форм її ефективного застосування в сфері управління, а, по-друге, у недостатньому розробленні адекватного формально-теоретичного апарату кількісно-якісного опису як самої “інформаційної зброї”, так і способів її застосування. Проте подає надію те, що спроби створення системології інформаційних відносин із загальним формалізованим математичним представленням завдань і процесів управління

інформаційним суперництвом (боротьбою) і співробітництвом сторін, а також основ загальної теорії інформаційної боротьби дозволяють запропонувати ряд раціональних теоретичних положень із виявлення проблем застосування й оцінювання ефективності "інформаційної зброї". Найбільшу практичну актуальність у даний час складає проблема визначення раціональних способів застосування "інформаційної зброї" на головному "театрі" інформаційної боротьби (війни) – у сфері інформаційної взаємодії конфронтуючих ергасистем.

Під способами застосування "інформаційної зброї" у даному випадку розуміється обраний порядок використання відповідних засобів і сил для досягнення поставлених цілей з урахуванням специфіки й умов розв'язуваних завдань інформаційної боротьби.

Власне "інформаційна зброя" застосовується в ході ведення інформаційної боротьби у таких найбільше широко відомих її видах (визначаючих основні способи й активні форми застосування "інформаційної зброї"):

– "організаційна" боротьба (наприклад, нав'язування супротивнику в рамках "культурного" інформаційного співробітництва безперспективних комп'ютерних інформаційних технологій);

– інформаційно-технологічна боротьба (суперництво в сфері "технологій" ведення розвідки і контррозвідки – від агентурної до повітряно-космічної);

– інформаційно-психологічна боротьба;

– радіоелектронна й електронна (комп'ютерна) боротьба, ін.

Звідси, з урахуванням перерахованих основних видів інформаційної боротьби (протидії) і запропонованого загального визначення поняття "інформаційна зброя" до раціональних способів і можливих форм її застосування можна зарахувати такі.

За першим видом "інформаційної зброї" – ЗМІ:

– впровадження в структури державного і військового управління так званих "агентів інформаційного впливу", що сприяють руйнуванню даних структур зсередини, прийняттю неефективних економічних програм, які гальмують розвиток озброєння і військової техніки, наприклад, у формі "культурного інформаційного співробітництва";

– пропаганда чужого способу життя (як правило, жорстокості, жадібності, аморальності, національної нетерпимості, вседозволеності тощо), перекручування історичної пам'яті і мови національної культури народу, формування "п'ятої колони" серед національної інтелігенції (яка стане підтримувати, пропагувати й проводити квазіреформи тощо);

– інфільтрація дезінформації, що впливає на менталітет (духовність, свідомість, підсвідомість і психіку) персоналу конфронтуючих ергасистем, наприклад у ході "інформаційного бою".

За другим видом "зброї" – психотронних засобах:

– створення потужних деструктивних випромінювань, які здійснюють руйнуючий (гнітючий) дистанційний вплив на психіку і зомбування персоналу ергасистем;

– інфільтрація спеціальної відеографічної інформації, яка містить компоненти враження психіки, наприклад, у формі "електронно-психічної атаки".

За третім видом "зброї" – електронних засобах:

– створення потужних електромагнітних й інших випромінювань, які руйнуюче (гнітюче) впливають на речовинні й енергоносії та середовище поширення інформації, як правило, безпосередньо перед початком бойових дій для створення "електронного шоку" ще до першого пострілу, наприклад, у формі "суперелектромагнітного імпульсу" (так, під час шестиденної арабо-ізраїльської війни 1967 року було раптове масоване застосування засобів РЕБ протягом двох годин, 1,5% тривалості активних бойових дій, а в зоні Перської затоки 1991 р. – уже протягом доби 2,5%);

– радіоелектронне придушення певних частот і систем, заборонених до використання Статутом Міжнародного союзу електрозв'язку і Регламентом радіозв'язку, наприклад, при завданні "радіоелектронно-інформаційного удару" у ході ведення бойових дій;

– інфільтрація "комп'ютерних (завантажуваних з дискет) вірусів" в ергасистеми противника і модифікація (руйнування) цінної інформації, наприклад, у формі "інформаційного співробітництва" (так під час згаданої війни в Іраці система управління його протиповітряною обороною була виведена з ладу "вірусом", що активізувався, впровадженим напередодні війни в принтери, що поставляються до Іраку, у вигляді мікросхеми);

– дистанційне руйнування інформаційно-програмного забезпечення АІУС противника за допомогою спеціальних “мережних (переданих по лініях зв’язку) вірусів” і “програмних закладок”, наприклад, у формі “віддаленої інформаційної атаки”, “дистанційного інформаційного бою” чи при завданні “електронно-інформаційного удару” у ході підготовки до початку збройного вторгнення;

– тестування АСУ противника за допомогою спеціальних інформаційно-програмних засобів;

– нейтралізація ергасистем і технічних засобів розвідки противника, наприклад, у ході проведення спеціальної “інформаційно-ударної операції”;

– інфільтрація спеціальної технологічної дезінформації, що забезпечує дезорієнтування і дезорганізацію функціонування ергасистем противника, наприклад, у ході удаваної “інформаційно-ударної операції”;

– блокування і дезорганізація інформаційних процесів в ергасистемах противника за допомогою підключення або руйнування інформаційних каналів, а також нейтралізація (блокування) дестабілізуючих інформаційних процесів, наприклад, у ході спеціальної “інформаційно-ударної операції”.

За четвертим видом “зброї” – лінгвістичних засобах: нав’язування суперечливої (двозначної) термінології, семантично неоднозначних мовних зворотів мови тощо при складанні текстів міжнародних договорів, меморандумів, угод, пактів тощо, наприклад, у ході “дружніх” переговорів “без краваток”.

За п’ятим видом “зброї” – психотропних засобах: постачання слабовільних суб’єктів конфронтуючих ергасистем спеціальними фармакологічними засобами, ліками, наркотиками тощо з метою зміни менталітету, прищеплювання їм пагубної залежності і наступного використання або морального розкладання, наприклад, у формі “гуманітарної допомоги”, “культурних контактів” тощо.

Проблема формально-кількісного опису “інформаційної зброї” полягає, насамперед, у складності обґрунтування адекватних раціональних інформаційних показників ефективності його застосування. Розроблюваний у даний час формально-теоретичний апарат інформаційної теорії ергасистем дозволяє визначити ряд деяких важливих характеристик “інформаційної зброї”. Зокрема,

перші формально-математичні результати, отримані в цьому напрямку, дозволяють кількісно оцінити ефективність застосування відповідної “інформаційної зброї”:

– при впливі на менталітет населення (персоналу ергасистем, військовослужбовців) противника – виходячи з аналізу зміни показника інформаційної продуктивності (кількості змістової інформації в одиницю часу) ергасистем різного рівня і масштабу з урахуванням їхньої інформаційно-технологічної ефективності (раціональності використання кількості структурної інформації, яка міститься в ергасистемі, що визначає інформаційні, матеріальні й енергетичні витрати на перетворення змістової інформації);

– при впливі на інформаційно-технічну інфраструктуру держави на основі аналізу зміни показника інформаційного посилення, що характеризує силу впливу на ергасистеми (відношення загальної кількості інформації, що зберігається і циркулює в ергасистемі, до кількості інформації, яка міститься у відповідних рішеннях, реалізованих в ергасистемі противника), з урахуванням інформаційної добротності, яка характеризує економічність ергасистеми (відношення загальної кількості інформації до сумарної кількості споживаної змістової і структурної інформації).

Можливий збиток від застосування “інформаційної зброї” проти ергатичних систем державного рівня – систем управління ЗС, транспортом, енергетикою й ін. може перевищити збиток від впливу зброї масового ураження, оскільки за її допомогою можна зруйнувати систему державного управління в цілому. Особливої небезпеки “інформаційна зброя” набула в даний час, коли об’єднання інформаційно-комп’ютерних і телекомунікаційних технологій забезпечило створення єдиного глобального інформаційного середовища. При цьому доступ до каналів машинного обміну інформацією й управління інформаційно-телекомунікаційними системами, у тому числі й з території інших держав, у результаті входу у світове інформаційне співтовариство (підключення до глобальних інформаційних систем Internet та ін.) створює найширші можливості для доступу до конфіденційної інформації й порушення функціонування будь-яких ергатичних систем. Протистояти цій загрозі можна за умови забезпечення тісного взаємозв’язку впровадження прогресивних НІТ із забезпеченням комплексної

інформаційної безпеки на основі використання раціональних технічних, криптографічних й організаційно-режимних засобів захисту інформації і засобів інформаційної протидії.

Найбільшу небезпеку "інформаційна зброя" складає через те, що її застосування носить знеособлений характер і легко маскується під заходи захисту, наприклад, авторських і комерційних прав фірм. А при створенні програмних продуктів великого обсягу не складає труднощів утворити зони по декілька команд, що при експлуатації програмної системи сформуються в дефект будь-якого типу. Крім того, вона дозволяє навіть вести наступальні дії анонімно, без оголошення війни.

Заборонити розроблення й використання інформаційної зброї навряд чи можливо, як це зроблено, наприклад, для хімічної або бактеріологічної зброї. Обмежити зусилля багатьох країн щодо формування єдиного глобального інформаційного простору також неможливо.

3.5. Державне і військове управління як об'єкт інформаційної боротьби

Інформаційна безпека значною мірою визначає, з одного боку, рівень захищеності і, як наслідок, стійкості основних сфер життєдіяльності суспільства (держави) по відношенню до небезпечного (дестабілізуючого, деструктивного, уразливого тощо) інформаційного впливу, а з іншого боку – інтенсивність розвитку суспільства в тій чи іншій сфері за рахунок ефективного використання накопичених людством знань. Важливо зрозуміти, що інформаційна безпека – це проблема управління знаннями. Сама по собі інформація не має реальної вартості, вона набуває її тоді, коли починає впливати на процеси управління. Перевага тези "*знати*" над тезою "*мати*" стає базовою у соціальних, політичних та економічних процесах, що дозволяє значно ефективніше використовувати знання у порівнянні з капіталом у сучасних розробках.

Розглянуті завдання інформаційної боротьби обумовлюють об'єкти впливу, а саме: інформаційні ресурси, інформаційні технології і фахівці з аналітичного опрацювання інформаційних потоків, які

безпосередньо вирішують завдання інформаційно-аналітичного забезпечення органів державного управління.

3.5.1. Напрями і механізми інформаційного впливу на систему державного управління

Вплив на інформаційні ресурси (ІР) можна організувати як за якісними, так і за кількісними показниками. Інформаційна ізоляція (інформаційний голод), або, навпаки, перевантаження, завчасно розроблені та передані тези та аргументи, дезінформація можуть суттєво впливати на процес прийняття рішень.

Вплив на кількісні показники інформаційних ресурсів в сучасних комп'ютерних мережах активно здійснюється, наприклад, шляхом "засмічування". Його метою є втягнення фахівця-аналітика у купу зайвої інформації. Сутність механізму полягає у використанні ключових понять, які за допомогою технології гіпертекстових структур виходять на семантичне поле пов'язаних понять і нарощуються великою кількістю інформації. Сюжет розгортається як у класичному детективі: інформація тримає, доки не буде вичерпаною. Як наслідок, корисної інформації дуже мало, а час, витрачений на її вивчення, знижує, а інколи і зводить нанівець ефективність праці. Яскравим прикладом служить поняття "інформаційна боротьба", яке активно мусується в Internet.

Вплив на якісні характеристики (зміст та структуру) ІР здійснюється за рахунок втілення підготовленої дезінформації, тенденційно поданої інформації, викривлення її змісту (наприклад, в процесі її передачі або обробки). Це можуть бути також різного роду комп'ютерні віруси (КВ), які спотворюють, руйнують електронні ІР.

В радянському енциклопедичному словнику дається таке визначення *дезінформації*: "Дезінформація (від дез- та інформація) – це розповсюдження викривлених або свідомо хибних відомостей для досягнення пропагандистських (в буржуазному суспільстві), воєнних (введення противника в оману) або інших цілей.". З вище наведеного визначення можна виділити наступні основні властивості дезінформації:

– процесуальний характер дезінформації. Тобто дезінформація розглядається як система заходів, що в ідеальному варіанті

забезпечує оптимальне проходження потрібних протидіючій стороні відомостей від суб`єкта до об`єкта.

– цілеспрямованість дій. Тобто підпорядкованість послідовності всіх етапів системи заходів досягненню мети, сформульованою суб`єктом.

– основу дезінформації складають викривлені, неповні та хибні відомості.

Методи розпізнавання дезінформації значною мірою залежать від методів впровадження дезінформації (іншими словами "на кожну отруту є своя протиотрута") і мають базуватися на їх дослідженні. Серед традиційних методів цілеспрямованого впровадження дезінформації можна виділити наступні:

– *Переконання.* Сутність методу полягає у побудові змісту інформаційного повідомлення таким чином, щоб його правдоподібність не викликала сумнів. Це, як правило, досягається шляхом логічного поєднання вірогідних та хибних фактів.

– *Надмірність***.** Сутність методу полягає у впровадженні дезінформації не по одному каналу (особливо це стосується стратегічної інформації), а розгалужується по декільком каналам. Як правило, для важливої стратегічної дезінформації організується витік "таємної" інформації у засоби масової інформації. Такий метод активно застосовувався американськими спецслужбами під час конфліктів у Персидській Затоці.

– *Маскування***.** Служить, як правило, для підтримки правдоподібності вербальної дезінформації (відомостей). Заходи спрямовані на імітацію певних дій та ситуацій для підтримки хибного уявлення про реальну обстановку. В сучасних умовах, при підготовці ймовірним агресором нападу суттєво зросла роль маскування, так як з'явилися нові засоби, способи та прийоми маскування, більше уваги стало приділятися їхньому розмаїттю, переконливості і безперервності протидії розвідці противника, активному введенню його в оману. Більш реальним і важливим стало не стільки "закриття" самих об'єктів розвідки, скільки дезінформування про їхнє призначення, точні координати, дійсний стан та діяльність. Найважливішим завданням є приховування строків початку, характеру та задуму дій.

Заходи з маскування та введення в оману об'єднуються єдністю цілі, спрямованої на максимальне зниження ефективності розвідки та

створення у керівництва хибного уявлення про наміри та можливості противника.

– *Підтасування***.** Цілеспрямоване укладання фактів з метою впливу на процес виводу у бажаному для себе напрямку. Особливість такої дезінформації полягає в тому, що в її основі лежить не хибна або викривлена інформація, а достовірна інформація, яка однобоко розкриває певні події або стан взагалі, тобто є достовірною, але неповною. Іншими словами, основою дезінформації виступає не змістовна суперечність відомостей, а хибність їх логічного подання.

Доволі часто цілеспрямовані заходи щодо впровадження дезінформації підкріплюються психологічними засобами впливу, які мають на меті усипити пильність противника, деморалізувати опір тощо. Так, наприклад, під час організації операції "Буря в пустелі" на фоні розгорнутої кампанії впровадження дезінформації засоби масової інформації пропагували силу, міцність та бойовий дух іракської армії, яка готова дати опір "роз'єднаним і некваліфікованим коаліційним силам".

Крім того, сучасні технології передачі інформації сприяють розвитку нових методів впровадження дезінформації, яку за змістом власне і не можна назвати хибною чи неповною, але за метою вона виконує ті ж самі функції, що і дезінформація.

Так, наприклад, при підготовці до раптового нападу комплекс заходів з воєнно-політичної та стратегічної дезінформації включає різні галузі:

– *політичній* – висловлювання та заяви державних та політичних діячів, дипломатичні візити на вищому рівні, пропозиції щодо поширення культурного співробітництва, про укладання пакту про ненапад, а також інші політичні акти, що свідчать про прагнення до миру та зниженню напруженості міжнародної обстановки і покращенню політичних відносин;

– *економічній* – укладання крупних і довгострокових торгівельно-економічних угод і договорів, надання значних кредитів та інше, що свідчить про прагнення до поширення торгівельно-економічних стосунків;

– *воєнній* – проголошення про плановані дії навчально-бойового характеру, маневри та навчання, під виглядом яких буде

здійснюватися розгортання угруповань збройних сил та інші заключні заходи по підготовці до нападу.

Яскравим прикладом комплексного впровадження дезінформації слугують окремі події Другої світової війни. Так, у книзі "Воспоминания и размышления" Маршал Радянського Союзу Г.К.Жуков писав: "По вказівці Гітлера, даній на нараді 3 лютого 1941 року, начальник штабу верховного головнокомандування фельдмаршал Кейтель видав 15 лютого 1941 року спеціальну "Директиву по дезінформації противника". Щоб приховати підготовку до операції по плану "Барбаросса", відділом розвідки і контррозвідки головного штаба були розроблені і здійснені багаточисельні акції по розповсюдженню хибних чуток і відомостей. Переміщення військ на Схід подавалося "у світлі найвеличнішого в історії дезінформаційного маневру з метою відволікання уваги від останніх приготувань до вторгнення в Англію".

Були надруковані в масовій кількості топографічні матеріали по Англії. У війська відряджалися перекладачі англійської мови. Готувалося "оточення" деяких районів на узбережжі протоків Ла-Манш, Па-де-Кале і Норвегії. Розповсюджувалися відомості про удаваний авіадесантний корпус. На узбережжі встановлювалися хибні ракетні батареї. У військах розповсюджувалися відомості в одному варіанті про те, що вони йдуть на відпочинок перед вторгненням в Англію, в другому – що війська будуть пропущені через радянську територію для виступу проти Індії. Щоб підкріпити версію про висадку десанту в Англію, були розроблені спеціальні операції під кодовими назвами "Акула" і "Гарпун". Пропаганда цілком спрямована на Англію і призупинила свої звичайні випади проти Радянського Союзу. В роботу включилися дипломати і т.д.".

Дезінформаційні заходи є складовою і невід'ємною частиною інформаційно-психологічного забезпечення війн та бойових дій в сучасних воєнних доктринах іноземних держав. Дезінформація з боку імовірного противника стає одним з основних стратегічних факторів реалізації політики в інформаційній сфері, який спрямований на викривлення даних щодо реальної обстановки, виключає або ускладнює об'єктивність прийняття воєнно-політичних рішень на всіх рівнях керівництва, що в решті забезпечує раптовість нападу і гарантує переваги в часі при веденні бойових дій.

Розмаїття і гнучкість методів впровадження дезінформації визначається ступенем протистояння, в якому знаходяться учасники конфлікту (протидіючі сторони), цілями які вони ставлять перед собою, об'єктами впливу, каналами передачі тощо. Ступінь протистояння протидіючих сторін визначається наявністю протиріч і проявом конфліктних ситуацій між двома сторонами.

Іноземні держави зокрема США, Німеччина, Ізраїль, Росія виділяють значні кошти для розробки програм організації дезінформації з урахуванням саме ступеня протистояння. Розробкою таких програм займаються спеціальні військові структури, що входять до складу психологічного забезпечення військових операцій. Наприклад, в США існує так зване управління по координації операцій, до складу якого входять представники ЦРУ, МО, КНШ, держдепартаменту та інших відомств. Це управління забезпечує планування, координацію та здійснення дезінформаційних акцій.

Аналіз досвіду локальних війн і воєнних конфліктів показує, що більш повно цілі дезінформації досягаються у тих випадках, коли заходи по її здійсненню проводяться комплексно і не тільки в воєнній, а й в політичній і економічній галузях, як на стратегічному, так і на оперативно-тактичному рівні. Завдяки чому вдавалося зберегти у таємниці плани розв'язання війни, дезорієнтувати противника і нав'язати йому свою волю. Причому, дії по введенню в оману противника на стратегічному рівні призначалися для збереження в таємниці планів війни в цілому, а на оперативно-тактичному – для дезорієнтації командування іншої сторони відносно положення, стану і можливих дій.

Сутність дезінформаційних заходів організованих воєнною системою іноземних держав для перелічених періодів, що відбивають ступінь протистояння, проаналізуємо на прикладах минулих локальних конфліктів.

Здійснення дезінформаційних заходів у мирний час. Цей період характеризується скритим протіканням протиріч між протидіючими сторонами. Слід зазначити, що на інформаційному рівні організація дезінформації на цьому етапі визначається багатьма факторами, а саме: можливість залучення інформаційних каналів, ступінь залежності економіки, наявність кризової ситуації в країні, проти якої застосовують дезінформацію тощо. Так, протистояння двох

спільнот: соціалістичного і капіталістичного табору після Другої світової війни, сприяло реалізації політиці "холодної війни", результатом якої в інформаційній сфері стала "залізна завіса" між двома таборами. Обмеженість інформаційного впливу безпосередньо на населення, неможливість суттєво впливати на економіку через міжнародні фінансові організації визначили особливості розробки програм втілення дезінформації.

Яскравим прикладом періоду "холодної війни" може бути інформаційне протиборство у галузі розробки космічної зброї, пов'язане з програмою "Стратегічної оборонної ініціативи" (СОІ). Дезінформаційні заходи були спрямовані на вище військово-політичне керівництво колишнього СРСР.

Основними цілями дезінформації були:

– послаблення обороноздатності Радянського Союзу через підрив економіки;

– нав'язати керівництву СРСР думку про перевагу американської воєнної науки в галузі космічної зброї;

– змусити СРСР витратити значні кошти на розробку нереальної програми.

"Початкова мета дезінформації про програму протиракетної оборони полягала в тому, щоб зашкодити Радянському Союзу отримати правдиву технологічну інформацію про найвищого ступеня експериментальний проект мала розвинутися у програму, яка б втягнула Союз у значні матеріальні витрати, в стратегію форсованого самовиснаження комуністичної імперії аж до її загибелі". Для реалізації дезінформаційної програми були сфальсифіковані експериментальні випробування. "10 червня 1984 року експериментальна ракета-перехоплювач, яка була запущена американцями у рамках проекту СОІ з атолу Квадженлейн в Тихому океані, безшумно досягла висоти 150 кілометрів, буквально рознесла вщерть боєголовку міжконтинентальної балістичної ракети "Мінітмен".

Таке повідомлення мало викликати стрес і перегляд майже всієї стратегії Радянського Союзу, але завдяки використанню комплексних методів збору, перевірки та аналізу всієї отриманої інформації керівництво СРСР було проінформовано стосовно дійсного перебігу подій у цьому питанні. Слід підкреслити, що фахівці Сполучених

Штатів при піднесенні цієї інформації дотрималися майже всіх вимог щодо успішного впровадження дезінформації і навіть провели експериментальний запуск ракети, крім того навіть американські конгресмени не були проінформовані про реальний задум цього проекту. “Щоб забезпечити видимість успіху, ми сфальсифікували випробування шляхом встановлення на ракеті-мішені радіомаяка. На ракеті-перехоплювачі встановили приймач. Влучання в ціль виглядало блискуче. Так що у Конгресу питань не виникло.”

Для доказу неймовірності втілення такої ідеї в життя керівництво Радянського Союзу виділило значні кошти на наукові розробки в галузі космічної зброї та здійснило велику кількість заходів по перевірці факту запуску та перехоплення ракети. Дезінформація була виявлена, але той факт, що Союз був змушений відволікатися від розробки основних програм та виділити додаткові (й значні) кошти у відповідь на інформацію такого роду вже підтверджував частковий успіх проведення дезінформаційної операції.

Механізм впровадження дезінформації базувався на практичній імітації успішного випробування і розгляді результатів експерименту у державних установах США, для можливого витоку цієї інформації до розвідувальних служб (СРСР та дружніх з ним держав). Цікаво, що засоби масової інформації були використані, як для підтвердження вірогідності “таємної інформації” для розвідувальних служб СРСР так і для введення в оману власного уряду.

Аналіз останніх війн і воєнних конфліктів показав, що при підготовці до раптового нападу протидіюча сторона використає певні дії, а саме:

– жорстка протидія розвідці;

– широкомасштабне маскування і викривлення розвідознак своїх заходів по підготовці, які проводяться;

– широкомасштабна імітація хибних заходів з метою введення в оману в потрібному йому напрямку відносно істинних намірів і заходів, що проводяться;

– широкомасштабні заходи по імітації, маскуванню і викривленню розвідознак призначення об’єктів і характеру їх діяльності.

Тому для підвищення об’єктивності і точності отримання даних в умовах дезінформації необхідно:

– виявляти і використовувати для оцінки обстановки як змога більшу кількість різноманітних ознак;

– комплексно використовувати ознаки, які виявлені в результаті аналізу відомостей від різного роду джерел та, які отримані з використанням різних засобів і методів;

– широко використовувати не тільки прямі, неявні, а й побічні, слабо пов‘язані ознаки з обстановкою;

– глибоко аналізувати і узагальнювати відомості про всі можливі ситуації, а не тільки явно критичні, уточнювати на цій основі інформативність ознак відносно конкретних ситуацій;

– вивчати випадки надзвичайної відсутності будь-яких ознак, а також випадки наявності одночасних суперечливих відомостей;

– використовувати кількісні методи аналізу та узагальнення відомостей, оцінки взаємозв‘язку між фактами та подіями, виявляти закономірності, визначати достовірність відомостей, об’єктивно враховувати кількість негативної та позитивної інформації стосовно обстановки, що складується у виявленій сукупності ознак;

– вивчати і використовувати при викритті дезінформації погляди противника на маскування та введення в оману, канали, способи і прийоми дезінформації.

Таким чином, розробку методів розпізнавання дезінформації у процесі добування інформації слід зосередити на таких напрямках:

– розробка методів оцінки та обґрунтування вимог до параметрів, які забезпечують (максимальний) рівень відповідності розвідувальної інформації дійсності при обмежених витратах сил та засобів на її отримання;

– забезпечення дезінформаційної стійкості системи отримання інформації при розпізнаванні ситуацій на основі аналізу поточної оперативної інформації про стан та діяльність об’єктів, спостереження в реальному масштабі часу;

– забезпечення дезінформаційної стійкості системи при прогнозуванні обстановки на базі комплексних інформаційних моделей з використанням інформації баз даних в аспектах стану та діяльності об’єктів спостереження у масштабі часу, близькому до реального.

І якщо прийняти це до уваги, то діапазон втілення дезінформації в потік інформації, що надходить, дуже об’ємний. Крім того, слід

враховувати, що ефективність дезінформації (маскування і введення в оману) забезпечується:

– розмаїттям заходів, що проводяться, способів, прийомів та засобів, які використовуються, виключенням шаблону під час проведення заходів дезінформації;

– постійністю маскування і своєчасністю проведення заходів по введенню противника в оману;

– здатністю правильно оцінити можливості зі збору інформації;

– суворим забезпеченням скритності;

– правдивістю та природністю заходів, що проводяться, логічною відповідністю їх умовам обстановки;

– гнучкістю планів маскування і введення в оману, яка дозволяє розвивати неочікуваний успіх або запобігти провалу загального плану у випадку невдач окремих заходів.

Тому, для викриття дезінформації необхідне глибоке вивчення цілей, сил та засобів, способів і прийомів маскування, каналів впровадження хибних відомостей, питань її планування і організації, умов досягнення успіху на думку ймовірного противника.

Узагальнення прикладів впровадження дезінформації, дає можливість зробити основний висновок, що головною метою будь-якої дезінформації є здійснення впливу на думку людини, як елемента загальної соціосистеми, людини, яка приймає рішення, людини, яка планує майбутні дії, людини, яка впливає на перебіг поточних подій тощо.

3.5.2. Інформаційні технології в управлінні як об'єкт інформаційної боротьби

Головною рушійною силою розвитку людської цивілізації сьогодні стає інформація та інформаційні технології. Яскраво вираженого інформаційного характеру набула військова справа. З'явилися принципово нові концепції ведення війни, які передбачають завоювання інформаційної переваги над супротивником з метою досягнення своїх політичних цілей без збройної боротьби. У воєнній літературі багатьох держав тема інформаційного протиборства стала пріоритетною.

У закордонних арміях усе більш швидкими темпами проводиться інформатизація, спрямована на впровадження засобів обчислювальної техніки та інформатики в процес управління військами і повсякденною діяльністю воєнних організацій, створення високоточної зброї, робототехнічних комплексів й інформаційної зброї. Показово, що інформатика і засоби інформатизації займають одне з перших місць серед пріоритетних напрямків робіт Управління перспективних воєнних досліджень і розробок Міністерства оборони США (ДАРПА).

Війна в Перській затоці і збройний конфлікт у Югославії наочно показали, що технологічна перевага, заснована на широкому застосуванні в системах управління військами і зброєю нових інформаційних технологій, здатна звести нанівець кількісну перевагу конфронтуючої сторони в угрупованні військ і звичайних озброєнь. Іншими словами, *інформаційна сфера і рівень розвитку інформаційних технологій стають вирішальними показниками розвиненості держави.*

Очевидно, що переорієнтація провідних країн на нові інформаційні принципи обумовлює гостру необхідність визначення нових підходів до проблем забезпечення національної безпеки в інформаційну епоху, а саме – до проблем забезпечення інформаційної безпеки. Одне з ключових місць в галузі забезпечення інформаційної безпеки, як складника національної безпеки держави, займають інформаційні технології, які можуть виступати як у якості об'єкту, так і у якості засобу інформаційної боротьби. Введемо ряд понять та визначень і розглянемо інформаційні технології як об'єкт інформаційної боротьби.

Саме поняття "технологія" досить широке і багатогранне. У вузькому розумінні *технологія* – це оформлена документально система методів, способів, прийомів, засобів автоматизації (технологічного обладнання) і регламентованого порядку їх застосування, які забезпечують отримання потрібного продукту в заданих умовах і з заданим показником якості. За своєю суттю технологія являє собою *цілеспрямовану сукупність методів і способів, які реалізують досягнення необхідного результату в конкретній галузі діяльності.* В широкому розумінні *технологія* – це цілеспрямовано сформована сукупність знань про методи здійснення

виробничих процесів, що є основою для створення, удосконалювання і використання відповідної продукції.

Реалізаційною основою будь-якої технології є виробничий процес, який не слід розуміти в енциклопедичному, безпосередньому і давно застарілому смислі. У загальному випадку *виробничий процес* – це не технічні і не механічні дії, - це уречевлена у виробництві певної продукції творча діяльність людини. Складовою частиною виробничого процесу є *технологічні процеси*, які являють собою сукупність дій, спрямованих на досягнення певного (часткового) результату у виробничому процесі. Сукупність технологічних процесів і всіх допоміжних робіт утворюють виробничий процес (див. рис. 3.2).

Розглянувши загальне поняття технології і визначивши його таким чином, можна здійснити аналіз більш часткових технологій. З огляду на тематику досліджень, зупинимося на аналізі інформаційних технологій у контексті збройної (інформаційної) боротьби. Не претендуючи на стрункість і повноту, введемо з урахуванням розглядуваної галузі наступну класифікацію технологій і ряд визначень (див. рис. 3.3).

Технології можна поділити на два основних класи – технології військового і технології цивільного призначення, серед яких, в свою чергу, необхідно виділити технології подвійного застосування і критичні технології (*критичні технології* – технології, відсутність чи не використання яких загрожує безпеці держави).

Рис. 3.2.Структура виробничого процесу

Технології військового призначення підрозділяються на *оборонні технології*, тобто технології, спрямовані на забезпечення безпеки держави від зовнішніх загроз, і технології наступального характеру.

В наведеній вище класифікації технологій особливе місце посідають інформаційні технології, які залежно від їх призначення можуть надходити до будь якого з вищезазначених класів. При цьому зазначимо, що стосовно оборонних технологій інформаційні технології виступають як об'єкт інформаційної боротьби, а в технологіях наступального характеру – як засіб інформаційної боротьби.

Ґрунтуючись на загальному визначенні технологій, введемо поняття "інформаційні технології".

Інформаційні технології: 1) це технології, які забезпечують всебічний розвиток інформаційної інфраструктури та вплив на неї;

2) це матеріалізовані на базі інформаційної інфраструктури знання в галузі створення, збору, накопичення, зберігання, обробки, розповсюдження і використання інформації.

Під *інформаційною інфраструктурою* будемо розуміти сукупність центрів, каналів і засобів створення, збору, накопичення, зберігання, обробки, розповсюдження і використання інформації.

Інформаційні технології, в свою чергу, є складовою *інформаційного середовища*, під яким будемо розуміти сукупність інформаційної інфраструктури, інформаційних технологій, інформаційних ресурсів, каналів розповсюдження інформації та інформаційних відносин.

Основними відмітними характеристиками інформаційних технологій є: гнучкість, мобільність, можливість комплексування; орієнтація на існуючі і перспективні обчислювальні системи як широкого, так і спеціального призначення; широке використання методів інформатики для автоматизації окремих фаз, етапів, технологічних операцій; забезпечення цілеспрямованої діяльності колективів фахівців, стимулювання у них творчого потенціалу; простота в оволодінні, наявність засобів підказок і навчання, а також рекомендацій щодо порядку їх впровадження і пристосування до конкретних умов. *Нові інформаційні технології* характеризуються активним використанням сучасних методів подання й обробки знань.

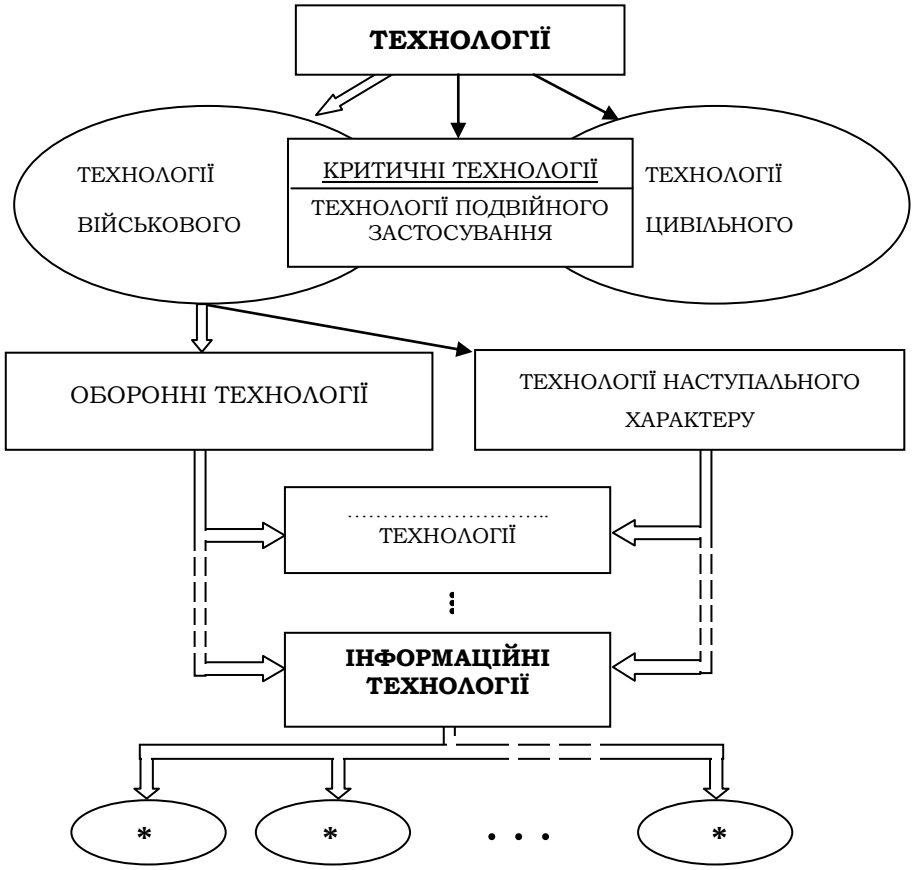


Рис. 3.3. Класифікація технологій

Ґрунтуючись на даних положеннях та визначеннях, можна класифікувати інформаційні технології за сукупністю наступних технологічних процесів: *виробництва (створення) інформації та засобів інформатизації; збору і накопичення інформації; зберігання інформації; обробки інформації; розповсюдження інформації; використання інформації.*

Така класифікація дозволяє продовжити аналіз інформаційних технологій як об'єкту інформаційної боротьби. Нагадаємо, що метою інформаційної боротьби є вирішення поставлених задач однією стороною за рахунок досягнення інформаційної переваги над протидіючою стороною. Однією з найголовніших задач інформаційної боротьби є цілеспрямований і комплексний вплив на свідомість і підсвідомість населення й особового складу, на всі фази виробництва, розповсюдження і використання інформаційних ресурсів, а також на інші складові інформаційного середовища протидіючої сторони в інтересах нав'язування їй бажаних рішень і керування її поведінкою. Звідси випливає що, при вирішенні завдання забезпечення інформаційної безпеки системи будь-якого рівня необхідно чітко розуміти, що загрози безпеці можуть бути як інформаційно-психологічними, так й інформаційно-технічними. До такого ж висновку призводить аналіз поняття інформаційних технологій, оскільки більшість інформаційних технологічних процесів містить у собі два основних фактори – технічний і людський, причому останній фактор в інформаційній сфері займає, як правило, чільне місце.

На рис. 3.4 наведена схема загроз інформаційним технологіям, представленим у вигляді сукупності технологічних процесів. Не претендуючи на повноту і бездоганність представленої моделі, коротко визначимо понятєву структуру кожної з виділених загроз стосовно до інформаційної сфери.

Організаційно-правові загрози – загрози, пов'язані з відсутністю чи недосконалістю організаційних заходів щодо забезпечення і координації дій, спрямованих на захист інформації, а також з відсутністю чи недосконалістю законодавчо-нормативної бази, яка визначає політику держави в інформаційній сфері.

Фізичні загрози – загрози, пов'язані з навмисним чи ненавмисним фізичним знищенням, руйнуванням, спотворенням засобів виробництва, збору, накопичення, зберігання, обробки, розповсюдження і використання інформації.

Психофізіологічні загрози – загрози, пов'язані з цілеспрямованим впливом на свідомість, підсвідомість і фізіологічний стан людини.

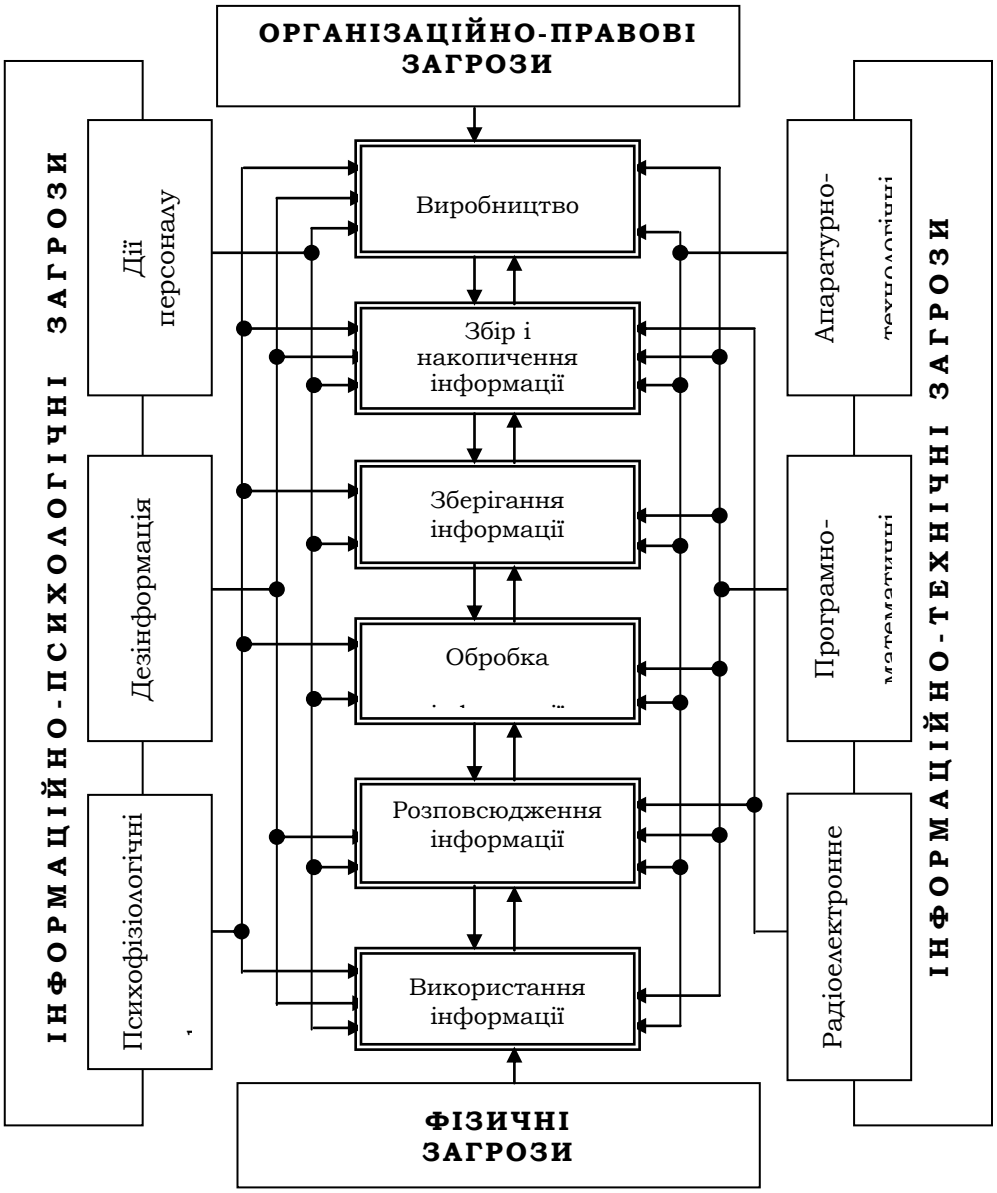


Рис. 3.4. Схема загроз інформаційним технологіям

Дії персоналу – загрози, пов'язані з індивідуальною професійною

підготовкою і психологічними особливостями сприйняття інформації особистістю.

Дезінформація – свідомо хибні відомості, які розповсюджуються з метою введення в оману.

Апаратурно-технологічні загрози – загрози, пов'язані з навмисним впровадженням в інформаційні засоби факторів негативного впливу з метою здійснення контролю над технологічним процесом, а також загрози, пов'язані з особливостями (фізичними принципами) функціонування інформаційних систем, наслідком яких може бути порушення цілісності чи захищеності інформації.

Програмно-математичні загрози – загрози, пов'язані з порушенням функціонування інформаційних засобів програмно-математичними методами і засобами.

Радіоелектронне подавлення (РЕП) – дезорганізація чи зниження ефективності функціонування об'єктів інформаційного середовища шляхом впливу на них електромагнітними й акустичними випромінюваннями.

Технологічні процеси збору і накопичення, зберігання, обробки і розповсюдження інформації є ключовими складовими інформатизації і комп'ютеризації в усіх сферах життєдіяльності суспільства і тісно взаємопов'язані між собою. Взаємозв'язок цих процесів стає все більш очевидним в міру розвитку глобальних і локальних обчислювальних мереж, технологій розподіленого зберігання й обробки інформації тощо. Найважливішим технологічним процесом ІТ є процес використання інформації, однією з найголовніших цілей якого є підтримка управлінської діяльності. Даний технологічний процес також знаходиться в тісному зв'язку з розглянутими раніше технологічними процесами. Зокрема, при вирішенні завдань управління військами (силами) першочергового значення набувають своєчасність збору й обробки інформації, яка надходить від різних джерел, знання оперативної обстановки і швидке прийняття обґрунтованих рішень на виконання різних заходів, оперативне доведення прийнятих рішень до підлеглих підрозділів і контроль реалізації цих рішень.

Такий взаємозв'язок технологічних процесів накладає жорсткі вимоги до принципів побудови системи інформаційної безпеки, оскільки реалізація інформаційних загроз у будь-якому окремо

взятому технологічному процесі може звести нанівець весь комплекс захисних заходів, реалізованих у решті процесах. Забезпечення інформаційної безпеки передбачає проведення комплексу організаційних і технічних заходів, спрямованих на виявлення та протидію різним видам інформаційних загроз. Проведемо аналіз загроз реалізації технологічних процесів (див. рис. 3.4) з метою вироблення основних рекомендацій зі складання плану захисту і розробки пропозицій щодо розвитку перспективних інформаційних технологій з урахуванням умов ведення інформаційної боротьби.

Організаційно-правові загрози - пов'язані насамперед зі здійсненням єдиної політики держави в інформаційній сфері, а точніше - з відсутністю чи недосконалістю такої політики, а також з недосконалістю організаційних заходів щодо забезпечення і, що особливо важливо, щодо координації дій, спрямованих на захист інформації і нейтралізацію дій протиборчої сторони по викраденню, знищенню, перекручуванню, фальсифікації достовірної інформації, а також дій по розповсюдженню і впровадженню дезінформації й психофізіологічному впливу в ході ведення інформаційної боротьби.

Основними факторами, які сприяють реалізації організаційно-правових загроз в галузі інформаційних технологій, є:

– недосконалість законодавчих актів, які регламентують стан і удосконалювання основних технологічних процесів ІТ;

– відсутність належного контролю з боку правоохоронних і спеціальних органів за виконанням законодавства в інформаційній сфері;

– відсутність координації зусиль основних державних структур з питань ведення інформаційної боротьби.

Наслідки реалізації організаційно-правових загроз можуть бути дуже серйозними, починаючи від витоку, перекручування і знищення інформації на будь-якій стадії виробничого процесу і закінчуючи нав'язуванням власних інформаційних технологій однією стороною з метою гальмування розвитку нових ІТ або забезпечення контролю над інфраструктурою та інформаційним простором іншої сторони.

Крім того, нав'язування (використання) імпортних інформаційних технологій може стати причиною реалізації іншого виду інформаційних загроз - *апаратурно-технологічних*. Можна виділити два класи проявів цих загроз. Перший клас пов'язаний з навмисним

впровадженням в об'єкти інформаційної інфраструктури спеціальних апаратних закладок, що контролюють чи порушують роботу інформаційних систем у відповідальні моменти. З урахуванням стрімкого розвитку засобів і методів інформаційної боротьби необхідно постійно мати на увазі, що, при наданні будь-якого виду матеріально-технічної і технологічної допомоги, іноземні держави-виробники керуються своїми власними інтересами з урахуванням "невідомого" майбутнього у відносинах з тією чи іншою державою.

Другий клас проявів апаратурно-технологічних загроз ґрунтується на наявності каналів витоку інформації, носіями якої є поля і сигнали, що утворюються в результаті функціонування різних технічних засобів розповсюдження, обробки, зберігання, відображення інформації і допоміжних технічних засобів і систем.

Основними причинами реалізації апаратурно-технологічних загроз є:

– відсутність сучасного комп'ютерного і телекомунікаційного устаткування вітчизняного виробництва;

– використання не сертифікованих імпортних інформаційних засобів і комплектуючих;

– відсутність чи недосконалість власних засобів технічного захисту інформації.

Наслідки від реалізації апаратурно-технологічних загроз можуть зводитися до контролю над функціонуванням об'єктів інформаційної інфраструктури, аж до повного порушення їхньої працездатності, порушення вірогідності і цілісності інформації, несанкціонованого доступу до інформації та ін.

Одним з найбільш дієвих (навіть у мирний період) видів загроз є *програмно-математичні загрози.* Реалізація програмно-математичних загроз стала здійснюватися практично одночасно з виникненням і поширенням комп'ютерних технологій. В останні роки закордонні країни активізували дослідження в галузі теорії і практики застосування інформаційних впливів на комп'ютеризовані інформаційні системи, АСУ військами і зброєю, об'єкти життєзабезпечення тощо. Підвищена увага приділяється застосуванню "програмних закладок", "логічних бомб", "троянських коней" й інших програмних вірусів, здатних блокувати функціонування інформаційних систем різного рівня і призначення.

Особливе занепокоєння викликає практично стихійний розвиток і використання мережі Internet, що створює сприятливі передумови для використання її можливостей злочинними угрупованнями й іноземними спецслужбами.

Основними причинами, що сприяють реалізації програмно-математичних загроз, є:

– використання в інформаційних системах не сертифікованого і неліцензійного програмного забезпечення;

– недооцінка значущості захисту інформації і відсутність чи недосконалість технічних засобів захисту інформації від несанкціонованого доступу до об'єктів зберігання, обробки й розповсюдження інформації.

Наслідки реалізації програмно-математичних загроз можуть полягати в знищенні, модифікації чи розкритті інформації; знищенні, модифікації чи збоях в роботі програмного продукту; порушенні цілісності і доступності інформації.

Наступним видом загроз інформаційним засобам є *радіоелектронне подавлення*, яке являє собою сукупність заходів щодо енергетичного придушення об'єктів інформаційної інфраструктури чи інформаційного впливу на них шляхом постановки різноманітних перешкод з метою дезорганізації чи зриву керування військами і зброєю. Основною причиною, що сприяє спотворенню чи повній втраті інформації внаслідок РЕП, є неудосконаленість сучасних засобів захисту інформаційних систем від навмисних перешкод.

Фізичні загрози в умовах ведення інформаційної боротьби пов'язані з навмисним знищенням (у воєнній чи передвоєнний час) елементів інформаційної інфраструктури державного і військового керування методами вогневого впливу і диверсій.

Основними об'єктами реалізації фізичних загроз, з урахуванням умов ведення інформаційної боротьби, є центри теле- і радіомовлення, центри телекомунікацій і зв'язку, центри командування і управління військами, центри радіо- і радіотехнічної розвідки тощо. Наочною ілюстрацією цього є практично всі збройні конфлікти і війни останніх десятиліть, особливо дії в зоні Перської затоки і на Балканському півострові.

Основними причинами, що сприяють реалізації фізичних загроз, є:

– неефективність систем охорони й оборони ключових елементів інформаційної інфраструктури;

– недостатня увага до питань забезпечення скритності і живучості інформаційних систем (у тому числі до питань оперативного й інженерного маскування).

Наслідки реалізації фізичних загроз очевидні.

Наступний блок загроз інформаційним технологіям пов'язаний з "людським" фактором, що, як зазначалося раніше, займає в інформаційній сфері, як правило, пріоритетне місце. Це твердження не є новим. Дійсно, людина бере участь, практично у всіх фазах (виробничих процесах) створення інформаційних технологій (як, втім, і всіх інших технологій), починаючи від виробництва засобів інформатизації і закінчуючи споживанням інформації. Іншими словами, - людина є ключовим компонентом інформаційного середовища, а тому і головним акумулятором і генератором інформаційних впливів. Пріоритет людського фактора в інформаційному протиборстві підтверджується глибоким історичним минулим, коли практично були відсутні технічні засоби інформатизації і всі інформаційні технологічні процеси (у нинішньому їх розумінні) існували переважно у соціальній сфері.

В інформаційно-психологічній сфері можна виділити три види загроз інформаційним технологіям: загрози, пов'язані з дією персоналу, дезінформація і психологічні загрози.

Загрози, пов'язані з *дією персоналу*, можна поділити на ненавмисні дії персоналу (некомпетентність) і навмисні дії (наприклад, шпигунство).

Загрози, що виходять із ненавмисних дій персоналу, у свою чергу, поділяються на *професійну некомпетентність*, яка є підґрунтям алгоритмічної і технічної уразливості інформаційних систем внаслідок некомпетентних дій персоналу, і *психологічну некомпетентність*, що полягає в суб'єктивності сприйняття інформації людиною, наслідком чого може бути неправильно прийняте рішення. Некомпетентність персоналу, безумовно, становить небезпеку для всіх складових інформаційних технологій, однак, сама по собі не є результатом (чи наслідком) інформаційної боротьби, на відміну від навмисних дій щодо збору, перекручування чи знищення інформації персоналом, наприклад, внаслідок його підкупу зацікавленою стороною.

Поняття "людський фактор" акумулює в собі особистісні якості, що відбивають цілісну характеристику людини як особистості, її відмінність від інших людей. На думку фахівців, незважаючи на розмаїття і "витонченість" спеціальної техніки для отримання бажаної інформації, люди залишаються одним із самих ймовірних джерел витоку інформації. Саме людина виступає основою будь-якої інформації. При підборі персоналу необхідно враховувати ділові, професійні, моральні якості і психологічні особливості кандидатів.

Отже, серед основних причин, які сприяють реалізації загроз, пов'язаних з дією персоналу, можна виділити наступні:

– недосконалість системи підготовки фахівців і наукових кадрів в області інформаційної безпеки й інформаційної боротьби;

– незадоволеність персоналу;

– відсутність чи недосконалість системи морально-психологічного виховання персоналу;

– недооцінка в питаннях підбору кадрів.

Наслідками від реалізації загроз інформаційним технологіям, пов'язаними з діями персоналу є: знищення, крадіжка, модифікація чи розкриття інформації; знищення чи нанесення збитку програмному і математичному забезпеченню; збій у роботі чи знищення каналів зв'язку; прийняття неправильних рішень.

Однією зі складових і невід'ємних частин психологічного забезпечення воєн і бойових дій у сучасних військових доктринах іноземних держав є дезінформаційні заходи. *Дезінформація* з боку можливого супротивника стає одним зі стратегічних факторів реалізації політики в інформаційній сфері, який спрямований на перекручування даних щодо реальної обстановки, виключає чи ускладнює об'єктивність прийняття рішень на всіх рівнях управління, що, врешті-решт, забезпечує раптовість нападу і гарантує виграш у часі при веденні бойових дій чи забезпечує необхідну орієнтацію населення і керівництва держави в мирний (передвоєнний) час.

Оскільки основним об'єктом дезінформації є не хто інший як людина, а точніше прийняте людиною рішення (оскільки практично всі дії людини залежать від прийнятого нею рішення), то і до основної причини реалізації загроз, пов'язаних з дезінформацією, слід, насамперед, віднести недосконалість чи відсутність технологій, що

дозволяють підвищити обґрунтованість рішень і зменшити вплив суб'єктивних факторів на процес прийняття рішень.

Особливе місце серед загроз інформаційним технологіям в умовах ведення інформаційної боротьби посідають *психофізіологічні загрози*, які можна умовно розділити на два види: загрози, пов'язані з цілеспрямованим впливом на свідомість (психологію) людей з метою їхньої корекції в бажаному напрямку; і загрози, пов'язані з впливом на психіку (підсвідомість) і фізіологічний стан людей спеціальними засобами і видами інформаційної зброї (психотронної, акустичної, лазерної тощо).

Основними засобами першого виду загроз є різного роду пропагандистські і психологічні компанії, діяльність місцевих ЗМІ, дипломатичні методи й ін. Подібного роду способи впливу на людину не пов'язані безпосередньо з використанням воєнної сили, однак цілком можуть призвести до війни з застосуванням збройних формувань чи, навпаки, – забезпечити рішення поставлених завдань без використання засобів збройної боротьби. Цілеспрямований вплив на свідомість людей може сприяти гальмуванню духовно-культурного розвитку держави, трансформації чи підриву духовно-моральних основ нації і, в кінцевому підсумку – призвести до політичних, соціальних, збройних та інших конфліктів.

До другого виду інформаційно-психологічних загроз відносяться, як відзначалося вище, загрози, пов'язані з впливом на психіку людини спеціальними засобами і видами інформаційної зброї. Серед основних засобів такого інформаційного впливу слід зазначити, насамперед, психотронну зброю. Її дія заснована на використанні дистанційного впливу “пси-обдарованого” оператора (екстрасенса) на іншу людину з метою коректування поводження чи впливу на фізіологічні функції. Існує також можливість створення відповідних технічних приладів, наприклад, різного роду бойових психотронних пристроїв (генераторів). Зазначеного ефекту можна також досягти за допомогою акустичної зброї, здатної уражати психіку людини за рахунок випромінювання енергії певної частоти. Застосування такого виду зброї може викликати в людини безпричинний страх, сильну головну біль, її дії можуть стати непередбаченими, можливе повне і незворотне руйнування психіки. До засобів, які здійснюють вплив на підсвідомість людини, можна віднести, так званий "ефект 25 кадру",

а також більш небезпечний і вже добре відомий "вірус № 666", що згубно впливає на психологічний стан оператора ЕОМ. Цей "вірус-убивця" видає на екран особливу колірну комбінацію, що приводить людину в стан гіпнотичного трансу і викликає підсвідоме його сприйняття, що різко змінює функціонування серцево-судинної системи, аж до блокування судин головного мозку.

До основних факторів, що сприяють реалізації психофізіологічних загроз можна віднести:

– втрату чи недостатній контроль з боку держави над ЗМІ;
– зневагу методами ведення контрпропаганди;
– відсутність чи слабку реалізацію заходів і методик, що сприяють підтримці психологічного і психічного стану особистості в умовах інформаційного впливу;
– відсутність чи слабку ефективність технічних засобів захисту від психотронної та інших спеціальних видів інформаційної зброї.

Отже, проведений аналіз інформаційних загроз, каналів інформаційного впливу і можливих наслідків від реалізації загроз інформаційним технологіям в умовах ведення інформаційної боротьби дозволяє зробити висновок, що інформаційна боротьба взаємозалежна з багатьма видами забезпечення і діяльності військ. Цей взаємозв'язок визначається наявністю загальних завдань для інформаційно-психологічної боротьби й морально-психологічного забезпечення; радіоелектронної боротьби; оперативного, маскування; управління військами і зброєю; захисту від несанкціонованого доступу до об'єктів і систем управління; забезпечення безпеки інформації на об'єктах автоматизованих систем управління; боротьби в комп'ютерно-телекомунікаційних мережах.

3.5.3. Інформаційно-аналітична діяльність як фактор безпеки прийняття управлінських рішень в умовах інформаційної боротьби

Особливої уваги потребують *проблеми забезпечення безпеки прийняття рішень та їх реалізації* органами управління на інформаційному рівні, тобто інформаційної безпеки державного і військового управління. Адже поточна інформація в загальному

випадку характеризується як великими обсягами та різнорідністю, так і невизначеністю, неповнотою, може бути хибною та перекрученою, а також містити дезінформацію. Сьогодні реальна ситуація – це прийняття рішень в умовах різноманітних проявів інформаційної протидії. Від адекватності сформованого інформаційного уявлення реальної обстановки, на основі якого приймаються рішення, від адекватності оцінки поточної ситуації залежить адекватність відповідних рішень і, як наслідок, ефективність управління Збройними Силами в цілому.

Останнім часом з'явилось поняття *"інформаційного фантому в управлінні"* як у державних структурах, так і у життєво-важливих сферах державної і суспільної діяльності, у тому числі й у воєнній сфері. Його сутність полягає в тому, що сьогодні управління здійснюється майже не виходячи з кабінетів, і це об'єктивно існуючий феномен. При цьому основою для прийняття рішень є інформаційне уявлення про обстановку чи поточну ситуацію, яке формується інформаційними потоками, породженими різнорідними джерелами. Ці джерела можуть бути як підконтрольними, так і не контрольованими, тобто зміст відповідних інформаційних потоків може формуватись протидіючою стороною цілеспрямовано з метою нав'язування бажаних для неї рішень шляхом формування відповідного інформаційного уявлення. Усвідомлення цього феномена само по собі є досить продуктивним. Його осмислення дає підстави принаймні для таких стверджень:

– на сучасному етапі різко підвищується роль інформаційно-аналітичних підрозділів у прийнятті рішень;

– існують досить реальні можливості з нав'язування протидіючою стороною бажаних для неї рішень, "управління" діями наших сил і їх розвитком в бажаному для іншої сторони напрямку шляхом впливу на зміст інформаційних потоків, інформаційні ресурси та інфосферу наших автоматизованих систем. Особливо ця тенденція проявляється у воєнній сфері і вона складає сутність однієї з найвагоміших інформаційних загроз воєнній безпеці України.

З наведеного випливає *висновок*, що створення розвинених інформаційно-аналітичних систем підтримки управлінської діяльності будь-якого рівня є нагальною проблемою сьогодення, актуальність якої зумовлена зростаючою тенденцією загострення методів ведення

інформаційної боротьби у сфері державного і військового управління. *Проблеми інформаційно-аналітичного забезпечення (ІАЗ) органів державного і воєнного управління значною мірою залежать* від таких його важливих складових, як: технічна база; якісні і кількісні характеристики інформаційних ресурсів, які залучаються в процесі інформаційно-аналітичної діяльності (ІАД); стан інформаційних технологій уречевлення ІР для потреб управлінської діяльності; стан методичного забезпечення аналітичного опрацювання джерел, професійний рівень та інтелектуальний потенціал фахівців, з аналізу інформації.

Під *інформаційно-аналітичною діяльністю* будемо розуміти процес створення нового інформаційного продукту, придатного для прийняття управлінських рішень, на підставі аналізу і систематизації всієї доступної інформації.

Умови, в яких працюють фахівці, визначаються обмеженістю часу на підготовку та укладання аналітичних документів. Отже, аналітику потрібно отримати найкращу відповідь при певних обмеженнях часу і вхідних даних. Експерти Американського розвідувального співтовариства так оцінюють роботу аналітиків: "Робота аналітика - це: діяти без свідків; робити пропозиції; враховувати думку інших; оцінювати альтернативні сценарії; прогнозувати напрямки і результати; відповідати політикам; оцінювати зацікавленість власної сторони (тобто державні інтереси), бути об‘єктивним (давати свій аналіз без політичної забарвленості)"[25].

Процес обробки інформації проходить наступні етапи:

1. Етап *вивчення* інформаційного матеріалу полягає у накопиченні знань з певного питання, яке має складати сутність вихідного аналітичного документа. На цьому етапі аналітик має дати відповіді для себе на ряд проблемних питань:

Що нового в цій інформації? Які нові моменти з‘явилися в характеристиці проблеми? Чому це трапилось? Які цілі, наміри, мотивація учасників подій? Які фактори можуть впливати на ситуацію? Чи усвідомлюють ці фактори учасники подій? Чи є в них програма або стратегія для подолання або використання цих факторів? Від чого може залежати успіх або провал розвитку подій для учасників? Які можуть бути наслідки як для учасників подій, так

і для власної сторони? Як сприйметься розвиток подій іншими зацікавленими сторонами? Яких заходів можуть задіяти основні учасники подій ? Які можуть бути альтернативні сценарії розвитку подій?

Цей етап обробки повністю покладається на офіцера-аналітика. Аналітик має підготовити докладні обґрунтовані прогнози, спираючись певною мірою на свою інтуїцію та знання політичної обстановки. В обов'язки аналітика входить постійний рух далі відомостей, які є в його розпорядженні.

2. *Аналіз* поточної інформації полягає в прагматичній її оцінці щодо корисності, новизни та достовірності. Оцінка інформації на достовірність здійснюється за такими показниками: оцінка джерела інформації, оцінка офіцера-розвідника, який зібрав цю інформацію, оцінка самої інформації.

Оцінка джерела інформації включає перевірку: надійності джерела; інформаційних (розвідувальних) можливостей джерела; мотивації джерела (гроші, ідеологія тощо); загальнокультурного рівня джерела; мовні характеристики джерела; політичний, економічний рівень поданої інформації (у співставленні з попередніми показниками).

Оцінка збирача інформації включає: характеристику робітника; можливості та здібності; професійні навички; загальнокультурний і мовний рівень; де і яким чином можна перевірити збирача інформації.

Оцінка інформації включає: точність інформації; відповідність попереднім повідомленням; відповідність змісту інформації інтересам користувача; повнота (що ще потрібно знати); достовірність (на основі співставлення з попередніми оцінками щодо джерела і збирача); які висновки та питання випливають з інформації; де можна знайти додаткову інформацію.

4. *Підготовка вихідного аналітичного документа.* Основні принципи синтезу вихідного аналітичного документа: визначити загальну картину; зробити попередні висновки; побудувати логічну структуру документа; використовувати мовні конструкції відповідно стилю вихідного документа; висловлювати свої думки ясно і лаконічно (досягати ясності думки); використовувати активний залог; самостійно редагувати; знати, що потрібно замовнику; проявляти

наполегливість (досягати більш високого рівня універсальності, ніж академічний або діловий стиль).

Аналітична обробка нерегламентованих текстових документів визначається наступними особливостями інформації:

— нерегламентовані текстові документи являють собою інформаційний ресурс, який безпосередньо не є підготовленим до певної задачі;

— текстова інформація може бути поданою різними мовами;

— інформація, яка надходить для аналізу, може мати невизначеність стохастичного та суб'єктивного характеру, а також може (а переважно так воно і є) бути неповною, мати змістове протиріччя, бути перекрученою, у тому числі і навмисно (наприклад, з метою дезінформування);

— аналіз поточної ситуації в тій чи іншій сфері в багатьох випадках потребує використання добре розвинених логіко-семантичних та аналітико-обчислювальних методів обробки інформації.

Одним із вагомих показників стану захищеності інформаційно-аналітичної діяльності є використання розвинених інформаційних технологій, перш за все, технологій з аналітико-синтетичної обробки інформації, оскільки такі технології, власне, і визначають рівень уречевлення знань в суспільстві. Теоретично є дві альтернативи з розвитку інформаційних технологій: запозичення закордонних, використання власних .

Запозичені системи на перший погляд більш привабливі з таких причин:

— не треба витрачати час, та і вкладені кошти набагато менші ніж розробка власної технології;

— запозичені системи технологічно поєднані з обчислювальною технікою, на яку вже витрачені кошти.

З іншого боку, необхідно усвідомлювати, що запозичені системи є результатом вчорашньої наукової думки. Отож, поки ми витрачаємо час і кошти на засвоєння запозичених програмних систем, постачальники удосконалюють свої інформаційні технології.

Інша негативна сторона запозичених технологій криється у новій якості інформаційних ресурсів, якої вони набули в сучасних умовах. Сьогодні інформаційні ресурси є важливим не тільки стратегічним,

але й тактичним об'єктом (особливо це стосується державних структур), який неможливо не враховувати при прийнятті рішень у всіх сферах державного управління. Відомо, що "хто володіє інформацією, той володіє світом" – і це не є перебільшенням. Звичайно, що за таких умов іноземним фірмам невигідно продавати передові технології, які б сприяли найефективнішому уречевленню інформації іншою державою.

Третій негативний наслідок запозичених систем полягає у тому, що вирішуючи свої прикладні задачі в чужому технологічному середовищі, ми підпадаємо під "інформаційний ковпак" відповідної держави. Адже за таких умов легко прогнозується (якщо відомі засоби обробки інформації) результат обробки поточних інформаційних матеріалів, а звідси і відповідні рішення, які можуть бути прийняті. А це сприяє втраті інформаційного суверенітету держави та створення умов реалізації інформаційних загроз.

Отже, реальний вихід - розробка власних інформаційних технологій, які б, з одного боку, містили останні світові наукові досягнення, а з іншого боку – реально сприяли б ефективному вирішенню завдань ІАД. Треба чітко усвідомлювати, що нова інформаційна технологія не має бути простою сумою готових програмно-інформаційних систем, а результат інтегрування і узагальнення набутого досвіду.

Розглянемо концептуальні засади захисту системи інформаційно-аналітичного забезпечення, як чинника інформаційної безпеки управлінської діяльності. Об‘єктами інформаційного впливу в процесі ІАД можуть виступати: людина або комп‘ютерна система. Під інформаційним впливом будемо розуміти цілеспрямовані заходи інформаційного характеру, які спрямовані на зміну поведінки (реакції) людини або роботи комп‘ютерної системи, в інтересах протидіючої сторони. Підходи до розв‘язання проблеми захисту людини в процесі ІАД на сьогодні відсутні навіть у постановочному плані. Запропоновані концептуальні засади захисту інформаційно-аналітичного забезпечення відбивають технічні аспекти захисту саме людини (фахівця) в процесі аналітичного опрацювання нею інформаційного матеріалу. В табл. 3.1 наведені фактори впливу на ІАД.

Таблиця 3.1.

Узагальнена модель інформаційних загроз стану інформаційно-аналітичного забезпечення

№ з/п	Джерела, канали реалізації загроз	Характер прояву загроз	Заходи із захисту від загроз
1	Інформаційні технології	Занепад власних технологій обробки інформації	Розробка власної інформаційної технології
		Імпортування запозичених інформаційних технологій	
2	Інформаційні ресурси	Перевантаження інформацією	Розробка методів стиснення інформації.
		Дезінформування	
		Приховування інформації (неповнота інформації)	Розробка методів виявлення дезінформації
		Тенденційне подання інформації	Оцінка інформації на повноту
3	Свідомість людини	Суб'єктивність оцінки інформації	Автоматизація ІАД

Як вже зазначалося, на процес аналітичного опрацювання інформаційного матеріалу негативним чином можуть впливати запозичені інформаційні технології. Розробка власної інформаційної технології має задовольняти наступним вимогам: випереджувальне володіння ситуацією на основі аналізу всієї доступної інформації у порівнянні з існуючими технологіями; орієнтація на обробку знань (тобто змісту інформації), а не текстів (тобто форми інформації); орієнтація на комплексну автоматизацію всіх етапів аналітичного опрацювання інформації.

Підсистема захисту ІАЗ органів державного і військового управління має включати розвинуті методи:

1) стиснення інформаційних потоків на основі їх узагальнення з

урахуванням вимог щодо її цілісності;

2) оцінки інформації на повноту;

3) виявлення суперечливої інформації, у тому числі і дезінформації.

1. Надмірність інформації виникає за рахунок повторювання однакових фрагментів знань в різних інформаційних джерелах, а також за рахунок "засмічування" корисної інформації купою зайвої. Отже, засоби стиснення інформації мають забезпечувати:

семантичне стиснення інформації за рахунок усунення повторювальних фрагментів знань в різних джерелах;

прагматичне стиснення інформації за рахунок відкидання тих фрагментів знань, які не відповідають цільовій настанові вирішення кінцевої прикладної задачі.

2. Оцінка інформації на повноту має включати:

зовнішню оцінку інформації, яка полягає у перевірці наявності більш ніж одного джерела за певною змістовою інформацією та незалежності цих джерел;

прагматичну оцінку інформації на повноту, тобто визначення всіх необхідних даних (фрагментів) знань для вирішення певної прикладної задачі.

3. Необхідність розробки методів виявлення суперечливої інформації, в тому числі і дезінформації в інформаційному потоці обумовлена наступним. Інформаційне забезпечення не є самоціллю, воно має бути підпорядкованим завданням управління. Підпорядкованість передбачає, що як інформаційне забезпечення в цілому, так і інформаційно-аналітичне забезпечення зокрема мають бути спрямованими на підтримку всіх етапів процесу управління. Отже, системи інформаційного та інформаційно-аналітичного забезпечення мають, насамперед, задовольняти вимогам з боку завдань, які вирішуються штабами на всіх етапах управління. Існує класична схема прийняття і реалізації рішень: оцінка ситуацій і прогнозування їх розвитку, вироблення рішення, а також реалізація рішення і контроль. Якщо першим двом етапам з точки зору їх інформаційно-аналітичного забезпечення сьогодні приділяється певна увага, то третій етап – реалізація рішення в плані його інформаційно-аналітичного забезпечення вимагає свого розвитку. Тут існують проблеми оптимізаційного характеру, а саме – формування інформаційних потоків, спрямованих на забезпечення процесу

реалізації рішення, оптимальних або узгоджених за обсягом, за змістом та за просторово-часовими характеристиками. Крім того, як і всі етапи управління, так і процеси їх інформаційно-аналітичного забезпечення є цілеспрямованими і підпорядковані певній єдиній меті. І ця обставина обумовлює необхідність створення методологічної бази як взаємопов'язаної сукупності науково обґрунтованих методів організації і автоматизації інформаційно-аналітичного забезпечення всіх етапів прийняття рішень.

На кожному із зазначених етапів існують свої можливі джерела інформаційних загроз. Основними передумовами для їх прояву є "некондиційність" наявної інформації, "ущербність" її якості, а також недосконалість засобів опрацювання цієї інформації. Найбільш небезпечним є можливість наявності дезінформації. Фахівці розрізняють близько 10 видів дезінформації. Як дезінформацію розглядають не тільки цілеспрямовано сформовану хибну інформацію, але і, наприклад, інформацію, що однобічно висвітлює деякі події тощо. Для аналітика ж у великому обсязі інформаційних потоків виявити дезінформацію – вкрай складне завдання.

Існують методи виявлення деяких видів дезінформації вже на рівні аналізу природно-мовного подання інформації. Зокрема проглядаються можливості виявлення дезінформації, що проявляється в неповноті інформації, в суперечливості інформації, що надходить з різних джерел, відносно одних і тих самих подій або явищ. Існують методи виявлення дезінформації, що проявляється через особливості конкретної предметної області. Суперечливість інформації може також проявлятися в наступних аспектах:

— суперечливість опису множини фактів реальній дійсності;
— суперечливість оцінки фактів різними джерелами;
— суперечливість оцінки подальшого розгортання подій (прогнозування, побудова альтернативних сценаріїв тощо) в процесі узагальнення та інтегрування інформаційного матеріалу тощо.

Автоматизацію виявлення суперечливостей можна реалізувати на основі знання-орієнтованого підходу до створення інформаційних систем і технологій [10, 11]. Адже при цьому підході вся змістова інформація, що міститься навіть в різномовних текстових джерелах, приводиться до єдиного подання автоматично, а не так, як це

робиться сьогодні шляхом попереднього препарування вхідних текстів або їх ручного опрацювання. Вона перетворюється до деякого приведеного (уніфікованого) формалізованого подання, і вже це подання можна опрацьовувати логіко-семантичними методами з точки зору аналізу на сумісність, повноту, суперечливість тощо. Знання-орієнтований підхід дозволяє автоматизувати вирішення й інших проблем. Наприклад, сьогодні гостро стоїть проблема формування табличної статистичної інформації на основі аналізу великих потоків природно-мовної текстової інформації, що циркулює в електронному вигляді. Ця інформація також може бути суперечливою. Вирішення цієї проблеми на основі знання-орієнтованого підходу досить ефективне, причому не із значними ресурсними витратами.

З точки зору формальної теорії будь-яка неструктурована інформація (до якої відносять і природно-мовну текстову інформацію) є надмірною, неповною і суперечливою одночасно. Суперечливості в тексті можуть мати як навмисний, так і ненавмисний характер. Для системи захисту інформації важливим є питання визначення кордонів між природною суперечливістю інформації та навмисним її викривленням. За функціональним призначенням до дезінформації відносять і тенденційно подану інформацію. З формальної точки зору ця інформація не є суперечливою, але вона однобічно висвітлює певні факти (події). Тобто, формально така інформація є неповною відносно об‘єктивного опису реальної дійсності.

Навмисне викривлення інформації, як правило, базується на способах:

— приховування частини інформації,

— нав‘язування "бажаної" інформації.

Сутність дії першого способу полягає у тому, що ознаки, які дають максимальний внесок в розпізнавання ситуації, пригнічуються. Сутність дії другого способу полягає в тому, що імітуються ознаки, які дають максимальний внесок в розпізнавання хибної ситуації.

3.5.4. Напрями удосконалення інформаційних технологій

Існує два шляхи удосконалення технологій, у тому числі й інформаційних: екстенсивний та інтенсивний. Екстенсивний шлях передбачає розвиток технологій, який базується на удосконаленні існуючого методологічного апарату. Так, екстенсивний шлях розвитку інформаційно-пошукових систем (ІПС) полягає в розвитку методології пошуку необхідної інформації, яка базується на використанні ключових понять і логічних відношень між ними. Переваги цього підходу такі: очевидні очікувані результати; відносно незначний обсяг робіт, необхідний для отримання цих результатів, та фінансових витрат на виконання цих робіт (адже йдеться про удосконалення уже існуючих ІПС). Недоліки: переважна більшість серйозних програмних виробів розроблено за кордоном; стрибок якості (+Δ-стрибок якості), який може бути потенційно досягнутим, буде відносно незначним, оскільки він визначається тими обмеженнями, які закладені в удосконаленій методології побудови цих систем. Так, на прикладі тієї ж ІПС – використовуючи існуючу методологію, практично неможливо реалізувати пошук необхідної інформації саме за її змістом.

Інтенсивний шлях розвитку інформаційних технологій полягає в розробці і реалізації методології, яка базується на принципово інших підходах, вільних від обмежень, притаманних існуючим методологіям. Реалізація саме такого підходу спроможна надати інформаційним технологіям +Δ-стрибок якості, який буде на порядок вищий від цього ж показника, досягнутого при реалізації екстенсивного шляху. Так, у разі ІПС – якщо в основу їх побудови закласти методи автоматизації вилучення і формалізації знань, які містяться в природно-мовних текстових джерелах, то такі ІПС уже здатні здійснювати пошук необхідної інформації саме за її змістом. Переваги такого підходу очевидні. Основним його недоліком, як уявляється, – це досить значні витрати на розробку таких технологій і систем. Однак, як буде показано нижче, це так здається лише на перший погляд.

Ще одним фактором, який обумовлює пошук нових підходів до обробки текстової інформації, є необхідність аналізу у ряді випадків великих обсягів інформації, що особливо актуально для інформаційно-аналітичних органів і служб вищого державного рівня. Слід зазначити, що багато повідомлень, які надходять до цих служб, за змістом дублюють одне одного, тому не є у повному сенсі інформативними і їх накопичення недоцільне. Однак визначити, що

певна група повідомлень містить один і той же зміст, в автоматичному режимі вкрай складно. Адже одне і те саме за змістом повідомлення можна виразити різними синтаксичними конструкціями однієї мови, не кажучи вже про можливість використання різномовних засобів. Так, фразу “в одному з провідних військових навчальних закладів (ВНЗ) розроблено програмно-технічний комплекс (ПТК) для моделювання інформаційної боротьби (ІБ)” можна, не змінюючи змісту, переписати у таких варіантах:

1) для моделювання ІБ в одному з провідних ВНЗ розроблено ПТК;

2) ПТК, який розроблений в одному з провідних ВНЗ, призначений для моделювання інформаційної боротьби;

3) в одному з провідних ВНЗ здійснена розробка ПТК для моделювання інформаційної боротьби.

Автоматизувати процес розпізнавання того, що наведені чотири фрази передають однаковий зміст, досить складно (це не дивлячись на те, що ці фрази є відносно простими). Це зробити набагато легше, якщо у відповідності з певними правилами лінгвістичного аналізу формалізувати зміст, який відображений наведеними фразами, і привести їх до єдиного подання, наприклад, у такому вигляді:

*“*Розроблювати */ дія_завершена (суб’єкт:* ВНЗ*/ атрибут_який:* провідний*; об’єкт:* ПТК */ атрибут_для чого:* для моделювання */ атрибут_об’єкт [моделювання]:*ІБ*)”*

Більш складним завданням є визначення того, що фраза “колектив провідного ВНЗ розробив ПТК, орієнтований на моделювання ІБ” також передає той самий зміст, що і попередні чотири, і її також можна перетворити до цього ж формалізованого подання. Порівняти ж формалізовані подання змісту цих фраз, природно, набагато простіше. Такий підхід дозволяє, у разі необхідності, замість розглянутих 5 фраз без шкоди для їх змісту зберегти лише один формалізований образ їх змісту.

Найбільш перспективним напрямком, який забезпечує якісний стрибок в сфері інформаційного забезпечення всіх галузей державної і суспільної діяльності, є створення *інтелектуально-ємних знання-орієнтованих інформаційних технологій і систем.* При цьому під інтелектуально-ємністю розуміються два аспекти: рівень уречевлення інтелектуальних зусиль, спрямованих на їх створення, і рівень моделювання в конкретній інформаційній системі відповідних

інтелектуальних функцій людини з аналізу інформації. Знання-орієнтованість передбачає, що основою функціонування цих систем є процедури автоматизації вилучення знань, які містяться в природно-мовних текстових джерелах, їх формалізації і обробки.

Висновки

Об'єктом методології інформаційної безпеки є інформаційні процеси в соціо- і соціотехнічних системах, предметом – дослідження механізмів інформаційного впливу на особистість, суспільство і державу, а також способів, методів, засобів та каналів реалізації загроз національним інтересам на інформаційному рівні. Основним завданням методології інформаційної безпеки є створення науково-методичних основ своєчасного виявлення потенційних інформаційних загроз у різних сферах діяльності та механізмів їх реалізації, а також попередження і нейтралізації.

Методологічно найбільш виправданим є підхід до дослідження проблеми інформаційної безпеки з позицій теоретичної соціології (мається на увазі лише та компонента інформаційної безпеки, яка обумовлена інформаційним впливом на соціальний об'єкт і людину, зокрема). Теоретична соціологія розглядає соціальний об'єкт як систему, що складається з двох підсистем: внутрішньої – інтереси і стосунки між ними, та зовнішньої – елементи поведінки і стосунки між ними. На підставі такого формального уявлення стає можливим змістовний аналіз таких фундаментальних понять, як залежність між соціальними об'єктами, політика, влада й управління. Це, на наш погляд, саме те, що цікавить усіх передусім у питаннях національної безпеки взагалі й інформаційної безпеки зокрема.

Проблема інформаційної безпеки сьогодні – одна з найактуальніших, оскільки ми входимо в інформаційне співтовариство. Незважаючи на те, що в державі є безліч не менш нагальних проблем, які потрібно вирішувати вже сьогодні, питання інформаційної безпеки не можна лишати поза увагою. Необхідно розробляти методологічні, теоретичні і практичні основи цієї безпеки. Адже майже усі взаємовідносини між суб'єктами інформаційного суспільства ґрунтуватимуться на споживанні й обміні інформацією. А

в цьому випадку питання інформаційної безпеки стає превалюючим.

Якщо державу порівняти з живим організмом, то система інформаційної безпеки – це його імунна система і від того, наскільки вона сильна, залежить робота всього організму. З іншого боку, інформаційну безпеку можна розглядати і як самостійно функціонуючий цілісний організм. Збалансоване функціонування системи інформаційної безпеки забезпечується за рахунок постійного обміну інформаційними потоками як усередині держави, так і між державами. У цьому відношенні можна говорити про кругообіг інформації або енерго-інформаційний обмін. Будь-який цілісний організм є відкритою системою і працює як на віддачу імпульсів, так і на їх приймання. Без врахування цього закону система, врешті-решт, втратить свою життєздатність, що й продемонструвала політика "залізної завіси". Якщо не відбувається природний обмін в інформаційному просторі, то система "розривається" сама в собі. Завдання політики на інформаційному рівні – керування процесом обміну. Останній не є хаотичним і підпорядковується цілком певним законам, один з яких можна сформулювати таким чином: інформація не викидається в інформаційний простір довільним способом, а посилається передусім туди, де вона необхідна і її здатні сприйняти.

Отже, інформаційні потоки можна порівняти з кровоносною системою людського організму. Інформаційні технології саме і мають забезпечувати якісний склад крові, очищати її від шлаків і насичувати киснем – від того, якою буде кров, чи зможе вона дійти до всіх клітинок організму, залежить його робота. Для системи інформаційної безпеки важливими моментами є стиск інформації, фільтрація повторюваної інформації, зіставлення й об'єктивізація інформації на основі уже відомих знань і аналізу реальних подій, одержання нових знань, їх розподіл. Усе це завдання інформаційних технологій.

Глосарій до розділу

Безпека інформації – стан, що забезпечує захист інформації від загроз для неї.

Безпека інформаційної сфери – це стан захищеності інформації та сфер її створення, накопичення, зберігання, оброблення, розповсюдження й використання.

Дезінформація (від де-, дез- та інформація) – це розповсюдження викривлених або свідомо хибних відомостей для досягнення пропагандистських (в буржуазному суспільстві), воєнних (введення противника в оману) або інших цілей.

Знання – 1) сукупність відомостей, що утворюють цілісний опис, який відповідає деякому рівню інформування про питання, предмет, проблему тощо, які описуються;

2) сукупність відомостей про закономірності проблемного середовища і змістовну інтерпретацію виразів мови і процедур ЕОМ;

3) взаємозв'язана сукупність відомостей, що утворюють цілісний опис реального чи абстрактного світу (його фрагментів) і процесів, що в ньому відбуваються;

4) інформаційне подання, що містить взаємопов'язану сукупність відомостей, які утворюють цілісний опис реального чи абстрактного світу або його фрагментів.

Інформаційна безпека – 1) такий стан інформаційної озброєності особистості, суспільства, держави, тобто озброєності їх знаннями, при якому досягається захищеність і реалізація їх життєво важливих інтересів і гармонічний розвиток незалежно від наявності внутрішніх і зовнішніх загроз;

2) такий стан інформаційного забезпечення завдань національної безпеки, при якому досягається захищеність і реалізація життєво важливих інтересів, гармонічного розвитку і потреб в інформації особистості, суспільства, держави незалежно від наявності внутрішніх і зовнішніх загроз;

3) стан інформаційного середовища, при якому гарантується його розвиток і використання в інтересах особистості, суспільства і держави;

4) захищеність від різного роду зовнішніх і внутрішніх загроз системи формування і поширення автоматизованих інформаційних ресурсів, яка забезпечує їхнє ефективне використання в інтересах громадян, суспільства і держави.

Інформаційна безпека особистості характеризується захищеністю психіки й свідомості від небезпечних інформаційних впливів: маніпулювання, дезінформування, спонукування до самогубства, образ й ін.

Інформаційна безпека суспільства, держави характеризується ступенем їхньої захищеності й, отже, усталеністю основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи, суспільної свідомості і т.д.) стосовно небезпечних (дестабілізуючих, деструктивних, які зачіпають інтереси країни й ін.) інформаційних впливів, причому як до впровадження, так і до викрадення інформації. Визначається спроможністю нейтралізувати такі впливи.

Інформаційна боротьба *(в широкому розумінні)* відображена в таких її взаємопов'язаних визначеннях:

– це об'єктивно існуюча форма прояву стосунків між суб'єктами під час досягнення певних цілей і розв'язання конфліктних ситуацій чи інших суперечностей на інформаційному рівні;

– це наука, що акумулює всі вироблені людством знання про закономірності, принципи, форми, методи й засоби завоювання інформаційної переваги над протидіючою стороною, тобто наука про механізми інформаційного протиборства;

– це комплекс заходів, спрямованих на досягнення певних цілей і розв'язання конфліктних ситуацій на інформаційному рівні, здійснюваних за єдиним задумом і планом та узгоджених за часом, місцем, залученими силами й засобами.

Завдання інформаційної боротьби:

1) цілеспрямоване добування інформації про поточну ситуацію з жорсткими вимогами до її своєчасності, якості, обсягу й темпу відновлення та оцінка на основі цієї інформації політичної (воєнно-політичної, воєнної, економічної, соціальної, екологічної тощо) ситуації. Виконання цього комплексу завдань ускладнене тим, що воно в загальному випадку здійснюється в умовах інформаційної протидії. При цьому інформація, що підлягає аналізу, характеризується невизначеністю об'єктивного й суб'єктивного походження, неповнотою за одними аспектами і надмірністю за іншими, суперечливістю, наявністю частково зруйнованої або перекрученої інформації, у тому числі і дезінформації;

2) цілеспрямований і комплексний вплив на свідомість і підсвідомість населення й особового складу, на інформаційні ресурси на всіх фазах їх виробництва, розповсюдження й використання, а також на інші складові інформаційного середовища протидіючої (конкуруючої) сторони в інтересах нав'язування їй бажаних рішень і керування її поведінкою. Особливої ваги набуває не так руйнівний, як цілеспрямований вплив саме на зміст інформації для забезпечення своїх інтересів у різних сферах діяльності особистості, суспільства, країни. Ця проблема обумовлює потребу в дослідженні механізмів формування дезінформації, розробленні науково-методичних засад її виявлення та створення автоматизованих систем аналізу поточних ситуацій в умовах інформаційної протидії, зокрема за наявності дезінформації. У цьому комплексі завдань особливого значення набуває можливість використання інформації (інформаційних потоків) як ефективного засобу формування позитивного іміджу України на міжнародній арені, а також можливість усунення політичної, воєнно-політичної, економічної й, особливо, воєнної напруженості у відносинах з іншими країнами та в різних регіонах країни;

3) захист власних інформаційних ресурсів та інших складових інформаційного середовища, у тому числі на рівні свідомості і підсвідомості людини**,** від впливу на них протидіючої сторони. Не зменшуючи важливості виконання завдань технічного захисту інформації, спрямованого в основному на забезпечення її конфіденційності, слід підкреслити особливу значущість завдань захисту власне змісту інформації від навмисного його спотворення чи перекручення, у тому числі й завдань виявлення дезінформації. До цього комплексу входять також завдання відновлення цілісності змісту частково зруйнованої чи спотвореної інформації, у тому числі й природно-мовної текстової інформації.

Метою інформаційної боротьби (*в широкому розумінні)* є забезпечення воєнно-політичних, економічних і воєнних інтересів країни за рахунок досягнення й утримання інформаційної переваги на найбільш значущих (чуттєвих, уразливих) в конкретних умовах напрямках.

Метою інформаційної боротьби *(у вузькому розумінні)* є створення сприятливих умов для успішного проведення операцій і

бойових дій, ефективного застосування своїх військ (сил), озброєння і військової техніки, а також зниження ефективності застосування військ (сил) і зброї противника шляхом захоплення й утримання інформаційної переваги над противником під час підготовки й в ході воєнних (бойових) дій опосередкованим введенням протидіючої сторони в контур свого управління на інформаційному рівні.

***Інформаційна загроза*:**

– такий інформаційний вплив (внутрішній або зовнішній), при якому створюється потенційна або актуальна (реальна) небезпека зміни напрямку або темпів прогресивного розвитку держави, суспільства, індивідів;

– небезпека заподіяння шкоди життєво важливим інтересам особистості, суспільства, держави шляхом інформаційного впливу на свідомість, інформаційні ресурси та інфосферу машинно-технічних систем;

– сукупність чинників, що перешкоджають розвитку і використанню інформаційного середовища в інтересах особистості, суспільства і держави.

***Інформаційна зброя*:** 1) це комплекс специфічних програмно-інформаційних засобів, створених для ураження інформаційного ресурсу противника;

2) це – засоби знищення, викривлення або викрадення інформаційних масивів; засоби подолання систем захисту; засоби обмеження доступу законних користувачів; засоби дезорганізації роботи технічних засобів, комп'ютерних систем;

3) це – засоби знищення, викривлення або викрадення інформаційних масивів, добування з них необхідної інформації після подолання систем захисту, обмеження або заборони доступу до них незаконних користувачів, дезорганізації роботи технічних засобів, виведення з ладу телекомунікаційних мереж, комп'ютерних систем, усього високотехнологічного забезпечення життєдіяльності суспільства і функціонування держави;

4) під термін "інформаційна зброя" підпадають технічні або програмні засоби для забезпечення несанкціонованого доступу або, навпаки, обмеження доступу до інформаційних баз даних; порушення штатного режиму функціонування технічних засобів і програмного забезпечення, а також виведення з ладу ключових

елементів інформаційної інфраструктури окремої держави або навіть регіону.

Інформаційна інфраструктура – сукупність центрів, каналів і засобів створення, збору, накопичення, зберігання, обробки, розповсюдження і використання інформації.

Інформаційний вплив – цілеспрямовані заходи інформаційного характеру, які спрямовані на зміну поведінки (реакції) людини або роботи комп'ютерної системи, в інтересах протидіючої сторони.

Інформаційний ресурс – інтелектуальний ресурс, фактор колективної творчості, і основна складність в розумінні його природи і функцій полягає в розкритті механізму переходу "знань в силу", способів його впливу на матеріальні фактори прогресу. Інформаційний ресурс можна розглядати як "симбіоз" знання й інформації (інформації у вигляді поняттєвого знання). Розглянемо визначення понять "інформація" та "знання".

У контексті інформаційної боротьби видається за корисне таке визначення сутності поняття інформації.

Інформаційно-аналітична діяльність – процес створення нового інформаційного продукту, придатного для прийняття управлінських рішень, на підставі аналізу і систематизації всієї доступної інформації.

Інформація *(у контексті інформаційної боротьби)* – втілені в деякій формі відомості, які відбивають з будь-яким ступенем приближення сутності об'єктів та явищ абстрактного або реального світу. Інформація являє собою нерозривну єдність сутності й форми (in form) і не існує без носія інформації. Слід відрізняти поняття "зміст інформації" і "смисл інформації". Зміст інформації – це те, про що йде мова, смисл інформації – це те, що вкладається в цю інформацію (значення, інтерпретація інформації).

Інформація має троїсту сутність: вона об'єктивно існує незалежно від нас; вона є моделлю відповідних об'єктів і процесів; вона здатна породжувати певні матеріально-енергетичні процеси.

Технологія *(у широкому розумінні)* – це цілеспрямовано сформована сукупність знань про методи здійснення виробничих процесів, що є основою для створення, удосконалювання і використання відповідної продукції.

Інформаційна інфраструктура – сукупність центрів, каналів і засобів створення, збору, накопичення, зберігання, обробки, розповсюдження і використання інформації.

Технологія *(у вузькому розумінні)* – це оформлена документально система методів, способів, прийомів, засобів автоматизації (технологічного обладнання) і регламентованого порядку їх застосування, які забезпечують отримання потрібного продукту в заданих умовах і з заданим показником якості.

Критична технологія – технологія, відсутність чи не використання якої загрожує безпеці держави.

Інформаційні технології *:* 1) це технології, які забезпечують всебічний розвиток інформаційної інфраструктури та вплив на неї;

2) це матеріалізовані на базі інформаційної інфраструктури знання в галузі створення, збору, накопичення, зберігання, обробки, розповсюдження і використання інформації.

Зв'язок ключових термінів і понять

Рис. 3.4

Завдання і запитання для самоперевірки

1. Дайте визначення інформаційної безпеки.
2. Чим характеризуються інформаційна безпека суспільства, держави і особистості?
3. Дайте визначення інформаційної загрози.
4. Наведіть перелік загроз національним інтересам в інформаційній сфері.
5. Дайте визначення і сформулюйте завдання інформаційної боротьби.
6. Дайте загальну характеристику класифікації інформаційних ресурсів.
7. Які властивості притаманні інформаційній зброї?
8. Які існують різновиди класифікації інформаційної зброї?
9. Дайте визначення і розкрийте сутність інформаційних технологій.
10. Наведіть класифікацію загроз інформаційним технологіям в управлінні і розкрийте їх сутність.

Рекомендована література до розділу

1. Закон України “Про основи національної безпеки України” (19 червня 2003 року, № 964-IV, Орієнтир, 30 липня 2003 року, №139, с.1–6).
2. Конституція України. – К. Юніком. 1996.
3. *Литвиненко О.В., Бінько І.Ф., Потіха В.М.* Інформаційний простір як чинник забезпечення національних інтересів України. – К.: ІМВ КУ ім. Тараса Шевченка, 1998. – 47с.
4. *Лопатин В.Н.* Информационная безопасность России: Человек. Общество. Государство. – Санкт-Петербург: Фонд «Университет», 2000.
5. Інформаційна безпека держави у контексті протидії інформаційним війнам: Навчальний посібник (за ред. Толубка В.Б.). – К.: МОУ НАОУ, 2004.
6. *Толубко В.Б.* Інформаційна боротьба (концептуальні, теоретичні, технологічні аспекти) : Монографія. – К.: НАОУ, 2003.
7. *Толубко В.Б., Рось А.О., Замаруєва І.В.* Інформатизація управлінської діяльності як чинник інформаційної безпеки держави: Монографія. – К.: НАОУ, 2004. – 213 с.
8. *Петрик В.М., Кузьменко А.М., Остроухов В.В.* та ін.. Соціально-правові основи інформаційної безпеки: Нав. Посіб. /За ред.. В.В. Остроухова. – К.: Росава, 2007. -496 с.

Використані джерела

5. Закон України “Про основи національної безпеки України” (19 червня 2003 року, № 964-IV, Орієнтир, 30 липня 2003 року, №139, с.1–6).

6. *Поздняков А.И.* Информационная безопасность личности, общества, государства // Военная мысль. – 1993. – № 10.

7. *Рубан В.Я., Калитич Г.И., Широков В.А.,* та ін. Информатизация и моделирование в развитии Украины // Информатизация процессов экономического развития Украины. Сб. научных трудов. – ГосНИИ информатизации и моделирования экономики Минэкономики Украины. – 1994.

8. *Синецкий В.П.* О понятийном аппарате общей теории безопасности // Военная мысль. – 1994. – № 8.

9. *Голубков А.С.* Автоматизированные ресурсы России. Состояние и тенденции развития. Национальный доклад // Научно-техническая информация. Серия 1. Организация и методика информационной работы. – М.:ВИНИТИ. – 1994. – № 11.

10. Інформаційна безпека держави у контексті протидії інформаційним війнам: Навчальний посібник (за ред. Толубка В.Б.). – К.: МОУ НАОУ, 2004.

11. *Толубко В.Б.* Інформаційна боротьба (концептуальні, теоретичні, технологічні аспекти) : Монографія. – К.: НАОУ, 2003. .

12. *Каныгин Ю.М., Калитич Г.И.* Основы теоретической информатики. – К.: Наукова думка, 1990.

13. *Соловцов Н.Е., Глазов Б.И., Ловцов Д.А.* Классификация и способы применения “информационного оружия” // Стратегическая стабильность. – 1999. – № 4.

14. *Толубко В.Б., Рось А.О., Замаруєва І.В.* Інформатизація управлінської діяльності як чинник інформаційної безпеки держави: Монографія. – К.: НАОУ, 2004. – 213 с.

15. *Балабін В.В., Замаруєва І.В., Лєнков С.В., Рось А.О.* Інформаційні системи нового покоління як фактор забезпечення національних інтересів/К.: Наука і оборона. –2007. –№1. –С. 40–45.

16. *Глазов Б.И., Ловцов Д.А.* Информационная борьба как система отношений в информационной среде // Военная мысль. – 1997. – № 5.

17. *Гриняев С.Н.* Интеллектуальное противодействие информационному оружию / Серия “Информатизация России на пороге XXI века”. – М.: СИНТЕГ, 1999.

18. *Губарев В.А., Крутских П.П.* Концептуальная модель конфликта в информационной борьбе //Радиотехника. – 1998. – № 6.

19. Інформаційна безпека України: сутність та проблеми. Матеріали круглого столу // Стратегічна панорама. Щоквартальний науково-практичний журнал Ради національної безпеки і оборони України. – 1998. – №3–4.

20. Информационные вызовы национальной и международной безопасности / Под общей редакцией А.В.Федорова и В.Н.Цыгичко. – М.: ПИР_Центр, 2001.

21. *Комов С.А.* Информационная борьба в современной войне: вопросы теории // Военная мысль. – 1996. – № 3.

22. *Костин Н.А.* Общие основы теории информационной борьбы // Военная мысль. – 1997. – № 3.

19. *Толубко В.Б., Рось А.О.* Складові інформаційної боротьби // Наука і оборона. – 2002. – № 2.

20. *Фомін В.О., Рось А.О.* Сутність і співвідношення понять "інформаційна безпека", "інформаційна війна" та "інформаційна боротьба" // Наука і оборона. – 1999. – № 4.

21. *Хохлов А.* Один боевой генератор способен превратить дивизию в стадо идиотов // Комсомольская правда. – 15 октября 1996 г.

22. *Цыганков В.Д., Лопатин В.Н.* Психотронное оружие и безопасность России. – М.: СИНТЕГ, 1999.

23. *Слипченко В.И.* Войны шестого поколения. Оружие и военное искусство будущего. – М.: ВЕЧЕ. – 2002. – 382 с.

24. *Плет В.* Стратегическая разведка. Основные принципы. - М.: Издательский Дом «Форум», 1997, - 376 с.

25. Analytic Thinking and Presentation for Intelligence Producers / Liaison.- Unclassified

26. Автоматизированные информационные ресурсы России. Состояние и тенденции развития. Национальный доклад // Научно-техническая информация. Сер.1. Организация и методика информационной работы. М.:ВИНИТИ. – 1994. №11. – с. 2-30.

Розділ 4.

ІНФОРМАЦІЙНА БЕЗПЕКА СУСПІЛЬСТВА

4.1. Суспільна свідомість та її роль у формуванні національної ідеї

Інформаційні загрози є досить новим поняттям ери інформаційного суспільства. З поступовим переходом індустріального суспільства до суспільства знань та інформації, традиційні види соціальних відносин поступово трансформуються, набуваючи якісно нових характеристик. Реалії сьогодення доводять, що інформаційні загрози не є чимось далеким і абстрактним, а мають цілком реальні результати своєї діяльності, що позначаються як в матеріальних збитках, так і в духовному розщеплені та занепаді. Не стали виключенням і бойові дії та ведення війни: від довготривалих, чисельних і кровопролитних воєн суспільство поступово переходить до так званих "війн сьомого покоління", що характеризуються як безконтактні війни, полем бою яких став не територіальний простір, а кіберпростір (у технічному вимірі) та людська свідомість (у соціально-психологічному вимірі). Зброєю ж стала інформація – від когнітивного та електронного рівня до енерготехнічного та парапсихологічного. Тепер кожен, не будучи учасником бойових дій, може стати їх жертвою, бо від інформації неможливо втекти, заховатись і навіть просто існувати без неї.

4.1.1. Види колективної свідомості та їх роль в життєдіяльності суспільства

В основі розуміння процесів забезпечення інформаційної безпеки суспільства лежать такі центральні поняття, як свідомість, масова свідомість, суспільна свідомість, національна свідомість.

Свідомість є одним з основних понять філософії, психології та соціології, що позначає вищий рівень психічної активності людини як соціальної істоти. В самому широкому розумінні свідомість визначається як стан людини в здоровому глузді й пам'яті, здатність контролювати свої вчинки, почуття. Це визначення поєднує в собі властивості психічної активності людини як соціальної істоти, так біологічної.

В російському словнику-довіднику «Воєнна безпека Росії» за загальною редакцією В.Л. Манілова [1] наведено визначення поняття свідомості, яке розкриває властивості свідомості як об'єкта інформаційно-психологічного впливу.

Свідомість – вищий рівень психічного відображення людиною об'єктивної дійсності, що відрізняється: активністю, обробкою потоків інформації, взаємодією з навколишнім світом; спрямованістю на предмет; здатністю до самоспостереження та самопізнання психічних актів і станів; мотиваційно-ціннісним характером; різним ступенем ясності. Своєрідність свідомої діяльності полягає в тому, що відображення реального світу у формі чуттєвих і розумових образів передує практичній діяльності людини (суспільства), надаючи їй цілеспрямований характер. Свідомість носить не тільки індивідуальний, але й міжособистісний характер (див. суспільна свідомість; масова свідомість). У свідомості можна виділити, з одного боку, різноманітні інформаційні аспекти, які визначають активний процес пізнання в будь-якій знаковій формі, з іншої – власне психічний аспект, який реалізує свідомість. Ці два боки свідомості невід'ємні один від одного, вони постійно взаємодіють і, в кінцевому рахунку, визначають життєздатність особистості як в інтелектуальному, так і в біологічному сенсі. Порушення свідомої діяльності людини приводить до прийняття неадекватних реальній ситуації рішень, неадекватної поведінки, психологічної залежності, деструкції особистості.

Суспільна свідомість – погляди, які визначають спільні інтереси погляди, переконання, ідеї та переконання, які склалися в суспільстві на певному етапі історичного розвитку. Суспільна свідомість виступає у формі політичних, юридичних, естетичних, етнічних тощо теорій, філософії, моралі, соціальних норм та інших визначаючих її форм. Подібно тому як суспільство не є сумою його складових, так і суспільна свідомість не є сумою свідомостей окремих особистостей. Суспільна свідомість є особливою духовною системою, яка живе своїм відносно самостійним життям. Між особистим і суспільною свідомістю відбувається постійна взаємодія. У суспільній свідомості можна виділити три структурних рівні:

– верхній – суспільна думка, яка включає в себе масове ставлення громадян країни до соціальних подій, фактів і проблем, до діяльності окремих груп, організацій, особистостей і відрізняється значним динамізмом і мінливістю;

– основний рівень, який характеризує усталену систему понять, поглядів, світосприймання суспільства в цілому і має більшу стійкість, ніж суспільна думка;

– глибинний рівень, який є своєрідною базою суспільної

свідомості.

Основний рівень змінюється незначно та знаходить свою реалізацію в моралі, ідеалах, цінностях, поняттях добра і зла, а також у духовних і культурних традиціях народу.

Національна свідомість – сукупність соціальних, політичних, економічних, етичних, естетичних, філософських, релігійних та інших поглядів та уявлень, що характеризують зміст, рівень та особливості духовного і культурного розвитку населення країни.

Національна свідомість є тим ядром, навколо утворюється об'єднуюча національна ідея розвитку країни.

Масова свідомість – вид свідомості суспільства, що визначає співпадіння в якийсь момент основних і найбільш значущих компонентів свідомості значної кількості різноманітних «класичних» груп суспільства (великих і малих).

Масова свідомість найбільш уразлива до інформаційно-психологічних впливів, висока ефективність впливу полягає в тому, що людина в натовпі скоріше виступає як біологічна істота, ніж соціальна і спрацьовує так званий ефект "натовпу" або зграї. Як встановив у своїх дослідженнях відомий лікар психіатр Бехтєрєв В.М.[2], у колективі відбувається посилення ефекту сугестії (гіпнозу). Найбільш переконливі результати були отримані при впливі на емоції: вони зберігаються в глибинах підсвідомості, закодовані на генетичному рівні, у всіх мають подібну структуру. В експериментах було використано звичайну радіомережу або мікрофони. Було виявлено комплексні радіосигнали певного ритму, що викликали в слухачів легкий гіпнотичний стан, який сприяв би підвищеному стану переконливості в об'єкта впливу. Спочатку на них реагує невелика кількість людей, далі доволі швидко розповсюджується процес взаємної індукції, так званий ефект натовпу. Через деякий час характер сигналів змінювався таким чином, щоб ідеї вербального впливу закріплювалися у свідомості людини. Результати експериментів навели послідовників цієї наукової школи на висновок, що ця зброя дозволяє маніпулювати не тільки окремими колективами, але й народом у цілому, створюючи слухняні натовпи.

На підставі літературних джерел, що доступні авторам, важко зробити висновок, чи було практичне застосування теоретико-експериментальних досліджень видатного вченого та витік інформації за кордон. Але цікаво, що одночасно у двох сусідніх країнах з мало схожими народами - СРСР і Германії, стрімко закріпився культ двох диктаторів, різних за манерами, характером, інтелектом, переконаннями. Якщо звернути увагу на стиль вербального впливу, то в Гітлера - емоційний, що доходить до істерики, проникаючий до містичних і міфологічних глибин

свідомості. Саме так можна було "розпалити" раціональних німців, які звикли до порядку та спокою. Сталін, звертаючись до різнорідного, схильного до анархії російського люду, вибрав, за принципом контрасту, спокійну, розсудливу, повільну манеру переконання.

Таким чином керування суспільством здійснюється за допомогою інформаційного впливу на процеси і структури людської психіки. Основою керування цими процесами у суспільному вимірі стала своєрідна економіка уваги, метою якої є заволодіння і утримання на певних символах свідомості суб'єкта.

4.1.2. Моделі інформаційно-психологічного впливу, що діють у суспільстві

Моделі інформаційно-психологічного впливу, що діють у суспільстві, можна класифікувати за кількісними показниками. Це такі моделі "*один-один*", "*один-багато*", *"багато-один",* "*багато-багато*".

Модель "один-один". У цій моделі в ролі як суб'єкта впливу (тобто того, хто впливає), так і об'єкта впливу (тобто того, на кого впливають) виступає особистість. Прикладом такої моделі з точки зору зовнішньої загрози є вирішення задачі "вербовки". Практично ця модель реалізує схему протистояння двох особистостей. В основі функціонування моделі досягнення мети суб'єкта лежать закономірності показників розвитку особисті, що є об'єктом впливу, а саме: знання про навколишній світ, знання про себе та свій народ, система цінностей індивіда, система його цільових настанов (спрямувань), віра, інформаційний психотип людини, здатність до сприймання та аналізу інформації тощо.

Вирішальне значення при досягненні мети впливу мають апріорні знання суб'єкта про об'єкт впливу. Отже, сам процес впливу можна поділити на кілька етапів:

– збір та вивчення інформації щодо об'єкта впливу;

– вибір концепції впливу, що має включати виявлення незбалансованих компонентів в системі показників розвитку особистості, на яку здійснюють вплив, вибір каналів і джерел впливу;

– формування змістової частини інформації;

– формування кількісних, просторових та часових характеристик подання інформації з метою створення необхідного коридору довіри між джерелом та об'єктом впливу;

– комплекс заходів, спрямований на підтримку збудження інтересу до інформації з боку об'єкта впливу.

Реалізація такої моделі інформаційно-психологічного впливу є найбільш небезпечною за своїми наслідками для суспільства, коли в ролі об‘єктів впливу виступають перші особи держави, особи, які приймають рішення в сфері державного управління.

Модель "один-багато". У цій моделі в ролі суб‘єкта впливу виступає особа, а в ролі об‘єкта - угруповання (етнічне, професійне, релігійне тощо) або суспільство в цілому. Вербальний вплив на колектив, як правило, базується на ідеї, що об‘єднує окремі особистості в колектив або штучному створенні такої ідеї (порівняймо методи залучення до місіонерських церковних об‘єднань через проповіді по телебаченню, індивідуальні бесіди на вулицях тощо). Головну ідею штучного об‘єднання до колективу можна інтерпретувати наступним чином: ти не один, Бог тебе любить, єднайся з нами - і ти вирішиш усі свої проблеми. До цього також можна віднести рекламні кампанії, де також об‘єднуючим початком є ідеї штучного об‘єднання в колектив: ти хочеш бути самим красивим, сильним тощо. Реалізація ідеї базується також на використанні показників, що наведені раніше, але їх значення характеризують не окрему особистість, а подають узагальнені характеристики певного угруповання.

Розглянуті моделі інформаційно-психологічного впливу на суспільство є найбільш небезпечними для держави, бо визначаються цілісністю мети та єдністю заходів щодо її досягнення.

Моделі "багато-один" і "багато-багато" в сучасному суспільстві носять здебільшого стохастичний характер багатофакторного впливу. Ця особливість і включає в особистості "програму" саморегуляції (або самоорганізації) залежно від її (особистості) власних показників розвитку. Звичайно, щоб ця "програма" працювала без порушень, державним структурам потрібна кропітка робота щодо виховання у членів суспільства інформаційної культури. Прикладом функціонування моделі "багато-один" може служити кожний з нас. Це фактично той інформаційний простір, в якому відбувається життєдіяльність сучасної людини. З точки зору цілісності держави, функціонування її соціальних структур ми маємо модель "багато-багато". Незважаючи на відносно стохастичний характер функціонування цієї моделі, безпека суспільства та окремих його верств не в останню чергу залежить від контролю за інформаційним простором (і перш за все - за засобами масової інформації) з боку держави щодо гармонійного розподілу його складових. Іншими словами, з боку відповідних державних структур має бути регламентація кількісних, якісних, часових і просторових показників інформування членів суспільства, тобто: *Де? Коли? До якої? В якій кількості?* ми маємо доступ до інформації. Така регламентація має базуватися на науково-методичних засадах і задовольняти вимогам:

– оптимального (критичного) сприймання інформації людиною;

– сприяти захищеності особистості, угруповання, суспільства на інформаційному рівні;

– створення умов прогресивного розвитку суспільства.

Концепція інформаційної безпеки держави у воєнній сфері має враховувати й загрози нав'язування суспільству негативних думок, серед яких можна виділити:

– протистояння армії й народу в державі;

– відволікання армії від виконання своїх прямих обов'язків;

– деморалізація армії;

– дискредитація армії в очах власного народу та світового суспільства, інші.

Серед негативних факторів**,** що створюють умови реальної *загрози* успішного застосування інформаційно-психологічного впливу проти України, можна визначити такі**:**

– втрата (у порівнянні зі станом колишнього СРСР) репродуктивної функції відтворення нових знань;

– тимчасовий вакуум духовних та культурних цінностей в суспільстві;

– втрата культурно-мовних традицій.

Втрата функції відтворення нових знань у суспільстві призводить до того, що при сприйманні інформації відсутня основа для функції порівняння, що є однією з найважливіших (базових) при сприйманні та обробці інформації. І як наслідок, людина перестає критично сприймати інформацію і вірить тому, що їй насаджують. На жаль, становище, в якому опинилася сьогодні наука (основний осередок відтворення нових знань у суспільстві), фактично вже поставило нас перед реальною загрозою зовнішнього інформаційно-психологічного впливу з боку більш розвинутих у технологічному плані країн.

Наступний небезпечний момент перехідного суспільства – вакуум духовних та культурних цінностей. Сьогодні народ України ще не відчуває себе нацією. В його свідомості співіснують поруч ностальгія за минулим, забобони ідеалів радянських часів та прагнення до імітації зовнішньої соціальної атрибутики заможних країн. Це пов'язане з тим, що для утворення стійкої суспільної свідомості потрібний досить тривалий час. Мойсей водив свій народ по пустелі 40 років. За цей час відбувається повна зміна поколінь. Нашій державі лише 16 років, і те покоління, яке народилося в новій Україні, ще приймає повноправної участі в житті суспільства.

З останнім поєднано і втрату культурно-мовних традицій. З точки зору соціолінгвістики виділяються дві групи мовних ситуацій: екзоглосні – сукупності різних мов, та ендоглосні – сукупності

підсистем однієї мови, які можуть бути як збалансованими, так і незбалансованими. Збалансовані ситуації характеризуються функціонально рівнозначними компонентами, а незбалансовані - розподіленням компонентів за різними сферами спілкування та соціальними угрупованнями. Сьогодні в Україні ми маємо незбалансовану мовну ситуацію. З одного боку, українська мова набула статусу єдиної державної мови, з іншого боку, приблизно 60% населення не володіють українською мовою належним чином. Причини цього криються як в об'єктивному становищі, в якому знаходилась українська мова понад 70 років (єдину функцію, яку вона виконувала фактично в ці роки - це побутове внутріетнічне спілкування і фахове спілкування україністів, в інших всіх сферах панувала російська мова), так і в сучасній мовній політиці, яка недостатньо враховує особливості перехідного періоду, а саме: повільно йде робота щодо стандартизації української наукової термінології, практична відсутність власної лексикографічної бази. Як наслідок, володіння українською мовою здебільшого є штучним, воно не поєднується з історією, культурними традиціями нації.

Панас Мирний сказав: "Найбільше і найдорожче добро кожного народу – це його мова, ота жива схованка людського духу, його багата скарбниця, в яку народ складає і своє давнє життя, і свої сподіванки, розум, досвід, почування".

Отже, в мовній галузі існують ті ж самі хвороби, що і в нашому суспільстві взагалі. Зневага до української мови як одного з основних чинників забезпечення суверенітету країни, до проблем її становлення може призвести до того, що Україна врешті-решт піде не шляхом інтеграції до світового інформаційного простору, а сприятиме її експансії з боку заможних країн.

У свою чергу, розвиток гуманітарної сфери створює об'єктивні умови для єднання нації і впливає як на зниження конфліктного потенціалу в самому суспільстві, так і загроз вербального впливу ззовні. Розвиток української мови не може бути механістичним перенесенням її лексики та граматики, він здійснюється через розвиток всієї гуманітарної сфери суспільства. Комерціалізація засобів масової інформації, освіти, мистецтва сприяє реальній загрозі фактичного відриву цілих верств населення від вищої освіти та культурних цінностей. Матеріальний достаток і високий рівень споживання не вирішують проблеми гуманітарної кризи суспільства, тобто кризи цінностей, суспільних ідеалів, мотивацій поведінки та структур спілкування.

Крім того, концепція інформаційної безпеки має враховувати групи ризику, тобто *об'єкти захисту* від небажаного (і в першу чергу,

зовнішнього) інформаційно-психологічного впливу, серед яких можна визначити наступні:

- молодь;
- особовий склад армії та члени їх сімей;
- інформаційно-аналітичні підрозділи.

Об'єкти захисту розглядаються як групи ризику, не приділення уваги, які можуть стати загрозою воєнній безпеці України. Якщо дві перших групи не викликають сумнівів. Дійсно морально-психологічний стан армії залежить і від патріотичного виховання юнаків-допризовників навіть при переході на контрактну армію, оскільки вирішення тільки матеріальних і соціальних проблем не забезпечує повною мірою боєздатність армії, і від соціального статусу сімей військовослужбовців), то третя група потребує пояснення. Кінцевою метою інформаційно-психологічного впливу є нав'язування протидіючою стороною бажаних рішень і поведінки суспільству. Переважна більшість рішень, що приймаються державними структурами, мають інформаційну основу, а інформаційно-аналітичні підрозділи призначені для підготовки інформації, на підставі якої готуються рішення.

4.2. Чинники ескалації інформаційних загроз суспільству

В законі України "Про основи національної безпеки України" № 964-IV від 19 червня 2003 року[4] визначені основні загрози в соціальній і гуманітарній сферах. Переважну більшість цих загроз можна нейтралізувати на інформаційному рівні. В даному підрозділі розглянемо чинники ескалації інформаційних загроз суспільству.

Основним *чинником есклації загроз в інформаційному суспільстві є засоби масової інформації* (ЗМІ). За своєю природою вони покликані забезпечувати інформаційну безпеку особистості за рахунок «доставки» споживачу необхідних для прийняття рішення інформаційних ресурсів. Досить часто саме вони здійснюють негативний інформаційно-психологічний вплив, здатний призвести до значних порушень нормального функціонування й життєдіяльності не лише окремих особистостей, а і груп громадян, соціальних, суспільних, державних організацій. Такі дії, і не лише з боку ЗМІ, можуть викликати психоемоційну і соціально-психологічну дезорієнтацію і, як наслідок, неадекватну поведінку окремих осіб, груп і мас людей, їх наслідками можуть бути глибокі трансформації індивідуальної, групової, масової свідомості, зміни морально-політичного та соціально-психологічного клімату в суспільстві.

ЗМІ використовуються різними політичними й суспільними організаціями, фінансовими структурами, релігійними сектами як механізм здійснення інформаційно-психологічного впливу на особистість.

Одним із способів підтримки ЗМІ на відповідному рівні інформаційної безпеки є моніторинг, тобто відслідкування процесів, що в них відбуваються. При цьому увага повинна приділятися як тематиці, методам її висвітлення в ЗМІ, так і тому, які політичні, суспільні або інші сили займаються пропагандою своїх ідей і здійсненням інформаційного впливу на населення.

До числа чинників інформаційних загроз, спрямованих проти особистості, слід віднести іноземну присутність в Україні, у тому числі іноземну присутність в інформаційному просторі країни. Найпростішим прикладом, що підтверджує справедливість цієї тези, є домінування на українських теле- і радіоканалах інформаційної продукції зарубіжного виробництва.

Дослідження, проведені О.В. Литвиненком [5], свідчать про те, що ситуація в інформаційному просторі України близька до типової ситуації в слаборозвинених країнах. Так в межах вказаного дослідження було підраховано, що за період з 18 по 24 березня 1996 року на 9 телеканалах українського телебачення було продемонстровано майже 70% фільмів західного, переважно американського, виробництва. Таким чином можна говорити про розгортання рядом країн світу інформаційної і культурної експансії стосовно України і її громадян, а також намагання скоротити використання рідних мов (української, російської), як засобів спілкування.

Сутність стратегії іноземної інформаційної присутності полягає в тому, що для досягнення цілей зміни суспільного устрою слід міняти не базис суспільства, а його надбудову, здійснюючи «молекулярну агресію» у свідомості кожної особистості й суспільства в цілому, руйнуючи його культурне ядро. У тому, що така агресія відбувається, до того ж безперервно і цілеспрямовано, сумніватися практично не доводиться. Підтвердженням цьому є проведені російськими вченими дослідження інформаційного простору Російської Федерації, до якого через кабельне і супутникове телебачення частково входить й інформаційний простір України. У результаті цього дослідження були зроблені висновки про те, що країни Заходу реалізують свої геополітичні інтереси на нашій території через систему керуючих впливів, які в іноземних бойових документах носять назву психологічних операцій.

Особливе місце в структурі інформаційних загроз займає *інформаційно-психологічний вплив з боку різноманітних релігійних*

об'єднань. Його особливістю є комплексне проникнення не лише у свідомість людини, але й доведення необхідної інформації до глибин підсвідомості. При цьому сама інформація здійснює скоріше не свою першочергову – інформативну функцію, а функцію «програмування» людини на виконання певних настанов, змінюючи водночас її моральні цінності, життєві орієнтири. Людина долучається до системи навіювання та пригнічення. Вона стає не просто віруючою, а рабом релігійної психології. Особливу небезпеку в порівнянні з іншими інформаційними загрозами інформаційно-психологічний вплив з боку релігії являє собою тому, що, руйнуючи свідомість, він тим самим деформує сприйняття людиною інших інформаційних масивів, викликає неадекватність розуміння вхідних потоків інформації.

Г.Г. Почепцов запропонував тези конструювання релігійної комунікації, які можна подати в такому вигляді[6]:

1. Інформаційний вплив з боку релігійних інститутів відбувається в специфічному контексті сприйняття, що знімає опір, мінімізує ступінь недовіри.

2. Використовується індивідуальний, особистісний підхід, коли інформація спрямовується в найпотаємніші куточки свідомості. При цьому у об'єкта інформаційної дії складається враження, що звернення відбувається особисто до нього і саме він має відповісти на це своєю щирістю, відвертістю, готовністю до сприйняття.

3. Релігійна комунікація діє в колективі, коли всі сумніви індивіда поглинаються прикладом натовпу. Кожен має робити як всі, завжди разом з усіма. Особистість не може піти всупереч релігійній громаді.

4. Основою більшості релігій є антагонізм. Людину намагаються тримати в покорі, залякуючи її дияволом, ворогами церкви або карами, які впадуть на її голову в разі зради релігійним інтересам.

5. Використовується безальтернативність, коли всі інші релігійні течії визнаються ворожими. Заперечуються будь-які сторонні джерела інформації. Дозволяється лише одна істина. Ті, хто її заперечують, також визнаються ворогами і піддаються гонінням.

6. Занурення в глибини підсвідомості досягається шляхом багаторазового повторення, коли засвоєння певної інформації доводиться до автоматизму, тобто відбувається «програмування» людини, підміна цінностей.

7. Спрямування релігійної комунікації на певні верстви населення, зокрема на молодь. Це пояснюється легкістю впливу, яка пов'язується з незакінченістю процесів формування особистості молодої людини, відсутністю чітких поглядів на життя. Для залучення молоді в участі у релігійному житті використовуються й неординарні методи. Окремі псевдорелігійні об'єднання, які за своєю сутністю є злочинними формуваннями, створюють так звані «елітарні» клуби, секти, членами

яких можуть стати тільки багаті громадяни. У подальшому, використовуючи психічний тиск, ці «клуби» вилучають гроші і майно, водночас руйнуючи психіку людини.

Неоднозначність інтерпретації релігійних текстів дозволяє спрямовувати їх на великі аудиторії й пояснювати за їх допомогою будь-які події релігійного та суспільного життя минулого й сучасності в потрібному контексті.

9. Використовується ефект багатоканальності, коли інформація має як вербальний, так і невербальний вплив. Для цього використовуються музика, співи, прикраси тощо. Також широко застосовуються популістські заходи, такі як організація вечорів відпочинку, безкоштовні обіди, допомога у вигляді одягу, речей. І навпаки – обмеження в їжі, пости.

10. Релігійний вплив ґрунтується на засадах жорсткої ієрархії, коли всі підпорядковуються одній особі. При цьому велику роль відіграє авторитет. В основу створення переважної більшості нетрадиційних сект і подальшої діяльності покладений авторитет їх керівника. Прикладами таких об'єднань є секта Муна, відоме «Біле братство».

11. Широке використання символіки та вміння ефективно її застосовувати.

Однією із розповсюджених інформаційних загроз у суспільстві є матеріали інформаційно-психологічного впливу так звані патогенні тексти, дослідженнями яких займався Б.В. Потятиник [7]. На думку цього автора, до патогенних відносять тексти і повідомлення, які суперечать діючій ідеологічній системі. Зокрема, у різних системах цінностей патогенними вважаються тексти, що:

– спрямовані на підрив віри в Бога;
– на підрив національних та державних інтересів;
– загрожують суспільній моралі;
– загрожують глобальній безпеці;
– мають шкідливий психологічний вплив;
– призводять до нехтування основними правами та свободами.

Крім того, до патогенних текстів належать такі, що містять державну та інші види таємниці, втручаються в особисте життя тощо.

Формою патогенного тексту може виступати недобросовісна реклама.

Таким чином, інформаційні загрози суспільству можна класифікувати наступним чином:

– загрози, пов'язані з трансформаціями ціннісної системи та формуванням нових ідеологічних концепцій;
– загрози з боку патогенних текстів;
– загрози, пов'язані з негативним інформаційним впливом з боку

ЗМІ;

– загрози, пов'язані з іноземною інформаційною присутністю в Україні;

– загрози, пов'язані з негативним впливом з боку різноманітних релігійних течій;

– загрози, пов'язані із спробами маніпулювання громадською думкою з боку державної влади, фінансово-політичних кіл тощо.

Узагальнюючи викладений матеріал, далі наведемо основні *інформаційні загрози, чинники їх ескалації та можливі наслідки для суспільства і держави.*

1. *Обмеження свободи слова та доступу громадян до інформації.*

Чинники ескалації загрози:

Впровадження політичної цензури; тиск на ЗМІ з метою зміни їх політичного курсу; прояви політичного екстремізму стосовно журналістів; недостатня відкритість органів державної влади для громадського контролю; відсутність дієвих механізмів захисту прав громадян; фізичне й моральне старіння, скорочення або руйнування інформаційної інфраструктури; низька платоспроможність населення.

Можливі негативні наслідки:

Закриття опозиційних ЗМІ, розправи над журналістами; поширення необ'єктивної та неповної інформації; низька поінформованість про важливі аспекти державної політики; згортання демократичних процесів; встановлення авторитарного політичного режиму; уповільнення темпів розвитку суспільства, поглиблення відставання від розвинутих держав; міжнародна ізоляція України.

2. *Руйнування системи цінностей, духовного та фізичного здоров'я особи, суспільства, негативні зміни їх цільових настанов.*

Чинники ескалації загрози:

Негативний інформаційний вплив на (етичні та правові) засади індивідуальної та суспільної свідомості шляхом пропаганди жорстокості, насильства, порнографії, морального, правового та політичного нігілізму, вчень та релігійної практики релігійних культів тоталітарного характеру.

Можливі негативні наслідки:

Зростання злочинності, немотивованої жорстокості; соціальна апатія, маніпулювання свідомістю особи, погіршення стану її фізичного здоров'я; відсутність консолідації суспільства, міжетнічні, міжконфесійні та соціальні конфлікти.

3. *Маніпулювання громадською думкою з боку державної влади, фінансово-політичних кіл.*

Чинники ескалації загрози:

Фінансова несамостійність ЗМІ, їх залежність від впливу з боку держави, політичних сил, суб'єктів економічної діяльності, кримінальних угрупувань; вибіркова фінансова підтримка ЗМІ з боку держави; надмірна присутність державних ЗМІ в інформаційному просторі; обмежений контроль над державними ЗМІ з боку представників органів влади; монополізація окремих сегментів ринку інформаційних послуг.

Можливі негативні наслідки:

Негативний вплив ЗМІ на суспільну свідомість; поширення неправдивої конфіденційної інформації про особу, порушення демократичних принципів і норм діяльності держави; використання державних ЗМІ для здійснення впливу на хід і результати виборів (референдумів); загострення напруженості між гілками влади; встановлення авторитарного політичного режиму; негативне ставлення до України з боку світової спільноти.

4. *Обмеження можливостей органів державної влади прийняти адекватні рішення.*

Чинники ескалації загрози:

Недостатнє інформаційне забезпечення державної політики; відсутність цілісної системи інформаційно-аналітичної підтримки діяльності державних органів; ігнорування владними структурами системи громадської думки при підготовці важливих політичних рішень; ігнорування повідомлень про факти корупції, зловживань посадових осіб, порушення прав громадян; відсутність практики звернень державних органів до неурядових аналітичних структур із замовленням на аналітичну розробку певних рішень.

Можливі негативні наслідки:

Прийняття неефективних та/або помилкових державних рішень, що спричиняють значні збитки; гальмування соціально-економічного розвитку країни; зубожіння широких верств населення; відставання України від розвинутих держав; втрата підтримки з боку громадськості; відчуження суспільства від держави; масові акції протесту; посилення авторитарних тенденцій у суспільній свідомості.

5. *Порушення штатного режиму функціонування (руйнування) критично важливих інформаційних мереж, систем управління.*

Чинники ескалації загрози:

Слабка захищеність інформаційних мереж, систем управління транспортом, енергетичної та банківської сфер, державного управління, військових формувань та ін.; комп'ютерна злочинність, (комп'ютерні "віруси", атаки "хакерів", спотворення, блокування, порушення цілісності, нав'язування фальшивої інформації); радіоелектронне придушення ліній зв'язку та системи управління;

фізичне руйнування інформаційної інфраструктури, в т.ч. у результаті дій природних факторів.

Можливі негативні наслідки:

Порушення функціонування (руйнування) системи органів державної влади; банківської системи, транспорту, зв'язку, енергетики тощо; втрата керованості суспільно-політичними процесами, критично важливими галузями економіки країни; зниження боєздатності військових формувань; техногенні аварії та катастрофи з тяжкими наслідками.

6. *Несанкціонований витік таємної, конфіденційної та іншої інформації з обмеженим доступом.*

Чинники ескалації загрози:

Недостатня захищеність інформаційних мереж, автоматизованих систем управління; недостатній захист великих масивів конфіденційної інформації про особу (персональних даних), що накопичуються в різних державних і недержавних структурах; діяльність іноземних розвідок.

Можливі негативні наслідки:

Значні втрати політичного, економічного. воєнного та іншого характеру для держави; завдання моральної та матеріальної шкоди фізичним і юридичним особам; порушення авторських, немайнових прав і прав на інтелектуальну власність.

7. *Спотворення (знищення) інформаційних ресурсів, програмного забезпечення.*

Чинники ескалації загрози:

Слабка захищеність інформації з обмеженим доступом; комп'ютерна злочинність, високий рівень залежності комп'ютерних мереж від іноземних виробників програмного забезпечення.

Можливі негативні наслідки:

Завдання моральної та матеріальної шкоди фізичним і юридичним особам, державі; порушення штатного режиму функціонування (руйнування) елементів інформаційної інфраструктури та інших об'єктів.

8. *Низький рівень інтегрованості України у світовий інформаційний простір.*

Чинники ескалації загрози:

Нерозвиненість і низькі темпи розвитку інформаційної інфраструктури України; відсутність чітких і забезпечених ресурсами пріоритетів розвитку інформаційної сфери; висока конкуренція на світовому ринку інформаційних продуктів і послуг, низька конкурентоспроможність вітчизняних виробників; відплив за кордон спеціалістів у галузі інформаційних технологій; невідповідність правової системи України в інформаційній сфері основним

принципам законодавства розвинутих країн; масові порушення прав на інтелектуальну власність; неефективна податкова політика держави.

Можливі негативні наслідки:

Уповільнення темпів розвитку, зниження інтелектуального потенціалу суспільства; збільшення відставання від провідних держав у сфері інформаційних технологій; неконтрольований відплив національних матеріальних , фінансових, інтелектуальних та інших ресурсів; брак у міжнародного співтовариства об’єктивного уявлення про Україну; ізоляція України від світової економічної системи.

4.3. Сучасні технології маніпуляції суспільною свідомістю

В Оксфордському тлумачному словнику англійської мови слово маніпуляція (manipulation) трактується як поводження із об'єктами зі спеціальним наміром, особливою метою, як ручне управління, ручні дії. У переносному значенні Оксфордський словник визначає маніпуляцію як акт впливу на людей або управління ними зі зневажливим контекстом, як приховане управління чи обробка [9].

В інформаційному аспекті маніпулятивний вплив є особливим видом інформаційного впливу, при якому інформація виступає як засіб примушення особистості до здійснення вчинків, які є невластивими або неприйнятними для неї.

У загальному випадку маніпуляція може призвести до таких наслідків руйнування людської свідомості:

- некритичне сприйняття інформації та подій, що відбуваються;
- неадекватне розуміння ситуації;
- байдуже сприйняття подій;
- викривлення уявлень про події;
- маніакальне споживання інформації;
- страх перед інформацією (інфофобія) тощо.

Небезпека реалізації інформаційних загроз значно зростає через застосування різноманітних методів, методик і прийомів маніпулятивного інформаційно-психологічного впливу з урахуванням їх дії на суспільну та індивідуальну свідомість. Основні технології маніпуляції суспільною свідомістю розглянемо далі.

Під *негативними технологіями маніпуляції суспільною свідомістю* будемо розуміти можливі деформації системи масового інформування і поширення дезінформації, які ведуть до потенційних порушень суспільної стабільності, нанесення шкоди здоров'ю і життю громадян, унаслідок пропаганди чи агітації, що збуджують соціальну, расову, національну чи релігійну ненависть і ворожнечу. Ці впливи,

усвідомлювані чи неусвідомлювані, як показує життя, можуть призводити й у дійсності призводять до серйозних порушень психічного і фізичного здоров'я громадян, розмиванню природних і культурно-заданих норм поводження, до росту ризикованих соціальних і особистісних ситуацій.

4.3.1. Інформаційно-пропагандистський вплив на суспільство

Радянський енциклопедичний словник визначає поняття пропаганда в широкому і в узькому розумінні. В узькому розумінні пропаганда трактується саме як технологія впливу на суспільство.

Пропаганда (від лат. propaganda – те, що підлягає розповсюдженню) – розповсюдження політичної ідеології, наукових, релігійних тощо поглядів з метою формування у мас заданого світогляду [10].

Принциповою особливістю пропаганди є нав'язування інформації зверху від суб'єкта до об'єкта, тобто реалізація спрямованості комунікації „зверху – донизу". Ефективність такого впливу буде визначатися тим, наскільки суб'єкт впливу є авторитетним для об'єкта впливу [11]. Тому принципово важливим моментом для пропаганди є максимальне завищення статусу суб'єкта. Існування пропаганди як основної технології управління (маніпулювання) суспільством має ряд обмежень, а саме:

– узгоджене ієрархічне несуперечливе подання інформації від суб'єкта;

– постійне формування позитивного іміджу й авторитету суб'єкта у всіх членів суспільства незалежно від вікової групи, починаючи з дитячого садочка;

– блокування альтернативної інформації ззовні, тобто такої інформації, яка не збігається з цілями суб'єкта.

Дотримання першого обмеження обумовлює наявність інституту цензури всієї суспільної інформації. Так в колишньому СРСР будь-які інформаційні продукти, які були призначені для споживання суспільством, мали пройти цензуру з боку відповідних органів, і тільки після цього їх випускали в інформаційний простір країни. Інститут цензури дозволяв блокувати доступ будь-якої інформації, яка б ставила під сумнів авторитет суб'єкта (основним авторитетним суб'єктом в СРСР, від імені якого подавалася інформація членам суспільства, була Комуністична партія) або цілі й наміри суб'єкта. Те, що комунізм є єдиним в світі справедливим суспільним ладом, а Комуністична партія єдиним провідником ідей комунізму, знали діти вже дитячому садочку. Далі ця ідея закріплювалася на протязі всього

життя людини через вибудувану пропагандистською машиною систему знань про навколишній світ. Важливим обмеженням є позбавлення права доступу до альтернативної інформації, тобто інформації, сформованої іншим суб'єктом. Коли людина має доступ до інформації, яка висвітлює різні погляди (бажано полярно різні) на події, то спрацьовує механізм порівняння, який і є основою критичного сприймання інформації. Тому в основі інформаційної політики колишнього СРСР лежала політика «залізної завіси», яка повністю блокувала пряме (безпосереднє) проходження інформації із-за кордону, навіть із країн соціалістичного табору.

Дотримання перерахованих обмежень дозволяє країнам з тоталітарним режимом пропаганду зробити ефективною технологією стійкого управління суспільством. Так було в СРСР, в фашистській Німеччині, ряді інших країн. Порушення обмежень унеможливлює існування пропаганди як пануючої технології маніпуляції суспільною свідомістю і може призвести до повного падіння режиму. Так проголошення М.С. Горбачовим в СРСР принципів демократії і гласності підривало не лише авторитет Комуністичної партії як головного суб'єкта впливу, але й значною мірою сприяла розвалу Радянського Союзу, оскільки держава була позбавлена ідеологічної надбудови, стару ідеологію знищила гласність, а досвіду побудови демократії не було.

У сучасному суспільстві можна виділити наступні форми пропаганди, які досить ефективно діють і в умовах демократичного суспільства:

– *агітація*. Класичним прикладом є передвиборчі агітації, які пропагують політичні програми виборчих блоків. Завищення статусу суб'єкта базується здебільшого на обіцянках, чим більше може забезпечити суб'єкт для виборців, тим вище його статус;

– *чутки, плітки* є невід'ємним елементом у структурі неформальної комунікації будь-якого суспільства. Вони являють собою недостатньо перевірені відомості невідомого походження, передані в процесі міжособистісного спілкування. Розповсюдження чуток в суспільстві здійснюється через створення авторитета суб'єкту, хоча при цьому сам суб'єкт може залишатися анонімним. Класична схема розповсюдження чуток через ЗМІ наступна – «*з компетентних джерел* стало відомо». Поширеність чуток, пліток у суспільстві свідчить про те, що вони виконують деякі важливі соціальні функції. Вони сприяють ідентифікації особистості в соціумі, з одного боку, і підвищують однорідність думок у групі, з іншого. Внутрішньо-групове обговорення чуто сприяє кристалізації загальної точки зору. Чутки відіграють важливу роль у конфліктах різного роду: міжгрупових, міжнаціональних, міжнародних. Їхня значимість пов'язана з тим, що

в у багатьох випадках можливості впливу конфліктуючих сторін одна на одну істотно обмежені як законодавчими рамками, так і суспільною думкою. Крім того, часто результат конфлікту зважується в процесі легітимізації найбільш розповсюдженої в суспільстві точки зору. При цьому зростає значимість тих прийомів інформаційно-психологічного впливу, які пов'язані зі зміною уявлень про конфлікт у більшості в напрямку, вигідному для однієї з конфліктуючих сторін. Подібні зміни здійснюються за допомогою спеціально підібраних відомостей, розповсюджуваних як каналами ЗМІ, так і каналами неформальної комунікації. Саме останніми передаються чутки, які стають серйозною зброєю в політичному чи ідеологічному зіткненні. У порівнянні з використанням ЗМІ використання неформальної комунікації навіть переважніше, оскільки відсутні відомості про їхнього автора. Це зменшує підозри в політичній ангажованості чуток і сприяє тим самим його більшій ефективності;

– *виховання.* Процес виховання (особливо в сім'ї) базується на апріорно заданому авторитеті суб'єкта. Так дитина на початковому етапі ще має власного досвіду й користується досвідом (порадами) батьків, які прищеплюють правила поведінки в суспільстві, суспільні цінності тощо;

– *реклама.* Деякі види реклами також використовують прийоми завищення статусу суб'єкта (як правило, в якості суб'єкта можуть виступати міжнародні асоціації, виробник з великим досвідом тощо).

4.3.2. ПР-технології на службі маніпуляції суспільною свідомістю

Паблік релейшнз (ПР) як наука, що має справу із суспільною думкою, представляють особливий інтерес для дослідників інформаційно-психологічних впливів. За думкою Г.Г. Почепцова [12] будь-яка кампанія в галузі ПР може розглядатися як інформаційна міні-війна, оскільки в ній завжди присутні агресивні цілі (не за способом досягнення, а за результатом). ПР-технологія як технологія маніпуляції суспільною свідомістю на 180 градусів змінює схему впливу пропаганди. ПР основним в комунікації вважає зв'язок від об'єкта впливу (тобто від аудиторії, народу). ПР будується навколо двох центральних понять цільова аудиторія й ключове повідомлення.

ПР як технологія маніпуляції суспільною свідомістю ефективно працює в демократичному суспільством, її батьківщиною є США. Товариство ПР Америки в 1982 р. затвердило нормативне визначення предмета ПР [13]: «*Сприяючи досягненню розуміння між окремими групами і організаціями, паблік релейшнз допомагають нашому*

складному плюралістичному суспільству приймати рішення й діяти ефективно. ПР забезпечує гармонію приватного і суспільного життя». В підручнику Королько В.Г. «Основы паблик рилейшнз» дається наступне визначення ПР.

Паблік релейшнз – спеціальна система керування інформацією (в тому числі соціальною), якщо під керуванням розуміти процес створення інформаційних привидів й інформації від зацікавленої сторони, розповсюдження готової інформаційної продукції засобами комунікації для цілеспрямованого формування потрібної суспільної думки.

Принциповою особливістю ПР є завищення статусу об'єкта впливу. Для технології маніпуляції це є небезпечним, оскільки претензії висловити нікому, все, що робиться суб'єктом, подається від імені народу (об'єкта), а тому і звинуватити суб'єкт неможливо.

Серед ефективних форм ПР, які діють в суспільстві як маніпулятивні, можна визначити наступні:

- *цілеспрямовані соціологічні опитування*;
- *прихована агітація*;
- *анекдоти*;
- *реклама*;
- *«мильні опери»*.

Соціологічні опитування є способом дізнатися громадську думку із певних питань. Метою цілеспрямованих соціологічних опитувань є *формування заданої громадської думки*, яка в подальшому може використовуватися суб'єктом для прийняття управлінських рішень. В таблиці 4.1 наведено хрестоматійний приклад цільового соціологічного опитування. В лівій й правій колонках задані протилежні цілі й показано, яким чином ставляться питання, щоб сформувати потрібне (цільове) ставлення до вирішуваних проблем.

Питання в цільовому соціологічному опитуванні ставиться таким чином, що об'єкт фактично позбавлений права вибору вирішення проблеми. Далі все дуже просто, суб'єкт «ідучи на зустріч більшості членам суспільства» вирішує проблему за результатами опитування.

Прихована агітація досить нова для України форма ПР, яка активно використовувалася під час виборів у Верховну Раду в березні 2005 року. Під час свят в поштових скриньках громадяни знаходили адресні листівки-привітання (тобто звернення із вказівкою ім'я та по-батькові) зі святами, з яких вони дізнавалися, що лише їх трудами живе Україна, їм бажали подальшого успіху, натхнення тощо. В листівках-привітаннях не було жодного слова про вибори, лише підпис певного виборчого блоку (партії). Таке адресне звернення (і не просто звернення, а підняття статусу об'єкта до неомріяних висот)

напередодні виборів за своєю цільовою настановою фактично агітувало за певний блок (партію).

Таблиця 4.1.

Приклад цільового соціологічного опитування

МЕТА: СКОРОЧЕННЯ АРМІЇ	МЕТА: ЗБІЛЬШЕННЯ АРМІЇ
1. Чи вважаєте Ви: воєнний конфлікт – кращий спосіб розв'язання протиріч? 2. Чи хочете Ви, щоб ваші діти загинули на війні? 3. Чи зможе, на Ваш погляд, скорочення армії активізувати інші засоби розв'язання конфліктів? 4. Як Ви ставитеся до скорочення армії?	1. Як Ви вважаєте, незайнятість молоді впливає на ріст наркоманії та злочинності в країні? 2. Чи хочете Ви, щоб ваші діти поповнили ряди безробітних? 3. Чи вважаєте Ви, що служба в армії частково вирішує ці проблеми? 4. Як Ви ставитеся до збільшення чисельності армії?

Анекдоти. Анекдоти за своїм жанром є народна творчість (навіть незалежно від того, що їх цілеспрямовано можуть створювати певні структури). Анекдоти, як і чутки, проникає в суспільну свідомість поза контролем офіційної сфери. Анекдот є дуже привабливим як тип повідомлення, оскільки здатний самостійно розповсюджуватися. Основні цілі розповсюдження й створення анекдотів в сучасному суспільстві: створення відповідного іміджу лідеру, популяризація (розкрутка) лідерів.

„*Мильні опери*" кіно, взагалі, та «мильні опери», зокрема, будучи комерційним мистецтвом, обов'язково підстроюється під настрої масової аудиторії. „Мильні опери" використовуються як засіб відволікання верств населення від першочергових, „болючих" проблем.

Реклама реалізує як модель пропаганди, так і ПР–технологій. Якщо в рекламі сюжет побудований від імені представника «простого» народу, то реалізується ПР- технологія.

4.3.3. Нейролінгвістичне програмування

Спочатку *нейролінгвістичне програмування* (НЛП) спеціалізувалося на моделюванні методів роботи видатних американських психотерапевтів Ф. Перлза, М.Ериксона, В. Сатир [14]. Перші техніки и моделі НЛП представляли собою формалізовані прийоми їх роботи з пацієнтами. Це привело багатьох НЛП-істів в психологію і психотерапію, а психологів і психотерапевтів в НЛП. Це значною мірою пояснює те, що часто НЛП вважають напрямком в психології

або/і набором психотерапевтичних технік, не дивлячись на те, що такі визначення доволі сильно розходяться з точкою зору принаймні одного з засновників НЛП - Джона Гриндера.

НЛП – це „мистецтво і наука удосконалення особистості".

Нейро – говорить про відношення до мислення або чуттєвого сприймання тобто до процесів, які протікають у нервовій системі і грають важливу роль у формуванні поведінки людини.

Лінгвістичний – відсилає нас до мовних моделей, які є визначальними при досягненні порозуміння між людьми, на чому, власне, і тримаються всі комунікативні процеси.

Програмування – вказує на той спосіб, за допомогою якого ми організовуємо наше мислення, включаючи почуття і переконання, для того щоб в кінцевому рахунку досягти поставлених цілей – подібно тому, як ми використовуємо комп'ютер для вирішення певних завдань за допомогою відповідного програмного забезпечення.

Отже, сутність НЛП полягає в ЗМІ полягає в особливій техніці організації текстової інформації з метою утримання уваги читача, створити необхідне емоційне сприймання інформації, викликати максимальну довіру до інформації тощо і в кінцевому рахунку переконати його в необхідному ставленні до заданих подій. Основу сучасних друкованих матеріалів інформаційно-психологічного впливу складають технології і спеціальні психотехніки впливу на соціальні об'єкти, серед яких технологія нейролінгвістичного програмування особистості посідає перше місце.

Застосування НЛП в друкованих матеріалах інформаційно-психологічного впливу можна виділити 7 рівнів організації тексту, на кожному з яких є свої засоби впливу на свідомість: графічний, фонетичний, морфологічний, лексичний, синтаксичний, семантичний і логічний.

На *графічному рівні* організації тексту головна увага приділяється формі, кольору і способу подачі знаків. Цей рівень переважно впливає на загальну читаність тексту. Так, за допомогою зміни шрифтів можна або привернути увагу читача таким чином, що певна стаття не залишиться поза його увагою, або навпаки „заховати" її. Колір знаку впливає як на читаність, так і на формування надв'язуваних асоціативних зв'язків. Так, під час виборчої кампанії в деяких листівках можна було зустріти текстові фрагменти з позитивною семантикою, виділені помаранчевим кольором, а з негативною – блакитним. Спосіб подачі знаків також спрямований на утримання уваги читача. Так, на початку статті часто можна зустріти коротеньку анотацію, яка за своїм змістом містить певну інтригу, а за формою подачі виділяється жирним шрифтом, щоб привернути увагу читача.

Фонетичний рівень організації тексту впливає на емоційне сприймання тексту, а через це і до подій, що описуються в тексті. Сутність такого впливу полягає в тому, що задана комбінація звуків (а тексті – це комбінація букв) є благозвучною (приємною) для носія мови, або навпаки – неприємною (страхітливою тощо). Фонетичний рівень активно використовується для російськомовних текстів, це пов'язано з тим, що для російської мови ще 60-х роках були побудовані так звані фоно-семантичні таблиці, на базі яких на сьогодні розроблено принаймні 3 діючих фоно-семантичні системи. Сутність фоно-семантичного методу подання друкованих матеріалів інформаційно-психологічного впливу полягає в тому, що поєднання тих чи інших звуків викликають у носія даної мови негативні чи позитивні емоції (так, наприклад, російські слова, які повними синонімами «*труп*» і «*покойник*» мають зовсім інакше емоційне сприйняття. Таким чином, навіть досить нейтральний за змістом (семантикою) текст здатний викликати помітне негативне (позитивне) ставлення з боку читача. Обмеженість використання фоно-семантичних систем обумовлена тим, що для кожної вхідної мови мають бути розроблені власні фоно-семантичні системи, оскільки однакові комбінації звуків в різних мовах сприймаються по різному носіями в різних мовах.

Реалізація методів НЛП на *морфологічному рівні* організації тексту пов'язана з тим що, суфікси і префікси можуть мати самостійне семантичне значення, яке здатне змінювати семантику слова, до якого вони ходять (порівн.: *монтаж – демонтаж, інформація – дезінформація*) або надавати певного семантичного забарвлення (порівн..: *стрибати – стрибнути, працівники – працівнички*). На морфологічному рівні організації тексту, як правило, за рахунок додавання суфіксів і префіксів певного семантичного забарвлення також можна досягти заданого сприймання тексту. Так, наприклад, вживання суфіксів, які надають нейтральним словам іронічно-зневажливого значення: *"перше "чудо" … безробітні шахтарі, котрі з ризиком для життя добувають у саморобних дучках і штольнях* ***вугіллячко***" (підкреслює жалюгідний стан). Використання морфологічного рівня ефективно лише для мов з розвинутою словотвірною моделлю – російська, українська, білоруська.

Лексичний рівень організації тексту в друкованих матеріалах інформаційно-психологічного впливу представлений найбільш яскраво. Найчастіше ефект впливу здійснюється за рахунок частого повторювання слів з метою „витлумачення" потрібної інформації, вживання слів і словосполучень з прямим (тобто в тому смислі, як ми звикли вживати) негативним або позитивним значенням. Наприклад: в листівці рос. мовою: *"…озверевшие ублюдки* ***…****бьют железом по*

голове...». Широкого розповсюдження отримало також вживання всім зрозумілого специфічного сленгу. Наприклад: У статті "Подорож місцями важкого дитинства прем'єра" в описі міст Донбасу: "***бритоголові хлопці забивають косяки***"; "рівень ***беспредєла влади*** *заскалює*"; "*кандидат від влади хоче* ***засмішити*** *народ*", кореспондент агітаційної газети *"одержав редакційне завдання побувати на події районного* ***штибу",*** на карикатурі – напис на книзі: "*Закон* ***в натурі"***(«Наша столиця», 09.04.).

Розповсюджено також штучне словотворення: *прихватизація*, утворення абревіатур, які за своєю формою співпадають зі словами з прямим негативним значенням. Недоліком використання лексичного рівня організації тексту є відсутність прихованості впливу, тобто на перший план виходять емоції та їх передача з боку автора, а не керування емоціями читача. При цьому так звана пряма семантика може спричинити протилежну реакцію сприймання тексту, тобто читач, який має протилежні погляди на ту чи іншу подію, підсвідомо буде вишукувати негатив (підтвердження своїх поглядів) в тексті, де йому жорстко нав'язують те чи інше ставлення.

На *синтаксичному рівні* організації тексту вплив на читача досягається за рахунок побудови специфічних синтаксичних конструкцій. Так, психологами давно доведено, що рекурсивні синтаксичні конструкції викликають пригнічення, а прості речення сприяють активному сприйманню інформації. Дослідження художніх творів показали, що рекурсивні речення, які притаманні творам Достоєвського, викликають у читача стан пригніченості, безвихідності тощо. Найбільш розповсюджений спосіб використання синтаксичного рівня організації тексту в друкованих ЗМІ – використання громіздких синтаксичних конструкцій, що ускладнює сприймання змісту тексту і, як наслідок, читач залишає його поза увагою. Це робиться в тих випадках, коли певну подію необхідно з якихось причин висвітлити, але таким чином, щоб вона залишилась поза увагою громадськості.

Семантичний рівень акумулює негатив чи позитив, який пронизує всі рівні мовної системи, але найбільш проявляється через семантичну забарвленість лексики та їх контекстного подання. Контекстне управління семантичною забарвленістю полягає в тому, що нейтральні за семантикою слова (словосполучення) розміщуються серед слів (словосполучень) з прямою негативною або позитивною семантикою, це дозволяє шляхом встановлення штучних асоціативних зв'язків досягти позитивного чи негативного ставлення до нейтрального поняття, а через нього і до описуваного цим поняттям фрагмента реальної дійсності. Інформаційно-психологічному впливу через семантичний рівень організації тексту

притаманні такі ж недоліки, що й при впливі на лексичному рівні, а саме: присутність прямої семантики.

Логічний рівень впливає переважно на ступінь довіри до інформації з боку читача, як правило, при цьому або завищується статус суб'єкта впливу, тобто того хто впливає (така технологія отримала назву пропаганди), або завищується статус об'єкта впливу, тобто на кого впливають (така технологія отримала назву ПР-технології). Крім того, на цьому рівні значна увага приділяється відповідності „жанру", тобто текст за логікою будується таким чином, що негатив (чи позитив) нарощується під кінець до максимальної шкали.

4.4. Сучасні засоби впливу на суспільство

Друковані засоби впливу: сюди належать друковані ЗМІ та розважальна, наукова й аналітична періодика (газети, журнали, альманахи), література (дитяча, художня, наукова, спеціальна та енциклопедична), брошури, а також листівки, плакати, „бігборди" і т.п.

Вплив друкованими засобами здійснюється шляхом поширення друкованої продукції іноземними мовами, а також публікації матеріалів у засобах масової інформації своєї країни і держав-союзниць. Ця форма психологічного впливу має такі важливі особливості як доступність, наочність, різноманітність видів, здатність впливати на різноманітні масові аудиторії. Вплив за допомогою друкованих засобів вимагає достатньої кількості підготовлених творчих працівників і технічних фахівців, доброї поліграфічної бази, достатнього запасу видавничих матеріалів, а також технічних засобів доставки та поширення друкованої продукції.

Радіозасоби: вплив здійснюється шляхом передачі в ефір через радіопередавачі спеціальних радіопрограм. Це дозволяє оперативно й ефективно охоплювати масові аудиторії в межах радіуса прийому радіомовлення конкретної станції.

Жоден інший засіб масової інформації не може конкурувати з радіо за широтою охоплення аудиторії. Зараз близько 80 країн світу здійснюють радіомовлення на закордон. Програми мовлення є сукупністю різних інформаційних і публіцистичних повідомлень, структурно об'єднаних в єдине ціле і переданих протягом визначеного часу визначеним категоріям населення відповідно до поставлених цілей і завдань. Радіомовлення, як зазначається фахівцями інформаційно-психологічних операцій, має наступні переваги:

– своєрідність сприйняття інформації. Мовлення по радіо є одночасно засобом емоційного впливу (через інтонації, значеннєві паузи, акцент, порядок розміщення слів, музику, шуми) і засобом інтелектуального впливу (зміст слів);

– імітація прямого спілкування з людьми. У радіомовленні відправник інформації і її адресат знаходяться в стані акустичного контакту, завдяки чому виникає «ефект співучасті». Він зближує їх і сприяє кращому сприйняттю інформації;

– висока оперативність повідомлення інформації адресату. Витрати часу на підготовку радіопрограм звичайно незначні в порівнянні з часом, необхідним на підготовку друкованих, образотворчих, телевізійних матеріалів;

– здатність охоплювати масову аудиторію;

– широкі можливості мовлення. Радіомовлення та прийом можна здійснювати в будь-який час доби, у будь-яку погоду, за будь-яких умов. Воно дозволяє вести також і приховану (замасковану) пропаганду, тому що слухачеві (навіть професійному радисту) далеко не завжди вдається визначити істинного автора передачі;

– великий діапазон жанрів.

Засоби телебачення: вплив здійснюється шляхом передачі в ефір спеціальних телепрограм, причому будь-якої форми (новини, аналітичні та розважальні програми, мультфільми та кіно, ток-шоу, реклама та ін.) Така форма інформаційної агресії дозволяє оперативно й ефективно охоплювати масові аудиторії в межах радіуса прийому телемовлення конкретної станції. Телебачення – одна з найбільш ефективних форм інформаційно-психологічних впливів. Уже зараз більшість родин у розвинутих країнах Заходу і Сходу володіють більш ніж одним телевізором. Його роль безперервно зростає з розширенням мережі супутникового телебачення (ТБ), появою цифрового ТБ, з'єднання ТБ із комп'ютерними мережами Інтернет. Вплив ТБ на формування суспільної думки не можна порівняти з жодним іншим засобом інформації. Ефекти присутності, синхронності, причетності глядача до подій, що відбувають на екрані телевізора, змушують його вірити у правдивість наданого йому матеріалу (“краще один раз побачити, ніж сто разів почути”). ТБ здатне вводити глядача в оману навіть під час прямого репортажу. Телебачення дозволяє передавати факсимільним способом різні друковані видання, у тому числі листівки, в інші країни світу. Для цього телевізор обладнують спеціальною приставкою, з якої виходить стрічка з видрукуваною на ній інформацією, переданою на хвилях телевізійного діапазону. У випадку неможливості прямої передачі на телевізійні приймачі (чи ретрансляції передач) населення може дивитися їхній запис за допомогою відеомагнітофонів. Незважаючи

на те, що будь-який телевізійний канал у будь-якій країні й у будь-який час гранично ідеологізований і запрограмований, люди у своїй більшості сприймають телепередачі як індивідуальний засіб інформації. Їм здається, що ТБ за самою своєю природою дозволяє вільно оцінювати одержувану інформацію і робити незалежні висновки. Зрозуміло, подібна думка є колосальною оманою.

Засоби Інтернет. Internet – це глобальна інформаційно-комп'ютерна мережа. За своєю суттю це є організована на громадських засадах і самофінансована сукупність вузлів різних рівнів. Законодавства щодо діяльності у рамках Internet не існує, а це створює передумови для використання мережі з метою здійснення цільового впливу. Через практичну неможливість верифікації інформації, отриманої з мережі, а також її масовість, доступність і швидкість розповсюдження, Internet породжує 2 види загроз:

– несанкціоноване отримання інформації з обмеженим доступом (державна, комерційна чи приватна інформація) і вплив на функціонування комп'ютерів та мереж;

– розповсюдження цільової інформації з метою інформаційно-психологічного впливу.

Дуже ефективним засобом впливу є *реклама*, що здійснює одразу подвійний вплив: на рівні рекламованого об'єкту і на рівні ситуативної моделі поведінки, котра, до речі, засвоюється взагалі підсвідомо (напр., реклама шампунів чи жувальних гумок „прямим текстом" говорить про користь для здоров'я волосся чи зубів, а опосередковано створює спрощений шаблон стосунків між чоловіком-жінкою: адже варто вам скористатися цим продуктом і ви отримуєте „відмичку" (до речі, спостерігається глибоко замаскований шаблон грабіжницької поведінки) до сердець протилежної статі – саме це найчастіше і є паралельним відеосюжетом; також відбувається підміна цінностей – любити і цінувати починають не за особистісні якості людини, а лише за зовнішність).

Відеоігри є відносно новою, але вже широко використовуваною формою впливу на людей з метою трансформації в потрібному напрямку настроїв, почуттів, волі, впровадження у свідомість потрібних ідеологічних та соціальних установок, формування певних стереотипів мислення і поведінки.

Спочатку відеоігри були створені в якості тренажерів для персоналу, діяльність якого потребує швидкої реакції в обмежені інтервали часу і навчання якого на натурних об'єктах або неможливе, або потребує значних коштів. Поступово завдяки розвитку інформаційних технологій та мережі Інтернет вони перейшли до розряду елітарних розваг, а потім у масову культуру. Сьогодні ця індустрія динамічно розвивається. Світовий ринок відеоігор

оцінюється в 11 млрд. доларів на рік [15]. Стрімко зростає і кількість користувачів. За даними університету штату Айова (США), дев'ять з десяти американських підлітків грають у відеоігри, а кожного п'ятого можна назвати «комп'ютерним фанатом», або «геймером» (від англійського «game» – гра). У сучасних відеоіграх всі мультимедійні засоби (звук, колір, світло тощо) діють на гравця одночасно, доповнюючи одне одного, тому вплив на психіку посилюється багатократно. Відеоігри поринають гравця у віртуальну реальність і працюють як ефективна форма навіювання. Навіювання досягається вербальними (слова, інтонація) і невербальними (міміка, жести, дії іншої людини, оточуюча обстановка, колір, звук тощо) засобами. Оскільки відеігри мають повний набір таких засобів, то вони є практично ідеальною формою навіювання. Потужний потенціал відеоігор як форми навіювання визначив їх місце в інформаційно-психологічній боротьбі. Сьогодні комп'ютерні ігри стали одним з самих дієвих інструментів розповсюдження державної ідеології, формування національної самосвідомості громадян, створення сприятливого образу країни та її збройних сил у світі тощо. Індустрія розваг перетворилася в найпотужнішого виробника і розповсюджувача американських ідеологічних концепцій. Так США, які займають провідне місце у світовій індустрії відеоігор, створюють і розповсюджують комп'ютерні ігри, сюжет яких будується на головній ідеї – рятування світу американським суперсолдатом від різноманітних загроз, в тому числі і міжнародного тероризму. За сюжетом ігор доля всього людства залежить від дій американських солдатів. За допомогою подібного роду відеоігор формується образ сучасного військовослужбовця армії США - хоробрий, сильний, розумний воїн, здатний протистояти противнику, який значно переважає за чисельністю, ризикуючий життям заради національних інтересів країни і блага всього світу. Вони впроваджують у свідомість світової спільноти право сильного, формують толерантне відношення до жорстокості, насиллю, виробляють стереотип розв'язання конфліктних ситуацій за допомогою збої. Особливо це стосується відеоігор із жанру «стрілялок». При цьому відбувається символізація американської армії як такої, що має саме технологічне озброєння. Пропаганда має на меті переконати власний особовий склад в майбутніх перемогах, а противника в безперспективності чинити опір.

Спеціальні засоби.

1. *Психотронна зброя:* засоби прямого або непрямого дистанційного невербального впливу на психіку людини, причому об'єктом впливу може стати як окремий індивід, так і суспільна група. Основна мета використання даної зброї - повне чи достатньо

повне підпорядкування психіки людини впливові іншої людини. Побічним ефектом використання такої зброї можуть бути, наприклад, онкологічні захворювання, незворотні функціональні розлади внутрішніх органів і смерть людини, що підпала під її дію. За принципом дії психотронну зброю можна розподілити, за наявною інформацією, на 2 типи: кодову і випромінювальну.

– *Кодова зброя:* технології субліміального впливу, що подають інформацію поза пороговим рівнем природного сприйняття (технологія „25 кадру"). Єдина наукова інформація про досягнення у цій сфері – метод комп'ютерного психосемантичного аналізу, розроблений російським науковцем, „батьком російської психороніки" Ігорем Смирновим. Власне цей метод дозволяє кодувати як візуальну, так і аудіовізуальну інформацію, накладаючи необхідні вказівки чи образи на нейтральне тло (зображення, музику). Внаслідок цього вплив не усвідомлюється, але на підкірковому рівні відбувається декодування цієї інформації, завдяки чому людина потім сприймає навіяне як власні думки та рішення. Ведуться розробки і щодо „диспартного" надання сугестивної інформації – кожен кадр відеоінформації містить лише частину сугестивного образу, недостатнього для його усвідомлення. Лише при сприйнятті ряду відеокадрів відбувається „накопичення" частин образної сугестії в єдиний образ на несвідомому рівні. Єдина умова – елементи образу повинні мати спільну відмінність від загального „фону". Виявити це у відеопродукції практично неможливо, бо „картинка" створюється лише в мозку жертви.

Окрім іншого, останнім часом ведуться розробки методів і засобів комп'ютерного проникнення в підсвідомість людини й здійснення на неї глибокого впливу. Зокрема, в Інституті комп'ютерних психотехнологій Російської академії природничих наук розроблено і практикується метод проникнення в потаємні глибини підсвідомості так глибоко, «як Фрейду і не снилося». У перспективі очікується винайдення комп'ютерного психоаналізу, який дозволить контролювати свідомість, «відкривати душі, як консервні банки, змінюючи їх начинку на власний розсуд». У цьому ж ракурсі розроблявся й так званий «шолом віртуальної реальності», який рекламувався в різних друкованих виданнях. Цей шолом оснащений датчиками, через які сформовані комп'ютером сигнали можуть впливати на певні ділянки головного мозку, формуючи відповідні відчуття, емоції, ілюзії тощо. Оскільки можливості програмування ЕОМ безмежні, то безмежні й можливості цілеспрямованого впливу як на фізичний, так і на психічний стан людини.

– *Випромінювальна:*

різні типи електромагнітного випромінювання (низькочастотне,

високочастотне, надвисокочастотне та крайньовисокочастотне), дія яких ґрунтується на ефекті резонансу з біохвилями мозку та інших органів;

торсіонні та мікролептонні поля (у наукових колах щодо них точаться гострі суперечки), що діють на якісно нових засадах (переносять не масу чи енергію, а інформацію, мають практично миттєву швидкість розповсюдження у Всесвіті та всепроникність) та впливають на рівні інформаційних структур людини.

2. *Енерго-інформаційні впливи:* парапсихологічні впливи, що ґрунтуються на феноменальних здібностях окремих осіб (у даному випадку – медіумів енерго-інформаційної агресії).

4.5. Основні напрями державної політики забезпечення інформаційної безпеки суспільства

Державна політика забезпечення інформаційної безпеки України (далі політика) є невід'ємною складовою державної політики національної безпеки України і являє собою офіційно прийняту систему поглядів та практичну діяльність органів державної влади і управління, спрямовану на забезпечення такого стану соціальних суб'єктів, при якому дія будь-якої інформаційної загрози не призводить до зниження рівня їхньої інформаційної безпеки нижче припустимого, небезпечного високою ймовірністю реалізації негативних інформаційних впливів.

Політика спрямована на забезпечення гарантій прав соціальних суб'єктів в інформаційній сфері, закріплення обов'язків і відповідальності держави та її органів за інформаційну безпеку і ґрунтується на додержанні балансу інтересів всіх соціальних суб'єктів в цій галузі.

Політика є відкритою і передбачає інформування та участь соціальних суб'єктів в діяльності органів державної влади і управління в галузі інформаційної безпеки з урахуванням обмежень, встановлених законодавством України.

Політика виходить з принципу безумовної правової рівності всіх соціальних суб'єктів, незалежно від їх політичного, економічного та іншого статусу. Вона ґрунтується на обов'язковому забезпеченні прав соціальних суб'єктів на вільне створення, пошук, отримання, накопичення, зберігання, перетворення і розповсюдження інформації будь-яким законним способом.

Виходячи з принципу розподілу влади між законодавчими, виконавчими і судовими органами, політика передбачає узгодженість

рішень, що приймаються цими органами з питань інформаційної безпеки і спрямовуються на забезпечення цілісності інформаційного простору України.

Основні принципи політики:

– узгодженість практичних дій з постійними, стратегічними цілями і інтересами українського народу і держави;

– запобіжність, що орієнтується на пріоритеті недопущення, тобто попередження можливості реалізації інформаційних загроз;

– формування нормативно-правової бази, що регламентує права, обов'язки і відповідальність соціальних суб'єктів в інформаційній сфері і є прерогативою держави;

– забезпечення захисту духовної сфери суспільства від хибної, шкідливої, викривленої і недостовірної інформації;

– контроль за створенням і використанням засобів захисту інформації шляхом їх обов'язкової сертифікації і ліцензування діяльності в галузі захисту інформації;

– підтримка діяльності вітчизняних виробників інформаційних продуктів і технологій, засобів інформатизації та захисту інформації і здійснення заходів для захисту внутрішнього ринку від проникнення недоброякісних засобів інформатизації, інформаційних продуктів і технологій;

– сприяння доступу соціальних суб'єктів до світових інформаційних ресурсів;

– формування і забезпечення виконання національної програми інформаційної безпеки, яка об'єднує зусилля всіх зацікавлених суб'єктів по створенню цілісної системи інформаційної безпеки України;

– забезпечення інформаційного суверенітету і цілісності інформаційного простору України;

– створення та розвиток національних інформаційних ресурсів;

– всебічний розвиток української мови як основного інструменту перетворення накопичених людством знань в інформаційний ресурс України.

Процесуальні основи політики:

– обмеження доступу до інформації є виключенням із загального принципу відкритості інформації і здійснюється тільки на основі законодавства України;

– відповідальність за зберігання інформації, її таємність і засекречування персоніфікується в установленому законом порядку;

– доступ до будь-якої інформації, а також встановлені обмеження доступу здійснюються з урахуванням законності прав, які визначаються власністю на цю інформацію.

Політикою передбачаються заходи і формуються механізми погодження інтересів соціальних суб'єктів в інформаційній сфері шляхом створення і організації ефективної праці науково-консультативних і суспільних структур на основі принципів професіоналізму, демократії і гласності. Механізми реалізації політики забезпечують гнучкість, ефективність, своєчасність і адекватність реакції на зміни, що відбуваються в державі та світі.

Основними напрямами забезпечення політики є:

– правове забезпечення;
– науково-технічне забезпечення;
– ресурсне забезпечення;
– організаційне забезпечення.

Держава розглядає правове забезпечення як головний і пріоритетний напрямок у формуванні механізмів реалізації політики інформаційної безпеки в Україні.

Правове забезпечення базується на фундаментальних принципах сучасного права (верховенство права, презумпція невинності, додержання законності, забезпечення балансу інтересів суб'єктів права, невідворотність покарання) і включає:

– нормотворчу діяльність в галузі створення законодавства, регулюючого відношення в системі забезпечення інформаційної безпеки;

– виконавчу і правничу діяльність в системі виконання законодавства в галузі інформаційної безпеки.

Нормотворча діяльність в цій сфері передбачає:

– оцінку стану діючого законодавства і його удосконалення;

– формування правового статусу всіх соціальних суб'єктів в системі інформаційної безпеки і визначення їх відповідальності за порушення інформаційної безпеки України;

– розроблення правових механізмів створення і функціонування системи забезпечення інформаційної безпеки України, в тому числі і механізмів, регулюючих збір і аналіз даних про вплив інформаційних загроз, їх наслідки;

– порядок ліквідації наслідків і відновлення порушених прав і ресурсів, реалізацію компенсаційних заходів.

Виконавча і правнича діяльність передбачає розроблення і реалізацію:

– процедур застосування законодавства і нормативних актів в системі забезпечення інформаційної безпеки, в тому числі і до соціальних суб'єктів, відповідальних або звинувачуваних у вчиненні злочинів і проступків в даній сфері;

– переліку правопорушень з урахуванням специфіки кримінальної, громадянської, адміністративної і дисциплінарної відповідальності.

Науково-технічне та ресурсне забезпечення політики спрямоване на розроблення наукових основ, програмних і технічних засобів, які забезпечують нормальне функціонування системи інформаційної безпеки України, і реалізується шляхом формування і виконання державних цільових програм і окремих проектів в даній галузі, що є невід'ємними частинами національної програми інформаційної безпеки. З цією метою в Україні створюється відповідна науково-дослідна, дослідно-конструкторська та інформаційна бази, що забезпечує:

– розроблення концептуальних основ політики, методології основних положень системи інформаційної безпеки і її допустимих рівнів;

– дослідження і розроблення нових засобів, моделей, алгоритмів, технічних і програмних засобів, технологій і організаційних рішень, які забезпечують інформаційну безпеку України на сучасному науково-технічному рівні;

– створення сучасної комп'ютерної лексикографічної бази української мови і мов інших народів України та світу як основи для розроблення національного лінгвістичного забезпечення інформаційних систем;

– моніторинг і вивчення глобальних інформаційних процесів, підготовку для керівництва держави аналітичних матеріалів і пропозицій щодо тенденцій розвитку інформаційної сфери з метою профілактики і попередження можливих інформаційних загроз.

Організаційне забезпечення політики являє собою сукупність державних і суспільних виконавчих механізмів і структур, що реалізують вимоги інформаційної безпеки соціальних суб'єктів України на практиці. Виконавчі механізми і структури організаційно-функціонального забезпечення політики повинні працювати в правовому полі інформаційного законодавства України, володіти необхідною функціональною повнотою і мати повноваження від держави на виконання своїх функцій у відповідних режимах. Діяльність виконавчих структур організаційно-функціонального забезпечення політики регламентується законодавством України.

Одним з напрямків реалізації політики інформаційної безпеки може бути об'єднання суспільства навколо національної ідеї. Для цього можна створити певні національні бренди. Для побудови бренду-лідера та ефективного брендінгу варто пам'ятати, що на відміну від комерційного брендінгу, при здійснені державного, країни наголошують на своїй національній ідентичності, в той же час демонструючи спільність з «глобальними» і загальнолюдськими цінностями. Тому варто приділити більше уваги в ЗМІ історичним та археологічним дослідженням праукраїнської нації, популяризувати ці

ідеї, підтримувати вітчизняних науковців та запрошувати, зацікавлювати провідних науковців інших країн. *Можливі бренд-проекти:*

– “Подніпров'я - колиска індо-європейської цивілізації” (напр., англійські вчені Robert McCrum, Whilliam Cran та Robert MacNeil у своїй книзі "The Story of English" (1986р.) так і назвали землі сучасного Подніпров'я - "Home of Indo-Europeans"; а голова Фонду індо-тюркських досліджень (The Foundation for Indo-Turkic Studies), колишній Посол в Турції та Азербайджані (1992-1996) у статті "AZERBAIJAN: keystone in energy rich Caspian Basin" зазначає *:"This writer believes that if south Russian Steppes or the near about is taken as the home of Indo-Europeans and thus of the Aryans"*);

– ““Кам'яна могила” - найдавніша бібліотека людства”. Це одна з найстаріших пам'яток людства, малюнкам якої близько 22 тисячоліть, а писемниі пам'ятки (петрогліфи) відносять до протошумерських письмен давниною VI-IV тис. до н.е. Написи і малюнки не мальовані, як у Кроманьйоні чи Неандерталі, а висічені на каменях. Відомий дослідник цієї пам'ятки - А. Кифішин, - розшифрував календар Кам'яної Могили, якому понад 14 тисяч років, а також з'ясував, що протошумерські піктограми "зерно", "ячмінь", "плуг", "колесо" вперше з'явилися на Кам’яній Могилі, в Подунав’ї та Придністров’ї в V-IV тис. до н. е.. Проте унікальну пам'ятку наразі змушені тримати засипаною піском від розграбувань, адже забезпечити належного догляду не можуть. Продажем квитків заповідник заробляє лиш кілька тисяч гривень на рік, а щоб оформити для екскурсій хоча б одну печеру, потрібно кілька десятків тисяч гривень. А можна було б перетворити заповідник у історико-культурний центр світового значення, що за кілька років міг би приносити значні прибутки до бюджету як туристичний об'єкт).

Популяризація ідей прадавності української нації не суперечить позиціюванню себе сьогодні як молодої і перспективної країни. Використовуючи теорію циклічності розвитку народів та цивілізацій, можна б було створити потужній бренд давньої нації, що зазнала розквіту ще за шумерських часів (на табличках шумерських архівів згадується про могутню і багату державу Аратту, з якою підтримувалися дуже тісні зв'язки ранні шумерські правителі. Між Араттою і Шумером велися інтенсивні торгівельні відносини, з метою підвищення ефективності яких було створено перше письмо (це розповідається в шумерській поемі "Енмеркар і правитель Аратти"); А. Кифішин стверджує, що він виявив піктограму "Аратта" серед написів Кам'яної Могили. Розповівши в одній зі своїх статей про протошумерські знаки, виявлені на Подунав’ї європейськими вченими понад 50 років тому, Кифішин висловив припущення, що

згадувана шумерами Аратта є Трипіллям. Цікаво, що серед знаків-символів, які українські археологи знайшли на трипільському посуді, є відомі давнім шумерам зірка Іштар, знаки "рослина", "вода", "будинок".). “Захід нації” відбувся в період “втрати державності”, але, маючи потужній потенціал, українці наразі переживають новий “світанок”, новий етап розвитку, коли всі найбільші досягнення попереду.

Такий підхід до етногенезу українців дає змогу: відродити почуття власної гідності і самоповаги; змінити погляд на світову історію розвитку цивілізацій; вигідно позиціонувати себе на міжнародній арені; визначити та поширювати позитивну систему цінностей (щодо українських цінностей можуть траплятися твердження про притаманну українцям заздрість, принцип „моя хата скраю – нічого не знаю”, зиск та хитрість; але якщо проаналізувати історичний розвиток, міфологію, пісенну спадщину давніх українців, то побачимо, що у них закладенні зовсім інші цінності – добро, взаємна підтримка, неприйняття підлоти і зради, любов і повага до праці, а ще – до краси духовної. Тож куди все це зникло?).

Серед інших заходів варто назвати:

1. Формування внутрішнього іміджу держави у власних громадян, національну свідомість, відчуття причетності кожного до побудови іміджу держави.
2. Організація постійного моніторингу та своєчасну протидію маніпулятивним інформаційно-психологічним впливам (ця проблема яскраво виявилася під час «газового конфлікту» 2006 року, коли протягом 1-14 січня навіть провідні національні канали перебували у стані «новорічної ейфорії», а керівництво держави не змогло дати гідну відповідь).
3. Здійснити перенесення внутрішнього потенціалу України (у економічній, технологічній, інтелектуальній, інформаційній сферах) у зовнішній.

Та головне - це відповідність створеному іміджу та задекларованим цінностям у реальному житті. Адже бренд – це віртуальна структура зі специфічним надконцентрованим значенням, а отже у реальності кожний символ бренду має розгортатися і поглиблюватися, стверджуючи відповідність репрезентованим значенням.

Висновки

Сучасний рівень знань та технологічні можливості надали такої різноманітності каналам і формам інформаційно-психологічного

впливу, що не буде великим перебільшенням говорити про глобальні масштаби його використання. На користь привабливості застосування інформаційно-психологічного впливу свідчать такі його переваги в порівнянні з відомими зразками зброї масового ураження:

– *Масовість впливу.* Вже зараз розміри телеаудиторій при показі окремих подій перевищують рубіж у два мільярди. І цей показник має тенденцію постійного зростання;

– *Вибірковість впливу.* Методи інформаційно-психологічного впливу дозволяють, використовуючи ті ж самі канали, впливати як на окрему державу, так і організувати дискредитацію, наприклад, окремих верств суспільства або відтворити бажаний імідж політичному діячу тощо.

– *Висока рентабельність засобів.* Інформаційна зброя надана суспільству самою природою, вона не потребує великих капітальних вкладів, а ефективність від її застосування може мати вирішальне значення. Крім того, її застосування не руйнує матеріальні цінності країни, які є метою впливу, і при вдалому використанні дає слухняну робочу силу (людський ресурс).

– *Практична відсутність міжнародних правових актів* щодо заборони та регламентації засобів, методів та форм впливу (це пов'язане, в першу чергу, з *прихованою дією*: так, інформаційно-психологічний вплив легко прикрити боротьбою ідей, полемікою з опозицією, приватними висловами, привабливими ідеями: типу відкритого суспільства, тощо) **.**

Потрібно зазначити, що без необхідного контролю залишаються й різні канали інформаційного впливу на осіб, які приймають рішення у сфері державного управління. Зокрема, необхідна організація рефлексивного аналізу потоків вхідної інформації й процесів її обробки з метою виявлення загрози потенційного управління особами, що приймають рішення.

Глосарій до розділу

Маніпуляція – 1) (в прямому значенні) поводження із об'єктами зі спеціальним наміром, особливою метою; ручне управління, ручні дії. 2) (у переносному значенні) акт впливу на людей або управління ними зі зневажливим контекстом, як приховане управління чи обробка.

Масова свідомість – вид свідомості суспільства, що визначає співпадіння в якийсь момент основних і найбільш значущих компонентів свідомості значної кількості різноманітних «класичних» груп суспільства (великих і малих).

Національна свідомість – сукупність соціальних, політичних,

економічних, етичних, естетичних, філософських, релігійних та інших поглядів та уявлень, що характеризують зміст, рівень та особливості духовного і культурного розвитку населення країни.

Нейролінгвістичне програмування (НЛП) – набір спеціальних психотехнік інформаційно-психологічного впливу на особистість з метою досягнення поставлених цілей.

НЛП – це „мистецтво і наука удосконалення особистості".

Нейро – говорить про відношення до мислення або чуттєвого сприймання тобто до процесів, які протікають у нервовій системі і грають важливу роль у формуванні поведінки людини.

Лінгвістичний – відсилає нас до мовних моделей, які є визначальними при досягненні порозуміння між людьми, на чому, власне, і тримаються всі комунікативні процеси.

Програмування – вказує на той спосіб, за допомогою якого ми організовуємо наше мислення, включаючи почуття і переконання, для того щоб в кінцевому рахунку досягти поставлених цілей – подібно тому, як ми використовуємо комп'ютер для вирішення певних завдань за допомогою відповідного програмного забезпечення.

Паблік релейшнз – спеціальна система керування інформацією (в тому числі соціальною), якщо під керуванням розуміти процес створення інформаційних привидів й інформації від зацікавленої сторони, розповсюдження готової інформаційної продукції засобами комунікації для цілеспрямованого формування потрібної суспільної думки.

Пропаганда (від лат. propaganda – те, що підлягає розповсюдженню) – розповсюдження політичної ідеології, наукових, релігійних тощо поглядів з метою формування у мас заданого світогляду.

Свідомість – вищий рівень психічного відображення людиною об'єктивної дійсності, що відрізняється: активністю, обробкою потоків інформації, взаємодією з навколишнім світом; спрямованістю на предмет; здатністю до самоспостереження та самопізнання психічних актів і станів; мотиваційно-ціннісним характером; різним ступенем ясності.

Суспільна свідомість – погляди, які визначають спільні інтереси погляди, переконання, ідеї та переконання, які склалися в суспільстві на певному етапі історичного розвитку. Суспільна свідомість виступає у формі політичних, юридичних, естетичних, етнічних тощо теорій, філософії, моралі, соціальних норм та інших визначаючих її форм.

Зв'язок ключових понять і термінів

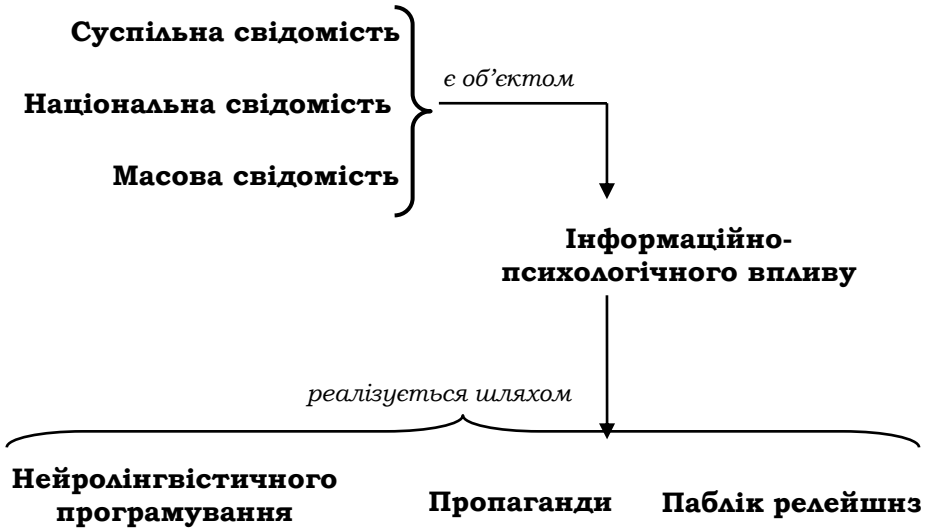


Рис.4.1.

Завдання і запитання для самоперевірки

1. Дайте визначення понять *свідомість, суспільна свідомість.*
2. Дайте характеристику рівнів суспільної свідомості.
3. Які тексти вважаються патогенними?
4. Сформулюйте тези конструювання релігійної комунікації.
5. Дайте стислу характеристику основних форм інформаційного пропагандистського впливу.
6. Які форми використовують для здійснення інформаційного впливу використовують ПР-технології?
7. Дайте стислу характеристику нейролінгвістичному програмуванню.
8. Назвіть найбільш розповсюджені інформаційні загрози суспільству та чинники їх ескалації.
9. Назвіть сучасні засоби впливу на суспільство й дайте їм стислу характеристику.

Рекомендована література до розділу

1. Інформаційна безпека держави у контексті протидії інформаційним війнам: Навчальний посібник (за ред. Толубка В.Б.). – К.: НАОУ, 2004. 176 с.
2. *Лопатин В.Н.* Информационная безопасность России: Человек. Общество. Государство. – Санкт-Петербург: Фонд «Университет», 2000.
3. *Хмельницький О.О.* Інформаційна культура: підготовка кадрів до інформаційної роботи: Навчальний посібник. – К.: КНТ, 2007. – 200 с.
4. *Почепцов Г.Г.* Информационные войны. М.: "Рефл-бук", К.: "Ваклер", 2000.
5. *Литвиненко О.В., Бінько І.Ф., Потіха В.М.* Інформаційний простір як чинник забезпечення національних інтересів України. – К.: ІМВ КУ ім. Тараса Шевченка, 1998. – 47с.
6. *Лисичкин В.А. , Шелепин Л.А.* Третья мировая информационно-психологическая война – М.: ИСПИ АСН, 2000.
7. *Королько В.Г.* Основы паблик рилейшнз. М.: "Рефл-бук". К.: "Ваклер". – 2003.- 528 с.

Використані джерела

1. *Абдурахманов М.И., Баришполец В.А., Манилов В.Л.* Военная безопасность России. Словарь-справочник. Под общей редакцией Манилова В.Л. – М.: «Пробел», 2000. – 389 с.
2. *Баландин А.Ф.* Секретное оружие Бехтерева. //" Техника молодежи", 1993, №4, с.2-5.
3. Інформаційна безпека держави у контексті протидії інформаційним війнам: Навчальний посібник (за ред. Толубка В.Б.). – К.: НАОУ, 2004. – 176 с.

4. Закон України "Про основи національної безпеки України" № 964-IV від 19 червня 2003 року
5. *Литвиненко О.В., Бінько І.Ф., Потіха В.М.* Інформаційний простір як чинник забезпечення національних інтересів України. – К.: ІМВ КУ ім. Тараса Шевченка, 1998. – 47с.
6. *Почепцов Г.Г.* Национальная безопасность стран переходного пери ода. – К., 1996. – 136.
7. *Потятиник Б.В.* Патогенний текст. – Львів, 1996. – 295 с.
8. *Почепцов Г.Г.* Информационные войны. М.: "Рефл-бук", К.: "Ваклер", 2000.

9. *Хорнби А.С.* Толковый словарь современного английского языка для продвинутого этапа: Специальное издание для СССР. Т. 2 M-Z. – 528 с.

10. Советский энциклопедический словарь /Гл. ред. А.М. Прохоров. - 4-е изд. - М.: Сов. Энциклопедия, 1986. - 1600с.

11. *Хмельницький О.О.* Інформаційна культура: підготовка кадрів до інформаційної роботи: Навчальний посібник. – К.: КНТ, 2007. – 200 с.

12. *Почепцов Г.Г.* Теорія комунікацій. – К., 1996. – 175 с.

13. *Королько В.Г.* Основы паблик рилейшнз. М.: "Рефл-бук". К.: "Ваклер". – 2003.- 528 с.

14. Методологія, теорія та практика соціологічного аналізу сучасного суспільства: Збірник наукових праць/Ред.. Якуба О.О. та ін.. – Х.: Видавничий центр Харківського національного університету ім.. В.Н. Карабіна. 2001. – 565 с.

15. В. Макаренкова Видеоигры в информационной и психологической борьбе // ЗВО, 2005/2, с. 17–25.

Розділ 5.

ІНФОРМАЦІЙНА БЕЗПЕКА ОСОБИСТОСТІ

Проблема інформаційно-психологічної безпеки особистості, її психологічної захищеності й способів формування психологічного захисту в умовах кардинальних змін суспільства стає нагальною як в теоретичному, так і у прикладному плані.

Інформаційно-психологічну безпеку особистості можна розглядати як стан захищеності її психіки від впливу чисельних інформаційних факторів, перешкоджаючих формуванню й функціонуванню адекватної інформаційно-орієнтованої основи соціальної поведінки людини (і в цілому, життєдіяльності у суспільстві), а також адекватної системи його суб'єктивного (особистісного, суб'єктивно-особистісного) ставлення до оточуючого світу й до самого себе.

5.1. Маніпулювання особистістю в різних культурно-історичних умовах

Було б помилкою вважати, що маніпулювання з інформацією, психологічні маніпулювання індивідами є надбання виключно сучасного суспільства й пов'язується лише із функціонуванням засобів масової комунікації.

У плані використання інформаційно-психологічного маніпулювання в різних сферах суспільного життя, *східна культура* має значний історичний досвід. Маніпулятивний підхід там органічно входить до воєнного мистецтва в частині прихованого керування противником, він є філософською, ідейною основою і практикою дипломатії і політики. Мистецтво складати поетапний багатокроковий план взаємодії між людьми з прихованими цілями, застосовуючи чисельні хитрощі й пастки з метою досягнення успіху, є із стародавніх часів відмітною рисою поведінки китайських державних діячів, дипломатів й полководців.

На протязі віків це мистецтво пильно приховувалося від представників інших народів. Був створений своєрідний банк даних, в якому в вигляді метафоричних схем були узагальнені й класифіковані методи маніпулятивного впливу та його використання в різних ситуаціях, що найшло своє відображення в "Трактаті про 36 стратагем". Саме поняття "*стратагема*" означає стратегічний план, в якому для противника передбачена якісь пастка або хитрощі. Розглядаючи семантику даного поняття, В.С.Мясніков

звертає увагу на то, що в китайській мові це поняття означає ще й кмітливість та винахідливість [1]. Харро фон Зенгер, автор монографії “Стратагеми. Про китайське мистецтво жити й виживати. Знамениті 36 китайських стратагеми за три тисячоліття” [2], обґрунтовує, що термін стратагема найбільш є адекватним відповідному поняттю у китайській мові. Аналізуючи зміст поняття “стратагема” в європейських мовах він показує, що його основним значенням є не тільки воєнні, але й будь-які хитрощі, прийоми чи інтрига з метою досягти певних переваг. Розглядаючи це поняття, він зазначає, що “в залежності від контексту китайські ієрогліфи можуть приймати різні значення... нас цікавлять два значення, присутні у певних типах текстів: 1) воєнні хитрощі та 2) хитрощі, пастки у політичному та приватному житті”[3, с.16-17].

Підхід до міжособистісної комунікації на Сході, зокрема, в Китаї нараховує тисячоліття й є невід’ємною частиною суспільної, національної та індивідуальної психології. Про це свідчать історичні джерела, що дійшли до наших днів [3]. В найбільш концентрованому вигляді, у лаконічній та метафоричній формі маніпулятивний підхід описаний близько двох з половиною тисяч років тому назад у “Трактаті про воєнне мистецтво”, автором якого вважається видатний китайський полководець і державний діяч, відомий під ім’ям Сунь-цзи. В останній час фахівці вважають, що під літературно-філософським псевдонімом Сунь-цзи виступав видатний полководець-"стратагемщик" Сунь Бинь, що жив у IV в. до н.е. у стародавньому китайському царстві Ци [4]. Стратагемність в цьому трактаті виступає як мистецтво психологічного протиборства, якому притаманні свої закони. На двадцяти сторінках Сунь-цзи дає основні положення й поради як має думати й діяти полководець, відстоюючи інтереси своєї держави, які відбивають суть маніпулятивного підходу й стратагемного мислення.

Про роль, значення та вплив ідей Сунь-цзи може свідчити, зокрема, той факт, що за дві з половиною тисячі років після виходу трактату, стосовно нього було написано й видано декілька сот коментарів. Якщо висловлюватися сучасною мовою інформаційно-комунікативних процесів, то можна сказати, що ця невелика праця породила на протязі віків потужну інформаційну хвилю, що стала феноменом східної культури й особливістю національної психології ряду східних країн, які є важливою частиною світової цивілізації.

Розглядаючи роль й історичне значення трактату для розвитку теорії й практики державного управлення, Н.І.Конрад підкреслює, що “є один специфічний бік цього трактату, який значною мірою зобов’язаний такою широкою популярністю. Багато з його положень завжди легко переносились із сфери війни в сферу політики й

дипломатії. Тому трактат Сунь-цзи має виключне значення для розуміння не тільки для військових, але й політиків країн Далекого Сходу, та до того ж не тільки в стародавні часи”[4, С.10].

Ідеї цього трактату використовуються сьогодні не тільки на Сході, але й в розвинутих країнах Заходу, зокрема, при організації ведення психологічної війни, психологічних операцій, тайних й спеціальних операцій, в діяльності спецслужб.

Колишній директор Центрального розвідувального управління (ЦРУ) США Ален Даллес, один із засновників й ідеологів американської розвідки, підкреслював, що заслуга Сунь-цзи не тільки у тому, що він першим дав кваліфікований аналіз методів шпіонажу, але й у тому, що він першим виклав рекомендації щодо організації розвідувальної діяльності, включи мистецтво контррозвідувальних операцій, теорію й практику психологічної війни, в яких основним було керування противником. За його словами, Сунь-цзи належить чітка концепція операцій щодо введення противника в оману й забезпечення власної безпеки, а “коротко все мистецтво розвідки”[5, с. 16-17].

Цікавими в цьому плані й поради колишнього президента США Р. Ніксона при призначенні Дж. Буша в 1975 р. директором ЦРУ. В своєму листі Р. Ніксон рекомендував Дж. Бушу звернути особливу увагу на спадок у сфері розвідки стародавнього китайського стратега Сунь-цзи, де головним, за думкою Ніксона, була теорія “керування противником". Ніксон навів один із афоризмів Сунь-цзи, що як би висловлював основну суть його листа: "Вершина мистецтва - це не вигравати сто битв, а, напроти, підкорити армію противника без битви”[6, с. 209].

Слід зазначити, що маніпулятивний підхід присутній не тільки в Східній культурі, але й з урахуванням конкретних історичних умов і традиційних цінностей інших культур, має свою специфічність, інші масштаби розповсюдження й впливу на суспільну й індивідуальну психологію, національні традиції різних країн.

Опис прийомів маніпулятивного впливу на особистість знайшло своє відбиття в роботах авторів різних країн і культур в різні історичні періоди. В античні часи - про це, зокрема, писав Аристотель ("Про софістичні спростування") [7]. В ті часи існував цілий напрямок, відомий як софістика. Достатньо відомі роботи Макіавелі, Шопенгауера, зокрема, в його книзі "Евристична діалектика" перераховуються 36 риторичних прийомів. У Росії в 1918 р. вийшла праця С. Поварніна "Спір. Про теорію й практику спора", в якій аналізуються методи маніпулювання та їх застосування в різних ситуаціях обговорень та публічних дискусій. Широко відомі книги Д. Карнеги, в яких розглядаються чисельні прийоми міжособистісної комунікації, в тому числі й маніпуляцій [8-10].

Розглядаючи це явище як феномен світової культури, Х. Зенгер, зокрема, відзначає: “Стратагеми, тобто неортодоксальні шляхи досягнення воєнних, цивільних, політичних, економічних або особистих цілей, є загальнолюдським феноменом. Однак, у зв’язку з деякими культурними й релігійними умовами, на Заході майже відсутні дослідження цієї теми. Розуміння стратагемності на Заході розвинуто слабко. Представники Заходу певною мірою вражені “стратагемною сліпотою”, хоча в своєму повсякденному житті вони постійно є жертвами стратагем й часто самі застосовують їх в залежності від ситуації, іншими словами, без всякої теорії й попереднього розрахунку”[2, с.18].

В той же час деякі історичні джерела свідчать, що в певних колах суспільства європейських країн стратагемний підхід не був новинкою й здійснювалися спроби поєднати його із християнською мораллю й цінностями. Про частково свідчать деякі афоризми з твору під назвою "Кишеньковий оракул або наука розсудливості" з підзаголовком - “Афоризми, вилучені із творів Лоренсо Грасіана", який був виданий в середині сімнадцятого століття (1647 р.) й отримав розповсюдження в ряді європейських країн. Особливо яскраво знайомство з маніпулятивним підходом проявляється, зокрема, в таких афоризмах, як: "*Діяти виходячи із задуму*", *"Змінювати прийоми, відволікаючи увагу", "До кожного знаходити свій ключ"* тощо [11, с.17-21].

Таким чином, європейська й американська культури пізніше в історичному плані визнали користування у масовому масштабі такого гострого психологічного засобу, як маніпулятивний вплив. Можливо, що саме брак історичного досвіду, відносна молодість сучасної західної культури й поясняють відсутність у людей, включених у цінності цієї культури, ефективної системи соціально-психологічного захисту від маніпулятивного впливу.

Тому в Західному суспільстві існує протиріччя між проголошеними цінностями та практикою використання психологічних маніпуляцій, і так боляче переживаються людиною їх наслідки. Про руйнівний характер такого впливу на особистість свідчить, з одного боку, збільшення побутової конфліктності й агресивності, з іншого, - зріст психічних розладів і неврозів у людей. Про це образно й емоційно пише американський психолог и психотерапевт Еверет Шостром, полемізуючи з Дейлом Карнегі й відзначаючи маніпулятивний характер багатьох його рекомендацій. “Намагайтесь уникати конфліктів... контролюйте себе... приймайте це легко”, - постійно радить Дейл Карнеги. “Що ж, попробуйте, але коли ви, вимотав до останнього свою нервову систему, прийдете до мене лікуватися, я вам дам прямо протилежну пораду”, - так пише Э. Шостром в своїй книзі

“Людина-маніпулятор”, яка стала бестселером у багатьох країнах світу[12, с.47].

5.2. Механізми сприймання інформації людиною

Центральним поняттям при визначенні розуміння механізмів процесу сприймання інформації людиною є *психіка*. Психіку людини можна умовно розділити на дві складові: свідомість і підсвідомість. Свідомість є вищим рівнем психічного відображення, властивого тільки людині як суспільно-історичній істоті.

5.2.1. Свідомість і підсвідомість особистості, механізми їх взаємодії

Оточуючий людину матеріальний і духовний світ виступає зовнішнім подразником, який відображається в психіці людини у вигляді ідеальних образів. Раніше, за часів марксистсько-ленінської ідеології, існувала аксіома про те, що свідомість сформувалась у ході суспільно-історичного розвитку на основі праці як специфічного виду людської діяльності. Вона являє собою таку функцію людської психіки, сутність якої полягає в адекватному, узагальненому, цілеспрямованому активному відображенні, що здійснюється в символічній формі, й творчому перетворенні зовнішнього світу, у зв'язку вражень, що постійно надходять, із попереднім досвідом, у виділенні людиною себе з навколишнього середовища і протиставленні йому як суб’єкт об’єкту. Свідомість полягає в емоційній оцінці дійсності, забезпеченні діяльності цілеполягання – у попередній побудові дій та передбаченні їхніх наслідків, у контролюванні поведінки й керуванні нею, у здатності особистості давати собі раду в оточуючому матеріальному світі, у власному духовному житті.

Звичайно, у даних положеннях є раціональне зерно, оскільки людина позбавлена соціальної інформації буде людиною у фізіологічному відношенні, проте особистістю, у прийнятному для нас розумінні, вона не стане. Тобто відображати реальну дійсність в абстрактно-понятійних образах така людина не зможе. Поряд з цим на сьогодні серед вчених все більше виникає сумнів щодо теорії еволюціонізму виказаної Ч. Дарвіним.

Цікавою в даному відношенні є точка зору дослідника Друнвало Мельхіседека, який обґрунтовує теорію “панспермії”, тобто опліднення Землі життям в тому числі і свідомістю із Космосу. Він обґрунтовує, що походження та особливості людської свідомості, розміри і віддаленість

зірок, планет і супутників, як і все, що створено людиною, бере свій початок від чудового Божественного створіння “Квітки Життя”[13].

Отже, свідомість – не просто образ дійсності, а особлива форма психічної діяльності, орієнтована на відображення та перетворення дійсності. Психічна діяльність залежить від накопичення людиною знань. Свідомість постає як *знання* про зовнішній і внутрішній світ, про самого себе. Однак свідомість не зводиться тільки до знання, не тотожна йому.

Свідомість виявляється не лише в узагальненому знанні навколишньої дійсності, а й у певному оцінковому, теоретичному і практичному ставленні до неї. Тому іншою необхідною складовою свідомості є *переживання* людиною того, що для неї в навколишній дійсності є значущим. Переживання свідчать про оцінку людиною оточуючого світу, вираження свого ставлення до нього, до власної діяльності та її результатів, до інших людей, до того, що задовольняє або не задовольняє її потреби, відповідає чи не відповідає її інтересам, уявленням і поняттям. Людина усвідомлює не тільки об’єкти, їхні властивості та зв’язки, а й їхню значущість для себе, суспільства, тим самим створюючи умови для розгортання цілеспрямованої діяльності.

Свідомість не дана людині від народження. Вона формується не природою, а суспільством. З’явившись на світ, дитина ще не здатна відразу суб’єктивно відокремити себе від зовнішнього світу, вона немовби “розчинена” в ньому. Її свідомість складається поступово через усвідомлення в процесі життєдіяльності багатств, накопичених суспільством.

Усвідомлення – це фокусування свідомості на психічних процесах, на тих чуттєвих образах дійсності, які особистість завдяки їм отримує. В основі усвідомлення лежить узагальнення власних психічних процесів, що приводить до оволодіння ними. Іншими словами, усвідомлювати - це осягати розумом, сприймати свідомо, розуміти значення, сенс чогось.

У загальному вигляді характеристику процесу усвідомлення психічних процесів можна уявити наступним чином:

– по-перше, людина може усвідомити те, що сприймає, згадує, про що думає, що заслуговує її уваги;

– по-друге, людина може усвідомити, що це саме вона сприймає, згадує, мислить, відчуває. Однак усвідомлення психічних процесів не означає , що людина завжди усвідомлює зміст свого сприймання, мислення, уваги та себе в цьому процесі [5].

Актуально усвідомленим є лише той зміст психіки, який виступає перед особистістю як предмет, на який безпосередньо спрямована увага, та чи інша її дія. Інакше кажучи, для того, щоб зміст, який сприймається, був усвідомлений, потрібно, щоб він зацікавив людину і

став метою її дії. Тільки порівняння ідеального та реального, бажаного й дійсного, мети і мотиву веде до усвідомлення.

Механізми усвідомлення досить складні та вимагають спеціального розгляду. У загальному вигляді його характеристика сформульована у "законі усвідомлення" Е. Клапареда: чим більше ми користуємося яким-небудь відношенням (між предметами, явищами, поняттями), тим менше ми його усвідомлюємо. Або інакше: ми усвідомлюємо лише в міру нашого невміння пристосуватися. Чим більше будь-яке відношення застосовується автоматично, тим важче його усвідомити.

Справді, у звичайних ситуаціях людина зовсім не замислюється, що те, що вона бачить, – це не сам по собі зовнішній світ, а зоровий образ зовнішнього світу. Інакше кажучи, людина не усвідомлює власний процес сприйняття. У цьому немає необхідності: людина пристосована діяти завдяки своїм зоровим образам, відношення між образом того чи іншого предмета й самим предметом, дією з ним є усталеним і використовується в процесі регуляції поведінки, діяльності автоматично. Лише коли звичне відношення з тих або інших причин ігнорується, включається процес усвідомлення.

Крім свідомих форм відображення дійсності, для людини характерні й такі, що перебувають немовби за «порогом» свідомості, не досягають належного ступеня інтенсивності або напруженості, щоб звернути на себе увагу. Терміни "несвідоме", "підсвідоме", "неусвідомлене" часто вживаються в науковій і художній літературі, а також у повсякденному житті. Інколи про людину говорять: "Вона зробила це несвідомо"; "Вона не хотіла цього, але так сталося" тощо. Часто ми звертаємо увагу на те, що ті або інші думки виникають у нас в голові мовби "самі по собі", в готовому вигляді, невідомо як і звідки.

Явища людської психіки дуже різноманітні. І далеко не всі з них охоплюються сферою свідомості. Психічна діяльність може не перебувати у фокусі свідомості, не досягати рівня свідомості (досвідомий чи передсвідомий стан) або опускатися нижче порога свідомості (підсвідоме). Сукупність психічних явищ, станів і дій, відсутніх у свідомості людини, що лежать поза сферою розуму, непідзвітні їй і принаймні в даний момент не піддаються контролю, належать до несвідомого.

Зона максимально ясної свідомості в психічній діяльності порівняно невелика. За нею починається смуга просто ясної свідомості, а потім мінімальної свідомості, за якою вже йде неусвідомлене. Останнє виступає то як потяг, то як відчуття, сприймання, уявлення та мислення, то як сомнамбулізм, то як здогадка, інтуїція, то як гіпнотичний стан або сновидіння, стан афекту чи несамовитості.

До несвідомих явищ відносять наслідування, інтуїцію і творче натхнення, що супроводжується раптовим "осяянням" новою ідеєю,

яка народжується немовби від якогось поштовху зсередини, і випадки миттєвого вирішення задач, які тривалий час не піддавалися свідомим зусиллям, і мимовільне згадування того, що здавалося назавжди забутим, та ін.

Несвідоме не є чимось містичним, його не варто уявляти як ірраціональне, "темну" силу, що затаїлася в глибинах психіки людини. Це цілком нормальна сторона психіки, особливий рівень психічної діяльності. Несвідомі процеси та явища реалізують специфічну функцію людської психіки, сутність якої полягає в адекватному відображенні людиною дійсності й ефективному регулюванні її стосунків з цією дійсністю, що відбуваються за порогом свідомості.

На відміну від свідомості несвідоме не передбачає попередньої уявної побудови дій, проектування їхніх результатів і постановки мети. Кінцевим результатом несвідомого відображення та пізнання є пристосування до дійсності, засноване на неосмисленому врахуванні інформації про властивості та відношення предметів зовнішнього світу.

Несвідомі процеси виконують певну охоронну функцію: позбавляють психіку від постійного напруження свідомості там, де в цьому немає потреби. Розум людини ніс би, мабуть, непомірно великий тягар, якби був змушений контролювати кожний психічний акт, кожний рух і дію. Людина не могла б ані результативно думати, ані розумно діяти, якби всі елементи її життєвої діяльності одночасно потребували усвідомлення.

Несвідоме як психічне явище характеризується не лише негативно – в розумінні чогось неусвідомленого (прихованого у даний момент, але здатного за певних умов з'явитись у свідомості або приреченого назавжди залишатися невиявленим). Воно має позитивну особливість: це специфічне відображення, що має свою структуру, елементи якої пов'язані як між собою, так і з свідомістю та дією, впливаючи на них і відчуваючи їхній вплив на собі.

Розглянемо деякі із структурних елементів несвідомого. Почнемо з відчуттів. Ми відчуваємо те, що впливає на нас. Але далеко не все, що впливає, стає при цьому фактом свідомості. Значна частина наших відчуттів не усвідомлюється нами, залишається підсвідомою.

Отримуючи одночасно велику кількість вражень, люди легко випускають із виду окремі з них. Так, ідучи вулицею, ми виступаємо свідками величезної кількості подій, чуємо безліч звуків, які допомагають орієнтуватися в потопі вуличного руху. Але вони залишаються поза нашою увагою до якогось утруднення чи незвичності. Нескінченна кількість речей, явищ, властивостей і відношень, що існують об'єктивно і постійно потрапляють у поле зору, не усвідомлюється нами. Якби на кожний вплив людина реагувала

усвідомлено, вона не впоралася б із цим, оскільки не здатна миттєво переключатися з одного впливу на інший або утримувати у фокусі своєї уваги практично нескінченні подразники. На щастя, ми маємо здатність абстрагуватись від одних впливів і зосереджуватися на інших, зовсім не помічаючи третіх.

Діяльність людини у звичайних умовах є свідомою. Разом із тим окремі її елементи здійснюються несвідомо або напівсвідомо, автоматично. У житті людини формуються складні звички, вміння і навички, в яких свідомість одночасно і присутня, і відсутня. Будь-яка автоматизована дія має неусвідомлений характер, хоча, зрозуміло, не кожна неусвідомлена дія є автоматизованою.

Свідома діяльність людини можлива лише за умови автоматичного здійснення максимальної кількості її елементів. Так для того, щоб майстерно володіти зброєю, потрібно мати навички й уміння, відпрацьовані за допомогою чисельних навчальних занять і вправ. А повністю зосередити свою увагу на змісті усного виступу може лише той, у кого сформований певний автоматизм самого процесу виголошення промови. Досвідчений промовець виступає без тексту і водночас реагує на реакцію аудиторії, на яку зосереджено всю його увагу.

Автоматизація функцій є суттєвою і необхідною особливістю багатьох психічних процесів (мислення, сприймання, мовлення, запам’ятовування та ін.), її порушення може паралізувати нормальний перебіг психічних процесів. Автоматизм відточує та полегшує різні види діяльності, у ряді розумових і практичних дій обслуговує вищі форми свідомої діяльності. Механізми психічної автоматизації позбавляють свідомість від постійного спостереження і непотрібного контролю за кожним фрагментом дії.

Несвідоме проявляється і в так званих імпульсивних діях, коли людина не відповідає за наслідки своїх учинків. Наші наміри далеко не завжди співпадають із нашими бажаннями. Іноді, здійснивши той або інший вчинок, людина сама не може зрозуміти, чому вона вчинила саме так. І досить часто саме про такі імпульсивні вчинки, коли їхні наслідки не прогнозувалися усвідомлено, нам і доводиться шкодувати.

Несвідоме проявляється в тій інформації, що накопичується протягом усього життя й осідає у пам'яті як досвід. З усієї суми наявних у нас знань у кожний даний момент у центрі свідомості осідає лише невелика їх частина. Про деякі знання, що зберігаються в пам'яті, люди навіть не підозрюють. Проте спеціальні дослідження показали, що в регулюванні поведінки людини значну роль відіграють враження, отримані в ранньому дитинстві і закладені в глибинах несвідомої психіки.

Формою прояву несвідомого є й так звана психологічна установка. Цей психічний феномен являє собою цілісний стан людини, який виражає динамічну визначеність її психічного життя, спрямованість особистості на активність у якомусь виді діяльності, загальний нахил до дії, стійку орієнтацію на певні об'єкти, що зберігається доти, доки очікування людини виправдовуються.

Проявляється несвідоме й в інших психічних процесах. Навіть мислення людини може протікати на несвідомому рівні. Що ж до уявлення або таких явищ, як інтуїція і творчість, то їх без участі несвідомих компонентів навіть важко собі уявити.

Таким чином можна зробити висновок, що свідоме і несвідоме є дві взаємозв'язані частини психічної діяльності людського розуму.

5.2.2. Обмеження впливу інформаційного простору на людину

Можливості впливу інформаційного простору на людину визначаються індивідуальними особливостями сприймання інформації і є досить обмеженими. Як такі обмеження виступають так звані інформаційні бар'єри. Вони є тим фактором, який обмежує ступінь впливу інформаційного простору на формування особистості. В навчальному посібнику Хмельницького О.О. «Інформаційна культура: підготовка кадрів до інформаційної роботи» [15] наводиться наступна класифікація обмежень:

– *географічні* – визначаються відстанню між джерелом та споживачем інформації;

– *історичні* (часові) – визначаються часовим проміжком між моментом появи і моментом споживання інформації;

– *державні* – визначаються як наявністю державних кордонів, так і відмінностями державно-адміністративного устрою;

– *відомчі* – визначаються, в першу чергу, функціональною структурою й функціями тих чи інших установ й організацій;

– *режимні* – є найбільш характерними для спецслужб, спрямовані на запобігання витоку конфіденційної інформації з метою охорони державної і військової таємниці;

– *економічні* – виникають як результат нестачі економічних ресурсів, необхідних для нормального обміну інформацією;

– *технічні* – виникають внаслідок недостатньої розвиненості технічних засобів, що перешкоджає руху інформаційних ресурсів;

– *мовні* – є результатом семантичної невідповідності різноманітних систем;

– *термінологічні* – виникають в результаті взаємодії різноманітних предметних областей;

– *психологічні* – є наслідком відсутності психологічної готовності з боку індивіда до сприйняття інформації;

– *резонансні* – є результатом прагматичної невідповідності інформаційних масивів потребам конкретного споживача.

До наведеної класифікації слід ще додати психофізіологічні можливості індивіда, які також виступають в ролі обмеження доступу до інформації. Фізіологічні можливості людини щодо сприйняття інформації обмежені 40-50 біт/сек. Реальна швидкість сприйняття інформації ще нижче. Зростаючі інформаційні потоки призводять до появи психологічного перевантаження і почуття дискомфорту, а в результаті часткове або повне не сприймання інформації. Тобто виникає феномен, коли в умовах «інформаційного буму» відчувається «інформаційний голод», людина занурюється в «інформаційному смітті» і не може отримати потрібну їй інформацію.

Наведені інформаційні бар'єри відіграють подвійну роль у передачі інформації від суспільства до людини. З одного боку, вони здійснюють регулюючу (позитивну) функцію, запобігають міграції надлишкових інформаційних потоків, недоцільному витоку інформаційних ресурсів. При цьому бар'єри виконують також захисну функцію, захищаючи індивіда від непотрібної для нього або навіть шкідливої інформації. Оптимізація системи розстановки інформаційних бар'єрів в подальшому може розглядатися як один із засобів для вирішення проблем організації інформаційної безпеки особистості. Водночас інформаційні бар'єри регулюють інтенсивність інформаційного потоку, його насиченість. З іншого боку, бар'єри виконують обмежувальну (негативну) функцію, позбавляючи в деяких випадках індивіда доступу до інформації.

З вищенаведеного можна зробити висновок про те, що визначаючою структурою в ієрархії інформаційного суспільства, під впливом якої відбувається формування особистості, є інформаційний простір. Саме останній є зв'язуючою ланкою між суспільством та кожною окремо взятою особистістю.

Саме інформація, а точніше знання, отримані з неї, орієнтують особистість у соціальній дійсності, впливають на формування її системи цінностей, визначають поведінку в суспільстві, виступають основою побудови власної внутрішньої моделі навколишнього світу. Безпосереднє доведення такої інформації до кожної, окремо взятої особистості здійснює суспільна система, яку умовно можна уявити у вигляді трьох елементів:

– культура;
– освіта;
– засоби масової інформації.

Не можна не погодитися з О.О. Хмельницьким, що визначальною в цій тріаді є культура. Адже саме вона містить духовні основи розвитку людини, визначає морально-етичні риси майбутньої особистості. При цьому спостерігається міцний зв'язок між культурою та інформаційним простором. Останній є своєрідним інформаційним прототипом культури. Він містить усі знання, які входять до складу цієї культури. Кожне суспільство формує найбільш прийнятний для нього симбіоз культурних, релігійних, ціннісних, ідеологічних, світоглядних та інших настанов. Культура може впливати на особистість як безпосередньо (шляхом встановлення правил, схем, моделей поведінки), так і опосередковано (через систему освіти, ЗМІ).

Освіта є гносеологічним продовженням культури. Освіта реалізує культуру в практиці й водночас підпорядковується цій культурі. Транслюючи культуру особистості, освіта відіграє провідну роль в її духовному й інтелектуальному становленні. Система освіти закладає життєві й ціннісні орієнтири, формує багаж знань, виводить індивіда на той чи інший рівень культури (як загальної, так і спеціальної). З іншого боку, система освіти за своєю природою є адаптивною відображаючою системою, яка, по суті, лише виконує суспільне замовлення на виховання й професійну підготовку особистості. Тип суспільства повністю детермінує тип системи освіти, тобто апріорно визначає ті чи інші масиви інформації (інформаційні ресурси), що мають закладатися до свідомості індивіда. У цьому випадку роль освіти зводиться до ретрансляції суспільних установок в особистісні.

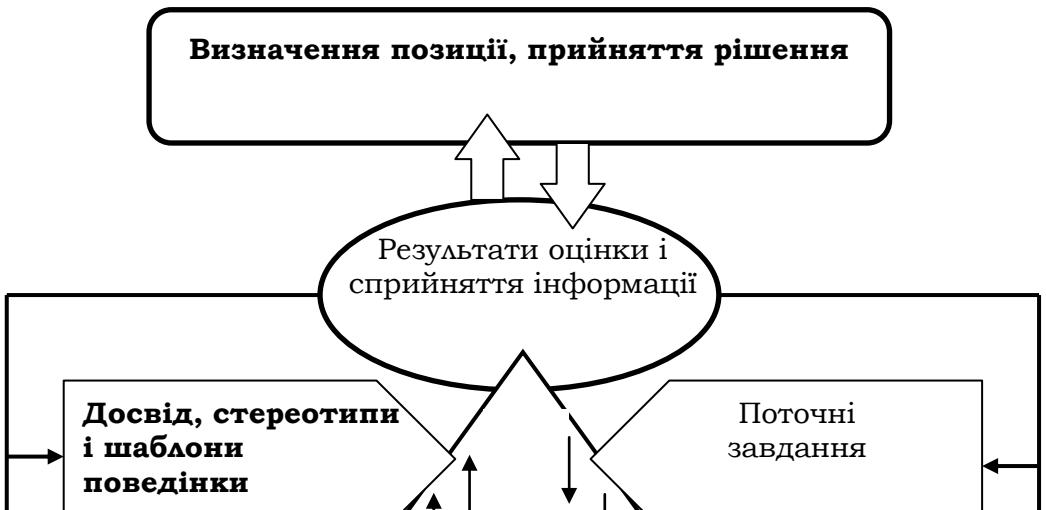
Зв'язок культури зі ЗМІ значно слабший, ніж її зв'язок з освітою. ЗМІ є виразником масової культури, яка носить тимчасовий характер. Однак це не заважає ЗМІ здійснювати значний інформаційний вплив на особистість. Те, що ЗМІ відіграють досить важливу роль у процесах формування особистості, пояснюється, насамперед, двома факторами – динамічністю і неперервністю впливу на особистість. Перше означає, що ЗМІ, як правило, повністю відображають динаміку життя суспільства в цілому і його окремих індивідів. Друге свідчить про сталість процесу, що розглядається. ЗМІ забезпечують передачу індивіду інформації з інформаційного простору, тоді як система освіти орієнтована на передачу особистості знань з наявних інформаційних ресурсів.

5.2.3. Морально-семантичний фільтр: складові та механізми сприймання інформації з оточуючого середовища

Для розуміння глибинної сутності механізмів дії інформаційно-психологічного впливу на особистість необхідно зрозуміти механізми

сприймання інформації індивідом (особистістю). В попередньому підрозділі ми розглянули бар'єри (обмеження) на сприйняття інформації з інформаційного простору. В цьому підрозділі розглянемо, як фільтрується інформація в свідомості людини. Введемо поняття *морально-семантичного фільтра* (далі – фільтра, див. рис. 5.1). Сутність механізму інформаційно-психологічного впливу полягає в наступному. Основним фактором, що визначає орієнтири в поведінці людини, її ставлення до поточної ситуації, мотиви прийняття того чи іншого рішення є її система цінностей й інтересів, які формуються протягом усього її життя, починаючи з дитинства. І тут основну роль відіграє те інформаційне середовище, в яке людина занурена. Під впливом змісту інформаційних потоків, які вона сприймає, акцентів на окремих його фрагментах, інших факторів у людини формується її образ мислення, її світогляд, система цінностей і інтересів, які з часом збагачуючись і розвиваючись в той чи інший бік, приймають участь під час аналізу поточної інформації уже у вигляді своєрідного *морально-семантичного фільтра*.

Особливе місце в реалізації інформаційного впливу на соціальні об'єкти сьогодні посідає ЕОМ, яка є невід'ємною складовою соціотехнічних систем. Прикладами таких систем є інформаційні й комунікаційні системи та мережі, в тому числі Internet, автоматизовані системи управління різного призначення тощо. У соціотехнічних системах соціальна і технічна частини складають одне ціле при аналізі ситуацій і прийнятті рішень. Адже в ЕОМ здійснюються такі етапи інформаційних процесів, як прийом інформації від людини або технічних засобів, її обробка, зберігання, формування нової інформації й видача її людині або іншим технічним засобам. І в цьому плані програмно-математичне і інформаційне забезпечення ЕОМ можна розглядати двоїсто: як аналог (модель) морально-семантичного фільтра людини, якісність і розвиненість якого залежить від рівня моделювання складових фільтру людини, з одного боку, і як додаткову складову фільтру людини, яка приймає безпосередню участь при аналізі інформації і прийнятті рішень, з іншого боку. Звідси випливає, що, контролюючи зміст і обсяг інформаційних потоків, що циркулюють в комп'ютерних мережах, незалежно від того, складовими яких соціотехнічних систем вони є, можна досягати такого ж ефекту в нав'язуванні соціальним об'єктам "бажаних" рішень і поведінки, що й при безпосередньому



впливові на них, а в ряді випадків комп'ютерні мережі виступають в ролі посилювачів цих впливів.

Власне, від орієнтації і сталості фільтра суттєво залежать вчинки, поведінка людини в тій чи іншій ситуації. На змістовні і якісні характеристики фільтру впливають система освіти, релігійні та філософські течії, ідеологічна пропаганда, інші складові інформаційного середовища, без оволодіння якими неможлива

свідома адекватна оцінка людиною явищ суспільно-політичного життя, усвідомлене формування своєї позиції, всебічно осмислений вибір шляху свого розвитку, духовного удосконалення тощо. І тут дуже важливими є якість і рівень інформування особистості, яке, в даному випадку, розуміємо в широкому смислі і включає всі аспекти інформаційного забезпечення особистості, суспільства, країни.

Розглянуті механізми лежать в основі *інформаційного управління як окремою особистістю, так і їх колективами*, в якості яких можуть бути суспільні групування, керівні структури, країни в цілому.

Адже глибинним фундаментом інформаційного впливу на особистість є моральні, етичні й загальнолюдські цінності, які визначаються діючою ідеологічною системою і формуються через систему освіти. Саме ідеологічні настанови можуть виступати як своєрідний бар'єр для здійснення того чи іншого інформаційного впливу або як сприяючий фактор. Тобто, ідеологія, за суттю, формує «інформаційний імунітет» особистості, детермінує його тип. Ідеологія з чітко визначеними пріоритетами сприяє інформаційній стійкості особистості, закріпленню її інформаційного імунітету. І, навпаки, ідеологія зі слабко вираженими пріоритетами сприяє появі інформаційних загроз, руйнує інформаційну стійкість. У часи колишнього СРСР існувала чітко сформована система цінностей, яка реалізовувалася тодішньою ідеологічною системою. Іншими словами, однозначно було вказано, що є «добре» і що «погано», до чого слід прагнути, а чого остерігатися. При цьому, звичайно, мова не йде про якість системи цінностей, її гуманістичну спрямованість. Єдиною позитивною якістю такої ціннісної системи є її схильність до стійкої концепції формування особистості.

Зараз відбувається активне насадження прозахідних цінностей, а значить, формування ідеології, що суперечить національному менталітету, тобто спрямованої на підрив інформаційної стійкості і, відповідно, інформаційної безпеки людини. Тому недаремно точаться гарячі дискусії щодо того, якою має бути сучасна ідеологічна концепція.

Безумовно, формування нової системи цінностей і вироблення ідеологічної системи, спрямованої на її підтримку, є складним завданням, яке вимагає ґрунтовного доробку. Разом з тим, відсутність такої системи шкодить як інформаційній безпеці окремих громадян, так і безпеці держави в цілому. Зазначена ситуація ускладнюється тим, що сама держава відвернулася від інформаційного й ідеологічного захисту своїх громадян. Це ще раз підтверджує необхідність спрямування інформаційної культури на формування інформаційного імунітету особистості, забезпечення її інформаційної стійкості.

5.3. Рефлексивне управління як технологія маніпуляції поведінкою особистості

Модель рефлексивного управління реалізує двосторонній зв'язок. У науковому плані формалізацією принципів рефлексивного управління в інтересах автоматизації управління особистістю займаються: російські фахівці – Лєфевр, українські – Таран [16]. Сутність підходу полягає в тому, що управління особистістю можливо, якщо пропозиції зовнішнього середовища перевищують очікування особистості.

Процес аналізу поточної інформації здебільшого побудований таким чином, що достовірність сформованого на основі її інформаційного представлення про поточну ситуацію пропорційна рівню "добротності" наявної інформації. При цьому під добротністю інформації розуміються її цілісність, повнота, правдоподібність, достовірність та інші характеристики, які визначають рівень довіри до неї. У свою чергу добротність інформації знаходиться в прямій залежності від обсягів і сталості ознак, що підтверджують ту чи іншу ситуацію. Рішення щодо оцінки ситуації, як правило, приймається на основі інформації, що характеризується максимальною добротністю. Цією обставиною протидіюча сторона може легко скористатися, навмисно створюючи своїми джерелами потік "добротної" інформації з метою формування стороною C_1 хибного інформаційного представлення.

Одним з напрямків підвищення якості оцінки поточної ситуації є реалізація підходу, базованого на багатократному відображенні у сторони, що приймає рішення, уявлень про можливості й цільові настанови протидіючої сторони (див. рис. 5.2). Цей підхід лежить в основі рефлексивного управління.

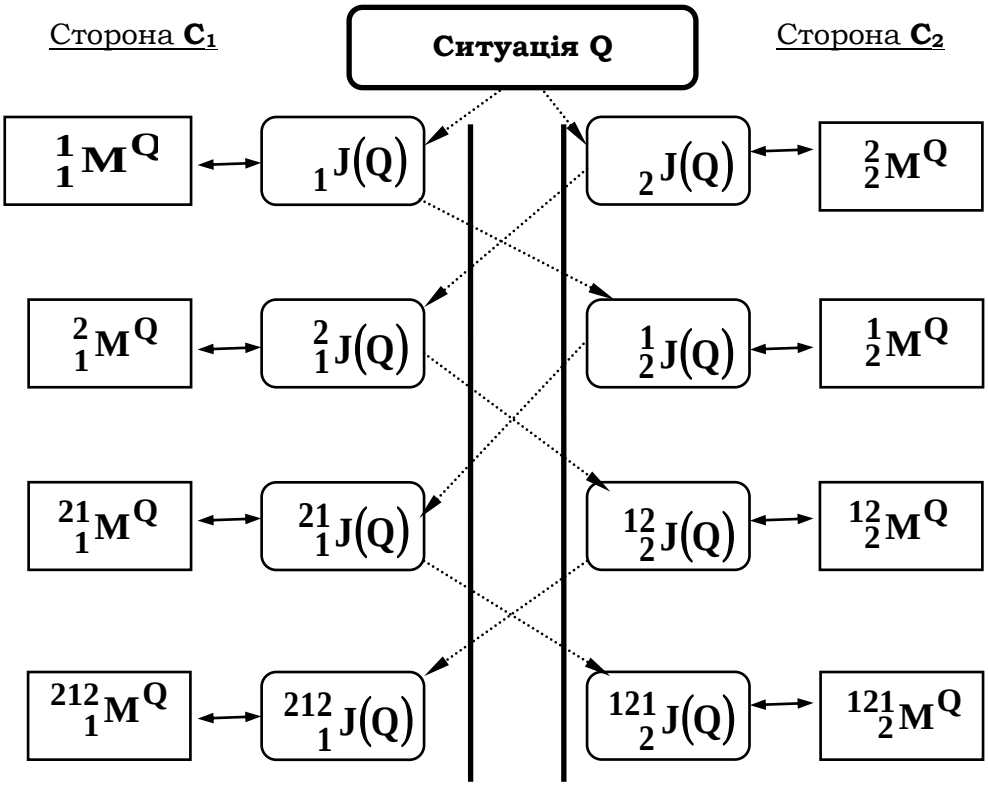


Рис. 5.2. Схема багатократного відображення інформаційного представлення про поточну ситуацію **Q**.

Основний принцип рефлексивного управління - захоплення й утримання інформаційної переваги над протиборчою (конкуруючою) стороною. Для досягнення успіху в операції (бою) необхідно тримати під контролем весь процес боротьби, охоплюючи управлінням не тільки свої війська, але й якимсь чином противника. Те управління, що в першу чергу спрямовано на психіку командира протидійної сторони, який приймає рішення, і носить відбивний характер, називають рефлексивним. Основне його завдання - поставити противника у важкі умови продовження боротьби або примусити його до прийняття рішень, які об'єктивно ведуть до поразки.

Управління противником полягає в проведенні комплексу взаємозалежних за метою, місцем і часом заходів, спрямованих на те, щоб, з одного боку, змусити його відмовитися від початкового задуму (плану), прийняти явно невигідні рішення, а з іншого боку,

парирувати аналогічні дії противника або використовувати їх на шкоду йому (контруправління).

Рефлексивне управління має характер невизначеності суб'єктивного походження: противник може розкрити ціль і задум проведеного заходу, прореагувати на нього, виходячи з власної оцінки обстановки й цінності результатів впливу, продемонструвавши при цьому перебільшену або, навпаки, зменшену його силу, проігнорувати вплив, спробувати використовувати його у своїх інтересах, провести відповідні кроки щодо контруправління. Звідси ясно, яке велике значення має в рефлексивному управлінні противником накреслення задуму його дій.

Примусити противника до прийняття рішень, бажаних для "управляючої" сторони, можна шляхом "страханням збитком" (дійсним або уявним) і "звабою вигодою" (дійсною або уявною). У цьому плані дезінформація, маскування й омана самі по собі носять характер тільки окремих прийомів. "Примушення" тим ефективніше, чим воно більш комбіноване, тобто на основі всієї одержуваної інформації противник повинен зробити висновок про дійсність шкоди або вигоди.

Дуже важливо зробити так, щоб у противника виник дефіцит часу для прийняття рішень і їх реалізації. Раптовість робить сильний психологічний вплив, вона не тільки впливає на вибраний алгоритм прийняття рішень, знижує ефективність системи управління, але й спонукає до передчасних, недостатньо підготовлених дій, вносить дисбаланс у плани противника.

В основі управління противником лежить "передача" йому інформації, яка стимулювала б прийняття ним рішень, об'єктивно вигідних (бажаних) "управляючій" стороні. При цьому можуть бути використані: силовий тиск; формування інформації про обстановку для прийняття рішення; формування інформації для продукування противником нової цілі дій, досягнення якої потребує додаткової підготовки, засобів і часу; передача інформації з метою впливу на відпрацьовані противником алгоритми вирішення завдань управління; вплив на момент прийняття ним рішення.

Прийомами силового тиску можуть бути: застосування переважаючих сил, демонстрація сили (силовий шантаж), "психічна атака", показ дійсного угруповання, об'єктів або озброєння, ультиматум, погроза застосування сили (санкцій), погроза ризиком (акцентування уваги на нерозумному поводженні, на делегуванні повноважень безвідповідальній особі), розвідка боєм, провокаційні маневри й випробування озброєння, недопущення противника у визначений район або його ізоляцію, переведення військ у більш високі ступені боєготовності, утворення військових союзів, офіційне

оголошення війни, підтримка внутрішніх сил, що дестабілізують обстановку в тилу противника, обмежений удар для виведення з ладу частини його сил, звеличення перемог, підвищена жорсткість у діях, прояв милосердя до союзників противника, які припинили боротьбу й ін.

До прийомів формування інформації про обстановку належать: маскування об'єктів і угруповань (показ слабості в сильному місці), створення несправжніх об'єктів і угруповань (показ сили в слабкому місці), позиційна жертва (залишення однієї позиції для посилення оборони на іншій, втягнення під підготовлений удар - "вогневий мішок"), показ одного об'єкта під видом іншого ("перевдягання", "перевтілення"), "дарунок данайців" (залишення на позиції небезпечних об'єктів), демонстрація неіснуючих відношень між об'єктами або утаєння істинних, зберігання в таємниці появи нової зброї або "блеф озброєння" (демонстрація макетів неіснуючої бойової техніки, повідомлення про неї в пресі), зміна режиму діяльності, навмисна утрата важливих документів або передача інформації відомим для противника кодом і тощо.

Змусити противника до формування нової цілі дій можна рядом заходів. Це ескалація або деескалація конфлікту (ступінчасте регулювання його напруженості); навмисний показ тієї або іншої цілі своїх дій, їхня раптовість; удар по базі противника, коли він знаходиться поза нею; проведення диверсій і провокацій; залишення шляху для виходу з оточення; проведення заходів, які змушують противника здійснювати відповідні дії, зв’язані зі значною витратою сил, засобів і часу.

На алгоритм прийняття противником рішення можна вплинути, наприклад, систематичним проведенням навчань за стандартними в його сприйнятті планам, опублікуванням навмисно перекрученої доктрини, ударами по елементах системи управління, включаючи "полювання" за ключовими фігурами, передачею хибної передісторії, роботою в допоміжному режимі, діями щодо нейтралізації оперативного мислення противника (вироблення таких планів дій, мета і задум яких не можуть бути розкриті, принаймні до заключного етапу операції, створення обстановки, коли можна припускати в діях "управляючої" сторони велике число приблизно рівно можливих варіантів, причому кожний із них дошкульний щодо очікуваного збитку й потребує певних зусиль для протидії).

Змусити противника змінити момент прийняття рішення можна в такий спосіб: зненацька почати бойові дії, передати йому інформацію про передісторію аналогічного конфлікту з тим, щоб він, сформувавши правдоподібний із його точки зору прогноз розвитку

обстановки, прийняв поспішне рішення, різко змінив прогноз і характер своєї діяльності.

Дії щодо управління противником спрямовані на конкретну особистість або групу осіб із визначеною психологією, образом мислення, фаховою підготовкою. При цьому можуть бути застосовані два підходи: універсальний і рольовий.

При універсальному підході вплив на свідомість противника здійснюється через ряд загальнолюдських психологічних мотивів відповідно до ієрархії їхньої сили. Мотивами можуть виступати: запобігання небезпеки, небажання "влазити в бійку" або "виконувати чорну роботу за іншого", орієнтація на протиборство щоб там не було ("нехай мені буде погано, але й тобі це задарма не пройде", "після нас хоч потоп") й ін. При рольовому підході аналізуються не можливі мотиви дії, а роль, яку відіграє та чи інша особа або група осіб (претензії на виняткову роль в історії, лідерство або, навпаки, положення підпорядкованого члена коаліції і т.д.).

Розходження підходів впливає на вибір засобів і способів впливу, а також на стиль і порядок передачі інформації. Серед заходів можуть бути й такі, що викликають ланцюгову реакцію поширення (хибні чутки, панічні заклики). Звідси завжди важливий аналіз не тільки істинності й надійності джерела відомостей, але й можливих мотивів їх видачі, особливо при використанні незвичайних каналів (непрямих або нейтральних) та форм передачі інформації.

В управлінні противником дуже важливо дотримати суворої відповідності між цілями, місцем та часом проведення заходів і способами їх здійснення, оскільки невдале здійснення одного з них може дезавуювати весь комплекс у цілому. Оскільки в цьому випадку "нереальне" повинно бути в усьому "реальним", тим більше важлива чітка узгодженість проведених заходів, нешаблонний, ненав'язливий їхній характер. Будь-яка дрібниця тут може перекреслити всі зусилля.

Закономірності рефлексивного управління противником випливають з основних законів управління, психології, людського мислення та розвитку суспільства. Серед них доцільно виділити ряд положень.

По-перше, зміст застосовуваних прийомів і їхніх комбінацій визначається закономірностями й внутрішніми зв'язками процесу мислення та психології, форма їх здійснення залежить від арсеналу технічних засобів, використовуваних у конфлікті.

По-друге, чим сильніше "управляюча" сторона прагне переконати противника в реальності своїх цілей і намірів, тим більше реальними повинні бути залучувані засоби, тим більше сил, засобів і часу буде потрібно на здійснення відповідних заходів.

По-третє, потужні технічні системи щодо досягнення критичного порога своєї сили перестають бути засобом, який можна використовувати для управління противником.

По-четверте, науково-технічна революція у військовій справі породжує нові засоби та прийоми ослаблення противника, наприклад, примусом його до значних витрат засобів і часу при проведенні аналізу, контролю й ефективного парирування заходів "управляючої" сторони.

По-п'яте, при виборі варіантів управління противником потрібно враховувати, що внаслідок розходження цілей, політичного й етичного підходів до вибору засобів і шляхів їх досягнення, внутрішня оцінка сторонами можливих результатів дій здійснюється за різними комплексними критеріями, які відбивають відносний характер їхнього протиборства.

По-шосте, коаліційний противник, оскільки інтереси і внутрішні оцінки окремих держав-учасників збігаються не цілком, являє собою складну систему, усталеність якої змінюється в залежності від характеру обстановки, стану учасників і їхніх відношень (змінюються внутрішні системи оцінок в окремих країнах).

Отже, управління противником являє собою високе мистецтво, яке спирається на наукові знання про процеси людського мислення та психології, знання військової історії, передісторії самого конфлікту й можливостей бойових засобів, і є одним із основних завдань інформаційної боротьби. Найбільш ефективним заходом з реалізації рефлексивного управління протидіючою стороною є формування грамотно продуманої і всебічно виваженої дезінформації.

5.4. Правові основи забезпечення захисту прав і свобод людини в інформаційній сфері

Забезпечення захисту прав і свобод людини в інформаційній сфері є однією з найважливіших цілей інформаційної безпеки, адже права і свободи людини у сфері інформації є ключовими інститутами громадянського суспільства, правової, демократичної держави, надбанням і цінністю європейської спільноти.

Дана думка підтверджується доповіддю Уповноваженого Верховної Ради України з прав людини Н. Карпачової [17], яка зазначила, що світова практика демократичного державотворення переконує в тому, що право на свободу думки і слова, на вільне виявлення своїх поглядів і переконань є одним з наріжних каменів розбудови демократичної, правової держави і громадянського суспільства.

На думку Арістової І.В. [18], у літературі висловлюються погляди, в яких право громадян на інформацію – лише складова частина свободи слова та преси, або, навпаки, свобода інформації – умовне позначення цілої групи свобод і прав: свободи слова або свободи вираження думок; свободи преси та інших ЗМІ; права на одержання інформації, що має суспільне значення; свободи поширення інформації.

5.4.1. Права людини на отримання інформації

Вважається, що право на інформацію не охоплюється цілком свободою слова і преси. Воно значно багатіше, змістовніше і має власну субстанцію, грає свою роль у задоволенні певних інтересів суб'єктів; тому зрізаність даного найважливішого права необґрунтовано. Навряд чи виправданий і такий, надмірно широкий, підхід до змісту права на інформацію. Аргументом на користь таких висловлень є, безумовно, законодавча практика найвищого рівня – конституційна. Йдеться, наприклад, про ст. 34 Конституції України, де закріплені не лише свобода думки, слова, але і право на інформацію. Зовсім не випадково закріплені свобода думки і слова та право на інформацію в різних частинах, хоча й однієї статті. Тим самим підкреслюється як їхній взаємозв'язок і взаємопроникнення, так і відома автономність, самостійність, «суверенність».

Взагалі, вперше поняття *«право на інформацію»* було визначено у ст. 9 Закону України «Про інформацію» від 2 жовтня 1992 року, а саме: «Всі громадяни України, юридичні особи і державні органи мають право на інформацію, що передбачає можливість вільного одержання, використання, поширення та зберігання відомостей, необхідних їм для реалізації ними своїх прав, свобод і законних інтересів, здійснення завдань і функцій».

Досить цікавим є також такі основні положення, що закріплюються відповідними нормами Закону «Про інформацію»:

1. Громадяни мають право доступу до інформації про них, а в період збору інформації мають право знати, які відомості про них і з якою метою збираються, а також оспорювати правильність, повноту, доцільність такої інформації.
2. Право на інформацію охороняється законом.
3. Держава гарантує усім учасникам інформаційних відносин рівні права та можливості доступу до інформації.
4. Інформація не може бути використана з метою, що завдає шкоди правам та свободам громадян України.
5. Не підлягають розголошенню відомості, які становлять де-

ржавну чи іншу передбачену законом таємницю.

6. Реалізація права на інформацію громадянами, юридичними особами і державою не повинна порушувати громадські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи та законні інтереси інших громадян, права та інтереси юридичних осіб.

7. Кожному громадянину забезпечується вільний доступ до інформації, яка стосується його особисто, крім випадків, передбачених законами України.

З прийняттям Конституції України в 1996 році, *право людини на інформацію* – самостійне конституційне право, яке дозволяє людині вільно збирати, зберігати, використовувати і поширювати інформацію будь-яким способом, що гарантується ч. 2 ст. 34 Конституції України [19].

Здійснення цього права може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя (ч. 3 ст. 34 Конституції України).

Комплекс прав та свобод в інформаційній сфері вважається непорушним та невідчужуваним. За основу положень розділу II «Права, свободи та обов'язки людини і громадянина» Конституції України взято ряд міжнародних нормативно-правових актів. Зокрема, Загальна декларація прав людини, Міжнародний пакт про економічні, соціальні і культурні права, Міжнародний пакт про громадянські та політичні права.

У цілому ст. 34 Конституції України відповідає ст. 19 Міжнародного пакту про громадянські і політичні права, який надає кожній людині право вільно шукати, одержувати і поширювати будь-яку інформацію та ідеї, незалежно від державних кордонів, та в будь-який спосіб за своїм вибором.

Структура конституційного права на інформацію, що закріплюється Конституцією України та Цивільним кодексом України, визначається такими складовими як:

– збирання інформації;

– зберігання інформації;

– використання інформації;

– поширення інформації.

Відповідно до Закону України «Про інформацію», структурою вищезазначеного права є:

– одержання;

– зберігання;

– використання;
– поширення.

Поняття «збирання» інформації, яке міститься у тексті Конституції, законодавчо не визначено, оскільки Закон України «Про інформацію» дає дефініції тільки таким поняттям як «одержання», «зберігання», «використання» та «поширення».

Під *одержанням* інформації законодавець розуміє набуття, придбання, накопичення інформації громадянами, юридичними особами або державою відповідно до чинного законодавства України.

Зберігання інформації – означає забезпечення належного стану інформації та її матеріальних носіїв.

Використання інформації – задоволення інформаційних потреб громадян, юридичних осіб і держави.

Поширення інформації – розповсюдження, обнародування, реалізацію інформації у встановленому законом порядку.

Цікавим є той факт, що даний Закон у ст. 38 закріплює також «право власності на інформацію», під яким розуміється «врегульовані законом суспільні відносини щодо володіння, користування і розпорядження інформацією». Отже, законодавець оперує такими поняттями, як «володіння», «користування», «розпорядження», які не визначені законодавчо.

Оскільки ч. 2 ст. 32 Конституції України забороняє збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, то досить цікавим є розгляд цієї проблеми детальніше.

Ст. 23 Закону України «Про інформацію» містить такі основні норми:

1. Основними даними про особу (персональними даними) є національність, освіта, сімейний стан, релігійність, стан здоров'я, а також адреса, дата і місце народження.
2. Джерелами документованої інформації про особу є видані на її ім'я документи, підписані нею документи, а також відомості про особу, зібрані державними органами влади та органами місцевого і регіонального самоврядування в межах своїх повноважень.
3. Забороняється збирання відомостей про особу без її попередньої згоди, за винятком випадків, передбачених законом.

5.4.2. Види інформаційних прав і свобод людини та їх зв'язок з іншими правами та свободами людини

Крім загального визначення права людини на інформацію в ст. 34 Конституції, є ряд інших інформаційних прав і свобод, що закріплюються конституційними нормами.

1. Свобода особистого і сімейного життя (ст. 32: «...не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини»).

2. Таємниця листування, телефонних переговорів, телеграфної й іншої кореспонденції (ст. 31: «...винятки можуть бути встановлені лише судом у випадках, передбачених законом, з метою запобігти злочинові чи з'ясувати істину під час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо»).

3. Право громадянина не зазнавати втручання в його особисте та сімейне життя, шляхом збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, знайомитися в органах державної влади, органах місцевого самоврядування, установах та організаціях із відомостями про себе (ст. 32: це відноситься до відомостей, що «не є державною або іншою захищеною законом таємницею»).

4. Право громадянина направляти індивідуальні або колективні письмові звернення або особисто звертатися в органи державної влади, органи місцевого самоврядування та до посадових і службових осіб цих органів (ст. 40).

5. Право кожного громадянина на сприятливе навколишнє середовище, достовірну інформацію про її стан (ст. 50: «...така інформація ніким не може бути засекречена»).

6. Право кожного на свободу творчості і право доступу до культурних цінностей (ст. 54: результати інтелектуальної, творчої діяльності громадянина «ніхто не може використовувати або поширювати їх без його згоди, за винятками, встановленими законом»).

7. Право кожного громадянина на одержання кваліфікованої правової допомоги (ст. 59: «...у випадках, передбачених законом, ця допомога надається безоплатно»).

Деякі конституційні положення, також мають відношення до інформаційних прав і свобод.

Так, за статтями 21, 24 усі люди є вільні і рівні у своєму *праві на інформацію,* яке є невідчужуваним та непорушним і не залежить від раси, кольору шкіри, релігійних та інших переконань, статі, етнічного та соціального походження тощо.

Без отримання необхідної інформації, вільного її використання людина не змогла б розвивати свою особистість (ст. 23).

Право на інформацію пов'язане з *правом на свободу світогляду і віросповідання,* яке включає свободу сповідувати будь-яку релігію або не сповідувати ніякої, безперешкодно відправляти одноособово чи колективно релігійні культи і ритуальні обряди, вести релігійну діяльність (ст. 35).

Реалізація *права на освіту* (ст. 53) неможлива без вільного інформаційного обміну між людьми. Процес навчання означає, перш за все, пошук і отримання необхідної інформації.

Ст. 34 Конституції можна також розглядати як певний розвиток і конкретизацію положення ч. 3 ст. 15, що забороняє здійснення в Україні цензури, тобто обмежувальних заходів щодо здійснення свободи слова в засобах масової інформації. Вона гарантує духовну і творчу свободу, не обмежену ніякою обов'язковою ідеологією. Положення статті гарантують доступ до засобів масової інформації політичним партіям і рухам, громадським організаціям, профспілкам, кожній окремій людині. Ніхто не може бути примушений до зміни чи висловлювання своїх поглядів і переконань.

Зрозуміло, що Конституція України закріплює основний зміст прав і свобод людини в інформаційній сфері, але їх конкретизація відображається в ряді нормативно-правових актах, а саме таких як: Закон УРСР «Про мови в Українській РСР» від 28.10.1989 р., Закон України «Про науково-технічну інформацію» від 25.06.1993 р., Закон України «Про інформаційні агентства» від 28.02.1995 р., Закон України «Про Концепцію Національної програми інформатизації» від 04.02.1998 р., Закон України «Про захист інформації в автоматизованих системах» від 05.07.1994 р., Указ Президента «Про додаткові заходи щодо безперешкодної діяльності ЗМІ, дальшого утвердження свободи слова в Україні» від 9.12.2000 р., Указ Президента «Про вдосконалення державного управління інформаційною сферою» від 16.09.1998 р., Розпорядження Президента «Про додаткові заходи поліпшення інформаційної діяльності» від 5.10.1998 р. тощо.

Як зазначають дослідники даної проблематики, конституційне закріплення права на інформацію ще не робить зрозумілим механізм його реалізації. Це стосується, наприклад, надання відповідної інформації державними органами і органами місцевого самоврядування за запитами громадян. Крім розробки чіткого та прозорого механізму здійснення права на доступ до різного роду інформації, її отримання, поширення, використання тощо, необхідно також внести зміни до чинного законодавства у зв'язку з дуже бурхливим розвитком сучасних інформаційних технологій та мереж, зокрема Інтернет, зробити ревізію застарілих законодавчих визначень і понять, приділити серйозну увагу узгодженню

національного законодавства з міжнародними нормами і стандартами в інформаційній галузі.

5.4.3. Правове забезпечення реалізації права на інформацію

Доволі дискусійним з точки зору забезпечення інформаційної безпеки України є Указ Президента України «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет і забезпечення широкого доступу до цієї мережі в Україні» від 31 липня 2000 року.

З одного боку, цей Указ закріпив, що з метою розвитку національної складової глобальної інформаційної мережі Інтернет, забезпечення широкого доступу громадян до цієї мережі, ефективного використання її можливостей для розвитку вітчизняної науки, освіти, культури, підприємницької діяльності, зміцнення міжнародних зв'язків, належного інформаційного забезпечення для здійснення органами державної влади та органами місцевого самоврядування своїх повноважень, повнішого задоволення потреб міжнародного співтовариства в об'єктивній, комплексній інформації щодо різних сфер суспільного життя в Україні, а також вирішення інших завдань, визначених в Посланні Президента України до Верховної Ради України «Україна: поступ у XXI сторіччя. Стратегія економічного та соціального розвитку на 2000–2004 роки», необхідно встановити, що розвиток національної складової глобальної інформаційної мережі Інтернет, забезпечення широкого доступу до цієї мережі громадян та юридичних осіб усіх форм власності в Україні, належне представлення в ній національних інформаційних ресурсів є одним з пріоритетних напрямів державної політики в сфері інформатизації, задоволення конституційних прав громадян на інформацію, побудови відкритого демократичного суспільства, розвитку підприємництва.

У зв'язку з чим, основними завданнями розвитку національної складової мережі Інтернет і забезпечення широкого доступу до цієї мережі в Україні визначено:

1) створення у найкоротші строки належних економічних, правових, технічних та інших умов для забезпечення широкого доступу громадян, навчальних закладів, наукових та інших установ і організацій усіх форм власності, органів державної влади та органів місцевого самоврядування, суб'єктів підприємницької діяльності до

мережі Інтернет;

2) розширення і вдосконалення подання у мережі Інтернет об'єктивної політичної, економічної, правової, екологічної, науково-технічної, культурної та іншої інформації про Україну, зокрема тієї, що формується в органах державної влади та органах місцевого самоврядування, навчальних закладах, наукових установах та організаціях, архівах, а також бібліотеках, музеях, інших закладах культури, розширення можливостей для доступу в установленому порядку до інших національних інформаційних ресурсів, постійне вдосконалення способів подання такої інформації;

3) забезпечення конституційних прав людини і громадянина на вільне збирання, зберігання, використання та поширення інформації, свободу думки і слова, вільне вираження своїх поглядів і переконань;

4) забезпечення державної підтримки розвитку інфраструктури, надання інформаційних послуг через мережу Інтернет; створення умов для розвитку підприємницької діяльності та конкуренції у галузі використання каналів електронного зв'язку, створення можливостей для задоволення на пільгових умовах потреб у зазначених послугах навчальних закладів, наукових установ та організацій, громадських організацій, а також бібліотек, музеїв, інших закладів культури, закладів охорони здоров'я, включаючи розташовані у сільській місцевості;

5) розвиток та впровадження сучасних комп'ютерних інформаційних технологій у системі державного управління, фінансовій сфері, підприємницькій діяльності, освіті, наданні медичної та правової допомоги тощо;

6) вирішення завдань щодо гарантування інформаційної безпеки держави, недопущення поширення інформації, розповсюдження якої заборонено відповідно до законодавства;

7) вдосконалення правового регулювання діяльності суб'єктів інформаційних відносин, виробництва, використання, поширення та зберігання електронної інформаційної продукції, захист прав на інтелектуальну власність, посилення відповідальності за порушення встановленого порядку доступу до електронних інформаційних ресурсів усіх форм власності, за навмисне поширення комп'ютерних вірусів;

8) забезпечення вступу України до відповідних міжнародних організацій, що займаються питаннями розвитку телекомунікаційних систем; захист прав на інформацію; протидія поширенню інформації, яка завдає шкоди людині і громадянину, суспільству і державі; внесення в установленому порядку відповідних пропозицій; сприяння залученню коштів міжнародної технічної допомоги, використання можливостей міжнародних програм для розвитку в Україні мережі

Інтернет.

З іншого боку, на основі вже згадуваного Указу Президента створено Департамент спеціальних телекомунікаційних систем та захисту інформації СБУ, який повинен контролювати увесь обіг інформації в органах державної влади, організаціях, на підприємствах, незалежно від форм власності, що використовують мережі передачі даних, зокрема Інтернет, тим самим, порушуючи основні права і свободи людини в інформаційній сфері, закріплені Конституцією. Дещо виправило ситуацію виведення даного департаменту зі складу СБУ у 2006 році.

Слід зазначити, що деякі з існуючих нормативних актів суперечать один одному чи взагалі застаріли, внаслідок чого почасти виникають колізії. Відсутність чітких демократичних правових засад, неточність, а часом відсутність офіційного визначення широковживаних термінів у цій галузі гальмує її розвиток в цілому, що саме по собі є загрозою національним інтересам в інформаційній сфері.

5.5. Безпека життєдіяльності людини в інформаційному просторі

Проблема інформаційної безпеки суспільства й особистості та їх захист від інформації має в своїй основі питання інформаційної стійкості і самоорганізації людини. Підхід, згідно з яким особистість являє собою самоорганізуючу систему, що має в своїй основі єдність стійкості і мінливості, дозволяє більш адекватно осмислювати актуальні проблеми її становлення й розвитку в інформаційному контексті.

5.5.1. Самоорганізація як шлях захисту особистості в інформаційному просторі

Загальноприйняте розуміння розвитку особистості – це стійкі зміни в структурі її життєдіяльності. Діалектика розвитку особистості полягає в тому, що вона завжди зберігає стан і одночасно змінюється в межах цього стану. Особистість може бути цілісною системою, коли вона має такі ознаки як стійкість і мінливість. Порушення цієї єдності в сторону стійкості веде до блокади самоорганізації; зміщення в бік мінливості руйнує цілісність системи.

Самоорганізація полягає в самоускладненні системи. Вона являє собою спрямовані зміни в організації й рівнях ієрархії системи, які

відбуваються відносно інваріантно стосовно самої системи. Самоорганізація визначається як найвища форма збереження живого, яка сприяє самоприскореному розвитку систем, їх прогресу. Зростання стійкості соціальних систем, розвиток їх самоорганізації обумовлюється активною взаємодією з оточуючим світом, змінами, які в ньому відбуваються.

Активність соціальних систем визначає стійкість їх організації, яка виявляється в здатності до збереження свого стану при зовнішніх, у тому числі й інформаційно-психологічних впливах. Зв'язок між стійкістю і розвитком полягає в тому, що стійкі стани є моментами розвитку системи. Стійкість індивідуального розвитку є основою спрямованості змін. Стійкий стан виступає як результат перетворень.

Стійкість є результатом дій і вчинків суб'єкта, в основі яких лежить свобода вибору, активність суб'єкта при прийнятті рішень, критичне ставлення до оточуючого світу.

В начальному посібнику Хмельницького О.О. «Інформаційна культура: підготовка кадрів до інформаційної роботи» дано визначення поняттю соціальна стійкість [15].

Соціальна стійкість – це суспільна характеристика, що визначає внутрішню здатність особистості до дії й проявляється як більш-менш спрямована й усвідомлена діяльність, зміст якої полягає як у перетворенні існуючої дійсності, так і в особистісному формуванні індивіда. Соціальна стійкість відображається когнітивно, реалізується в структурі спонукань, змісті діяльності, формах поведінки.

Соціально-стійка особистість – це самоорганізуюча, саморозвиваюча система відношень з гранично вираженою суспільною спрямованістю, яка являє собою динамічну цілісність сукупності стійких структур.

Основою соціальної стійкості особистості є її інформаційна стійкість. Різноманітна інформація по-різному може впливати на особистість. Вона може виступати як фактор, що стимулює самоорганізацію особистості і сприяє її стійкості, а може здійснювати дезорганізуючий, руйнівний вплив на людину. Інформаційна стійкість – це здатність людини протистояти деструктивному інформаційному впливу на свою свідомість і психіку. Підвищенню інформаційної стійкості повинен сприяти високий рівень інформаційної культури. Інформаційна стійкість є критерієм цілісності особистості. Не існує абсолютно стійких в інформаційному контексті живих систем. Інформаційна стійкість має межу, яка й детермінує цілісність особистості як складної системи. Заходи щодо захисту від інформації повинні спрямовуватися саме на підвищення інформаційної стійкості, її фундаментом має бути природне почуття, інстинкт самозбереження.

Адже, як писав відомий американський розвідник Ален Далес, «прагнення мати завчасну інформацію, без сумніву, породжено інстинктом самозбереження». Саме останній повинен захистити людину від надлишку інформації і деструктивного впливу з її боку. Інформаційна культура (ІК) індивіда повинна надати йому чітке уявлення щодо того, споживання якої інформації є бажаним, а якої – ні. У цьому контексті однією з основних функцій ІК є формування інформаційно-стійкої особистості шляхом усвідомлення нею існуючих загроз від інформації. Суб'єкт, який усвідомлює загрози і володіє необхідними засобами для протидії їм, знаходиться на найвищому ступені інформаційної безпеки. І навпаки, суб'єкт, який не усвідомлює існування інформаційних загроз, насамперед підпадає під їх дію. Підвищенню інформаційної стійкості особистості повинна сприяти і така складова інформаційної безпеки, як інформованість. Остання припускає можливість отримання всієї необхідної інформації, а також можливість її переробки в заданий проміжок часу, а також класифікацію й осмислення з метою напрацювання стратегічних та тактичних мотивацій і визначення конкретних проявів реалізації стратегії, що використовується.

Безпосередньо інформаційний вплив здійснюється шляхом обґрунтування, переконання, навіювання, спрямованого на аудиторію чи окрему особистість. Обґрунтованість являє собою осмислення логічних основ, які дають особистості впевненість у правильності свого розуміння. Тобто обґрунтованість – це спроба знайти «точки дотику» інформації і ціннісних настанов й орієнтацій особистості, на яку вона спрямована.

Впевненість може розглядатися як потік інформації, що знижує ступінь психічного опору особистості, яка піддається інформаційному впливу. Впевненість породжує переконання. Останнє формує певні настанови й через них – думки, погляди, відносини, які не завжди співпадають, а досить часто й суперечать особистісним настановам, які діяли раніше. Через переконання людина приходить до переконаності, яка розглядається як непорушна впевненість в істинності певних ідей і уявлень, в реальності засвоєних понять, образів і їх зв'язків з дійсністю. Впевненість дозволяє виробляти чіткі однозначні рішення.

Для усунення й нейтралізації різноманітних інформаційних загроз необхідно зосередити зусилля на активізації особистісних якостей, до яких, окрім вищезгаданих, слід додати ще одне – системність. Системне сприйняття інформації має велике значення для формування в особистості цілісної картини світу. Системний підхід дозволяє найбільш адекватним чином інтерпретувати та класифікувати всю інформацію, яка надходить до людини. При

цьому виявляються явні й приховані фактори, причинно-наслідкові зв'язки, внутрішня логіка подій. Системний аналіз сукупності окремих елементів дозволяє виявити ті з них, що мають патогенну спрямованість і становлять загрозу особистості.

Крім того, слід запропонувати ряд більш глобальних організаційних і педагогічних заходів. Перш за все необхідна розробка та реалізація цілісної концепції ідеологічної й пропагандистської дії, орієнтованої на встановлення пріоритету національних і культурних цінностей і світоглядних орієнтирів в противагу тим, що розповсюджуються з-за кордону. При цьому вказана концепція повинна стати основою для створення цивілізованого інформаційного простору країни, надання йому таких властивостей, як цілеспрямованість, системність, стійкість, безпечність. Однак тут повинен використовуватися не абстрактний підхід, як це було раніше, коли потужна ідеологічна система працювала сама на себе й при цьому повністю ігнорувала життєві інтереси та потреби особистості, а підхід, орієнтований на конкретних людей – громадян країни, на захист їх духовного здоров'я, попередження інформаційних загроз, збереження цілісної особистості як стійкої системи, що розвивається. Через загальнодержавні ідеологічні, педагогічні, організаційні та інші заходи слід сформувати в особистості захисний інформаційний прошарок, генетичну основу якого складатимуть загальнолюдські цінності й орієнтири. Саме він повинен захистити особистість від згубної інформаційної дії, а також від вищеперерахованих інформаційних загроз.

При цьому основи інформаційної безпеки особистості мають закладатися на початкових стадіях її формування. Процес виховання повинен ґрунтуватися на традиціях і принципах, що не суперечать діючим нормам і правилам суспільної поведінки, культурним ідеалам. Людина повинна розуміти та приймати норми й традиції свого народу і своєї країни. Прилучаючись до досягнень світової культури, вона повинна віддавати пріоритет вітчизняним зразкам, які також входять до складу світової культури. До того ж важливим елементом в системі виховання є патріотизм, який сприяє формуванню стійкої в соціальному, психологічному й інформаційному аспекті особистості, а також визначає особливості інформаційного сприйняття.

Успішна реалізація заходів інформаційної безпеки особистості можлива лише за умови принципово нових підходів до системи освіти, а також методів передачі й формування масивів знань. Осмислюючи новітні наукові досягнення в області синергетики, геоглобалістики, ноосферології, теорії фізичного вакууму, а також нові підходи до вирішення комунікативних, соціальних і екологічних проблем, учені приходять до висновку про необхідність переходу до

нової стратегії розвитку сучасної системи освіти, в основу якої покладена ідея випереджаючої освіти. Діюча система освіти реалізує концепцію так званої підтримуючої освіти, суть якої полягає в тому, що підготовка спеціалістів здійснюється на основі вимог сьогодення без урахування того, що очікує цих фахівців у майбутньому.

Концепція системи випереджаючої освіти полягає в її принциповій орієнтації на майбутнє. Вона повинна створюватися на основі синтезу новітніх знань різних наук. Однією з пріоритетних цілей такої системи повинно бути формування в людей таких якостей, які дозволять їм успішно адаптуватися в умовах інформаційного суспільства. При формуванні концепції випереджаючої освіти є виключно важливим зрозуміти, якими саме якостями повинні володіти люди, для того щоб швидко адаптуватися в мінливому світі, використовувати його нові можливості й захищати себе від нових інформаційних загроз. До таких якостей в першу чергу належать:

– *ноосферна свідомість;*
– *системне мислення;*
– *інформаційна культура;*
– *економічна культура;*
– *творча активність;*
– *толерантність;*
– *висока моральність.*

В основу концепції випереджаючої освіти покладені ідеї А.Д. Урсула, її основні принципи були сформульовані і розвинені К.К. Коліним [20]:

– формування у людей нового, глобального типу свідомості, який, згідно з ідеями А.Д. Урсула, можна назвати ноосферною свідомістю;

– формування науково обґрунтованих уявлень про основні закономірності розвитку природи та суспільства, а також про особливу роль інформації й інформаційних процесів. Тут слід підкреслити необхідність розвитку та впровадження в систему освіти нових принципів передачі знань й інформації;

– вивчення закономірностей становлення нового постіндустріального інформаційного суспільства, а також тих проблем і загроз, з якими людині доведеться зустрічатися;

– формування в людей науково обґрунтованих уявлень про тенденції й перспективи подальшого технічного розвитку цивілізації. Оволодіння методологією та практичними навичками системного аналізу інформаційних аспектів найважливіших соціальних, економічних і науково-технічних проблем, вивчення методів їх розв'язання на основі активізації інформаційних ресурсів;

– формування в суспільстві нового перспективного виду культури – інформаційної культури. Ця культура повинна дати людині в

інформаційному суспільстві не лише інформаційну свободу, тобто вільний доступ до всієї необхідної інформації, а і забезпечити безпрецедентні можливості для розвитку людини як особистості, для практичної реалізації нею своїх громадських прав і свобод;

– формування в людей нової якості особистісної інформаційної культури, яка повинна бути заснована не лише на знанні закономірностей інформаційних процесів в суспільстві, а також і на розумінні своєї відповідальності за забезпечення інформаційної безпеки всіх членів суспільства.

У межах концепції випереджаючої освіти необхідна розробка нових форм і методів роботи з інформацією, які б дозволили людині вільно орієнтуватися у великих масивах інформації, здійснювати їх моніторинг, підвищити ефективність пошуку потрібних відомостей. Такі форми та методи дозволять запобігти інформаційному перенасиченню й інформаційному тромбозу, підвищити якість інформаційної роботи. Для підвищення інтелектуальних і психофізичних здібностей людини щодо сприйняття інформації можна порекомендувати використання методів швидкісного читання.

Для попередження маніпулятивного впливу на особистість з боку іноземної інформаційної присутності в ЗМІ, суспільних і релігійних об'єднаннях слід звернути особливу увагу на підвищення інформаційної стійкості до патогенних текстів, які передаються різними каналами. При цьому культура, ідеологія й освіта повинні виступати єдиним комплексом, який має своєю метою стійкий розвиток людини.

5.5.2. Безпека ділового спілкування

Для того щоб не попадатися на маніпулятивні гачки, перш за все їх треба вміти розпізнавати. У випадку ідентифікації маніпулятивних прийомів, які використовує опонент, подальші дії можуть вибудовуватися в залежності від характеру, завдань й умов конкретного спілкування.

Розглянемо деякі загальні положення, які певним чином дозволяють виявити та знизити ефект дії маніпулятивних прийомів.

На першому етапі перед дискусією необхідно з’ясувати й чітко визначити для себе та своїх партнерів яких цілей ви хочете досягти. Це буде тим системотвірним фактором, який має визначити весь хід та спрямованість вашої участі в дискусії. Необхідно визначити і зафіксувати які цілі декларують ваші опоненти та намагатися спрогнозувати, наскільки вони розходяться з істинними намірами.

На протязі всієї дискусії необхідно постійно утримувати в “полі уваги” цілі, загальний план і хід дискусії.

Аргументацію, що використовується в ході дискусії можна поділити на так звану аргументацію доведення та контраргументацію. Для їх аналізу з метою виявлення слабких сторін, які можуть бути використані для посилення позицій опонентами, можна використати наступні правила аналізу [21].

Для аналізу доказової аргументації:

1. Чи є точними дані, що використовуються нами?
2. Чи є вірними висновки?
3. Які є протиріччя в аргументації?
4. Чи можна навести зрозумілі порівняння (аналогії)?
5. Які доводи можуть виникнути у опонентів на нашу аргументацію?
6. Чи носять розбіжності принциповий характер?
7. Чи можна досягти успіху поступками щодо непринципових розбіжностей?

Для аналізу контраргументації:

1. Чи є протиріччя в опонентів?
2. Чи можна спростувати факти та положення опонентів?
3. Чи є невдалі приклади або порівняння?
4. Чи є в опонентів помилкові або невдалі висновки?
5. Чи не занадто опоненти спростили проблему та чи можна показавши її інші сторони посилити доказовість власного тезису?
6. Чи є в опонентів хибні оцінки?
7. Якщо неможливо спростувати контраргументацію в цілому, чи можливо поставити питання до окремих складових?
8. Чи можна показати протиріччя в контраргументації опонентів шляхом уточнень і питань?
9. Чи не використовують опоненти спекулятивні (недозволені) прийоми та яким чином це можна використати для посилення власної аргументації?

У випадках, коли опонент використовує недозволені прийоми, це можна відкрито обговорити з ним, як про недопустиму тактику ведення диспутів. У випадках “злісного” використання опонентом маніпуляцій можливо відповісти своїми хитрощами, які б паралізували хитрощі опонента. Це небажаний прийом, який можна виправдати, коли всі інші способи себе вичерпали.

Використання, так званого “зворотного удару” засновується на виявленні у тезах опонента доводів, які можуть бути спрямовані проти його ж доведення. Таким чином показується логічна неспроможність опонента.

Виявлення пастки може будуватися на відповіді, в якій показується неправильність подібних міркувань на якомусь яскравому прикладі.

Спосіб звинувачення полягає у тому, що показується характер пастки й звертається увага на її навмисний характер. Така поведінка буває доцільною для того, щоб осадити грубого опонента. Цим краще не зловживати.

"*Метод Сократа*" полягає у постановці серії питань, на які просять дати однозначні відповіді. Питання ставляться таким чином, щоб опонент, відповідаючи на них, сам спростував свої тези. Однак треба пам'ятати, що цей метод сам перетворюється на пастку, якщо на питання не можна дати однозначну відповідь.

Пастки, що базуються на викривленні смислу, нейтралізуються за допомогою уточнень висловлювань, повторень аргументів тощо.

Важливо не піддаватися на провокації, які містять особисту образу. Їх можна перевести в атаку на проблему, що обговорюється, звертаючи увагу на те, що саме цим мають займатися учасники обговорення.

Не слід намагатися "*загнати опонента у кут*", особливо під час публічних обговорень, бо його захисна реакція може звести до нуля досягнуті результати.

Одна із головних вимог – дотримання *принципів і правил аргументації.* Якщо обидві сторони їх притримуються, то ніякі інші допоміжні прийоми не потрібні. Веденню дискусій конструктивного характеру сприяє також *вироблення концепції обговорення.*

Висновки

Виокремлення інформаційно-психологічної безпеки особистості із загальної проблематики інформаційної безпеки як самостійного напрямку визначається наступними основними причинами:

– перехід до інформаційного суспільства, збільшення масштабів та ускладнення змісту й структури інформаційних потоків значно посилюють їх вплив на психіку людини. Це визначає необхідність формування нових механізмів і засобів виживання людини як особистості і активного соціального суб'єкта в сучасному світі;

– взаємодія психіки людини з інформаційним середовищем відрізняється своєю специфікою та не має адекватних аналогів в інформаційній взаємодії інших біологічних, технічних, соціальних та соціотехничних систем;

– основною "мішенню" інформаційного впливу є людина, його психіка. Саме із окремих особистостей, їх взаємодії залежить

нормальне функціонування соціальних суб'єктів різного рівня складності, будь-яких спільнот і соціальних груп - от малої групи до населення країни в цілому.

Загальним джерелом зовнішніх загроз інформаційно-психологічної безпеки особистості є та частина інформаційного середовища суспільства, яка в силу різних причин не адекватно відображає навколишній світ. Тобто інформація, яка вводить людей в оману, у світ ілюзій, не дозволяє адекватно сприймати світ і самого себе.

Глосарій до розділу

Використання інформації – задоволення інформаційних потреб громадян, юридичних осіб і держави.

Зберігання інформації – означає забезпечення належного стану інформації та її матеріальних носіїв.

Одержання інформації – процес набуття, придбання, накопичення інформації громадянами, юридичними особами або державою відповідно до чинного законодавства України.

Підсвідомість – сукупність активних психічних процесів (інтуїція, паніка, гіпноз, сновидіння, звичні дії тощо), які не є центром смислу діяльності свідомості, але здійснюють вплив на протікання свідомих процесів. Підсвідомість можна розглядати як неусвідомлений рівень психіки, тобто як сукупність психічних процесів, актів і станів, обумовлених оточуючим середовищем, вплив яких суб'єкт не усвідомлює. Підсвідомість відрізняється від свідомості тим, що реальність зливається з переживаннями суб'єкта, тому і неможливий контроль дій, що здійснює суб'єкт, а також оцінка їх результатів. Вплив на підсвідомість являє особливо небезпечну загрозу, оскільки він ніяким чином не проявляється та не реєструється свідомістю. Вплив на підсвідомість дозволяє змінювати мотиви та смисл діяльності людини, програмувати його поведінку на підставі персональних стереотипів, а також активізувати сприймання інформації та творче мислення.

Поширення інформації – розповсюдження, обнародування, реалізацію інформації у встановленому законом порядку.

Психіка – функція головного мозку, яка полягає в активному відображенні людиною об'єктивного світу, побудові картини цього світу й саморегуляції на цій основі своєї поведінки та діяльності. В психіці представлені та упорядковані події минулого, теперішнього та можливо майбутнього часу. Головною формою психіки людини є *свідомість*, але вона не вичерпує підсвідомість. У людини ще є і неусвідомлені психічні процеси (див. підсвідомість).

Соціальна стійкість – це суспільна характеристика, що визначає внутрішню здатність особистості до дії й проявляється як більш-менш спрямована й усвідомлена діяльність, зміст якої полягає як у перетворенні існуючої дійсності, так і в особистісному формуванні індивіда. Соціальна стійкість відображається когнітивно, реалізується в структурі спонукань, змісті діяльності, формах поведінки.

Соціально-стійка особистість – це самоорганізуюча, саморозвиваюча система відношень з гранично вираженою суспільною спрямованістю, яка являє собою динамічну цілісність сукупності стійких структур.

Усвідомлення – це фокусування свідомості на психічних процесах, на тих чуттєвих образах дійсності, які особистість завдяки їм отримує. В основі усвідомлення лежить узагальнення власних психічних процесів, що приводить до оволодіння ними. Іншими словами, усвідомлювати - це осягати розумом, сприймати свідомо, розуміти значення, сенс чогось.

Зв'язок ключових понять і термінів

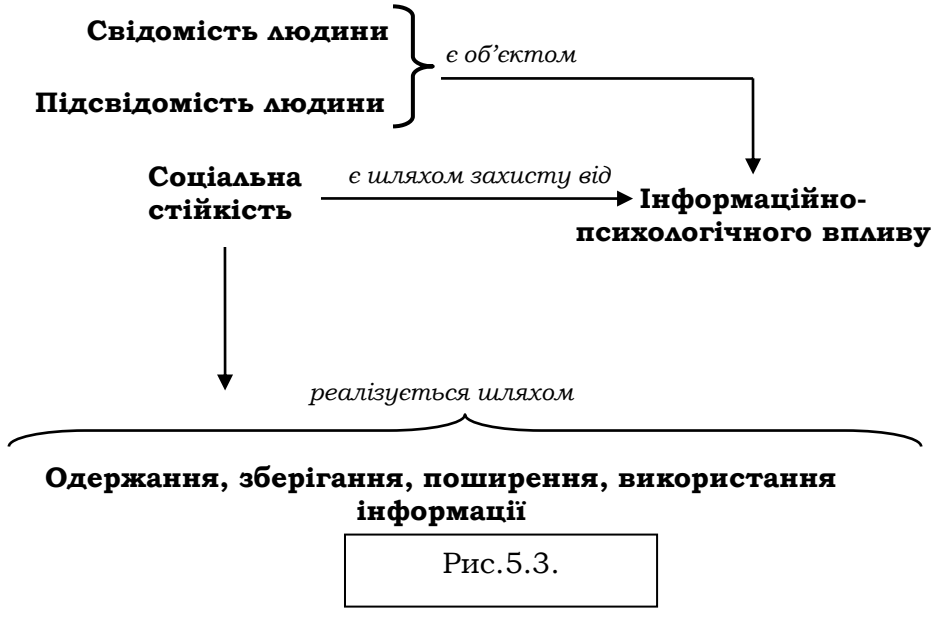


Рис.5.3.

Завдання і питання для самоперевірки

1. Розкрийте сутність інформаційно-психологічного маніпулювання в східній культурі.

2. Розкрийте сутність інформаційно-психологічного маніпулювання в західній культурі.

3. Охарактеризуйте зв'язок між соціальною та інформаційною стійкістю особистості.

4. У чому полягає сутність рефлексивного управління особистістю?

5. Назвіть основні права та свободи в інформаційній сфері, що закріплюються Конституцією України.

6. Якими рисами повинні володіти люди, для того щоб швидко адаптуватися в сучасному світі?

7. Назвіть прийоми безпеки ділового спілкування.

Рекомендована література

1. Конституція України. – К. Юніком. 1996.

2. Закон України “Про основи національної безпеки України” (19 червня 2003 року, № 964-IV, Орієнтир, 30 липня 2003 року, №139, с.1–6).

3. Закон України “Про інформацію”

4. *Хмельницький О.О.* Інформаційна культура: Підготовка кадрів до інформаційної роботи: Навчальний посібник. – К.: КНТ, 2007. – 200 с.

5. *Цыдря Ф.Н.* Информатизация, познание, социальное управление. – Кишинев, 1992. – 138 с.

6. *Кормич Б.А.* Інформаційна безпека: організаційно-правові основи: Навч. Посібник. – К.: Кондор, 2004. – 384 с.

7. Ліпкан В.А., Максименко Ю.Є., Желіховський В.М. Інформаційна безпека України в умовах євро інтеграції: Навчальний посібник. – К.: КНТ, 2006. – 280 с.

Використані джерела

1. *Мясников В.С.* Антология хитроумных планов (Вступительная статья к монографии Харро фон Зенгера "Стратагемы. О китайском искусстве жить и выживать. Знаменитые 36 стратагем за три тысячелетия"). - М. - 1995.

2. *Зенгер Х.* Стратагемы. О китайском искусстве жить и выживать. Знаменитые 36 стратагем за три тысячелетия. - М., 1995.

3. *Конрад Н.И.* Сунь-цзы. Трактат о военном искусстве. - М.-Л. - 1959.

4. Искусство войны Сунь-цзы /У Цзин. Семь военных канонов Древнего Китая. - СПб, 1998.
5. *Даллас А.* Искусство разведки. – М.:Международные отношения, 1992. – 288 с.
6. *Буш Дж.* Глядя в будущее. Автобиография. - М., 1989. С.209.
7. *Аристотель* О софистических опровержениях/Сочинения в четырех томах. Т.2, М. – 1978
8. *Карнеги Д.* "Как завоевывать друзей и оказывать влияние на людей". - М., 1989.
9. *Карнеги Д.* "Как вырабатывать уверенность в себе и влиять на людей, выступая публично". - М., 1989.
10. *Карнеги Д.* "Как перестать беспокоиться и начать жить". - М., 1989.
11. *Грасиан Бальтасар.* Карманный оракул, или Наука Благоразумия. - Минск., 1991. С.17-21.
12. *Шостром Э.* Анти-Карнеги, или Человек-манипулятор. - Минск, 1992.
13. *Друнвало Мельхиседек.* Древняя Тайна Цветка Жизни в 5-ти томах .Том1, Том 2/ Пер. с англ. Под ред И.В. Сутовской. – М: София, 2004.
14. Мировоззренческая культура личности / Іванов и др. – К.: Наукова думка, 1986. – 232 с.
15. *Хмельницький О.О.* Інформаційна культура: підготовка кадрів до інформаційної роботи: Навчальний посібник. – К.: КНТ, 2007. – 200 с.
16. Лефевр В.А., Смолян Г.Л. Алгебра конфликта. - М.: Знание, 1968.
17. *Кормич Б.А.* Інформаційна безпека: організаційно-правові основи: Навч. Посібник. – К.: Кондор, 2004. – 384 с.
18. *Ліпкан В.А., Максименко Ю.Є., Желіховський В.М.* Інформаційна безпека України в умовах євро інтеграції: Навчальний посібник. – К.: КНТ, 2006. – 280 с.

19. Конституція України. – К. Юніком. 1996.
20. *Колин К.К.* Информационные ресурсы в системе опережающего образования // Информационные ресурсы России. - №5. – 1997. – с.6-12.
21. *Мицич П.* Как проводить деловые беседы. М., 1987.

ПІСЛЯМОВА

Проблема інформаційної безпеки виникла в процесі формування інформаційного суспільства в Україні. Цей процес набирає темпів, і в ході його в державних структурах та в суспільстві в цілому закріпилось розуміння того, що без ефективного використання інформаційного ресурсу неможливо вирішити не тільки виникаючі соціальні проблеми, але навіть чітко, ясно та зрозуміло сформулювати державні цілі, переконати та об'єднати всіх членів суспільства в необхідності їх досягнення в спільних інтересах.

Як показує вітчизняний та зарубіжний досвід, в процесі інформатизації виникає проблемна суперечлива ситуація. З одного боку, відставання в темпах інформатизації, низька якість інформаційних послуг призводять до зниження темпів економічного розвитку, зниження обороноздатності, інформаційної залежності від інших країн. Це небезпечно.

З іншого боку, розвиток інформатизації відкриває нову небезпеку для суспільства. Різного роду комп'ютерні злочини, приховування або спотворення інформації, використання її проти особи та суспільства. Виникають задачі "захисту інформації" та "захисту від інформації".

Ігнорування проблем інформаційної безпеки може призвести до труднощів в прийнятті найважливіших політичних, економічних, військових та інших рішень, створення атмосфери напруженості і політичної нестабільності в суспільстві, спровокування соціальних, національних і релігійних конфліктів, масових безпорядків, порушення функціонування органів державної влади і управління. А це, у свою чергу, може завдати значних збитків як окремо взятій людині, колективу людей, так і суспільству і, навіть, в цілому всій цивілізації.

Проблеми інформаційної безпеки не можуть бути вирішеними без залучення нових ідей, нових знань, нової політики в сфері інформатизації. Підґрунтям для їх розвитку є розглянутий в підручнику знання-орієнтований підхід до аналітико-синтетичного опрацювання природно-мовної текстової інформації. Найважливішими очікуваними результатами від впровадження знання-орієнтованого підходу є:

створення електронних інформаційних ресурсів та їх оперативне використання в найважливіших сферах державної діяльності;

істотне розширення інформаційного простору за рахунок інтегрування закордонних інформаційних фондів (сучасних досягнень науки, технологій тощо) в національні інформаційні ресурси. Це досягається впровадженням багатомовних ІПС, систем машинного перекладу і реферування;

підвищення якості оцінки поточної ситуації в політичній, економічній, екологічній, соціальній та інших сферах на основі автоматизації обробки великих обсягів інформації, яка розосереджена по різнорідних джерелах, і її аналізу на наявність викривленої і суперечливої інформації, що буде сприяти адекватності рішень, які приймаються на високих державних рівнях.

Всесвітня федерація вчених у серпні 2000 року першою в списку загроз людству в XXI столітті поставила загрозу інформаційній безпеці. Дотепер, однак, розроблення, виробництво, поширення і застосування інформаційної зброї не регулюються міжнародним правом. Три прийняті Генеральними Асамблеями ООН (у 1998–2000 роках) з ініціативи Росії резолюції, хоча і привернули увагу до проблеми інформаційної безпеки, не стали основою для прийняття конкретних кроків з підготовки міжнародного документа, що зупиняє гонку озброєнь в інформаційній сфері.

ДОДАТОК 1.

Засоби самооцінювання

(пояснювання і обґрунтування правильних і застереження проти неправильних відповідей і рішень під час самоконтролю)

Розділ 1

1. Дайте визначення і назвіть сфери національної безпеки держави.

Визначення поняття національної безпеки наведено в Законі України «Про основи національної безпеки України», в статті 6 цього закону перелічено сфери національної безпеки та загрози в кожній сфері.

Підказку на питання дивись:

на сторінці 11наведено визначення національної безпеки (воно також наведено й в глосарію до першого розділу);

на рисунку 1.1. визначені сфери національної безпеки.

2. Як співвідносяться поняття «національна безпека» і «національні інтереси»?

Визначення понять «національна безпека» та «національні інтереси» наведено в Законі України «Про основи національної безпеки України», а також на сторінці 11. Співвідношення понять «національна безпека» та «національні інтереси» представлено на рисунку 2.1. Відповідь на питання, яким чином національна безпека забезпечує національні інтереси, містить стаття 8: «Основні напрями державної політики з питань національної безпеки» Закону України «Про основи національної безпеки України».

3. Сформулюйте основні принципи забезпечення національної безпеки.

Основні принципи забезпечення національної безпеки перераховані в статті 5 Закону України «Про основи національної безпеки України», пояснення дивись в підрозділі 1.1 даного підручника.

4. Сформулюйте основні пріоритети національних інтересів України.

Основні пріоритети національних інтересів України сформульовані в Законі України «Про основи національної безпеки України» в статті 6. Пояснення і обґрунтування дивись в підрозділі 1.2.

5. Сформулюйте основні напрями державної політики з питань національної безпеки України в інформаційній сфері.

Основні напрями державної політики з питань національної безпеки України в інформаційній сфері сформульовані в Законі України «Про основи національної безпеки України» в статті 8. Роль і місце інформаційної безпеки в системі національної безпеки України розкрито в підрозділі 1.3 даного підручника.

6. Дайте загальну характеристику основних функцій системи забезпечення інформаційної безпеки України.

Характеристика основних функцій системи забезпечення інформаційної безпеки України наведена в п. 1.3.1. даного підручника.

7. Назвіть суб'єктів системи забезпечення інформаційної безпеки та дайте характеристику їхнім повноваженням.

Суб'єкти системи забезпечення національної безпеки визначені в статті 4 Закону України «Про основи національної безпеки України». Суб'єкти системи забезпечення інформаційної безпеки та характеристика їх повноважень викладено в п. 1.3.1. даного підручника.

8. Обґрунтуйте положення, що інформаційна безпека є складовою інших сфер національної безпеки держави.

Обґрунтування викладене в п.1.3.2 даного підручника.

Розділ 2

1. Розкрийте сутність інформаційної війни в широкому та вузькому розумінні.

Визначення інформаційної війни в широкому та вузькому розумінні наведено в глосарію до розділу. Сутність поняття розкрито в підрозділі 2.1.

2. Дайте загальну характеристику чинникам, які обумовлюють неминучість інформаційних воєн.

Чинники, які обумовлюють неминучість інформаційних воєн, та їх загальна характеристика наведена в підрозділі 2.2.

3. Яка роль відводиться інформаційній війні в Стратегії національної безпеки США для нового сторіччя?

Роль і місце, які відводяться інформаційній війні в Стратегії національної безпеки США для нового сторіччя, описані в п. 2.3.1 даного підручника.

4. Дайте загальну характеристику поглядів військового керівництва США на ведення інформаційної війни.

Характеристика поглядів військового керівництва США на ведення інформаційної війни наведена в п.2.3.1 даного підручника.

5. Дайте загальну характеристику поглядів на інформаційну війну китайських військових аналітиків.

Характеристика поглядів на інформаційну війну китайських військових аналітиків наведена в п.2.3.2 даного підручника.

6. Дайте загальну характеристику поглядів російських військових фахівців на роль інформаційної компоненти у війнах майбутнього.

Характеристика поглядів російських військових фахівців на роль інформаційної компоненти у війнах майбутнього наведена в п.2.3.3 даного підручника.

Розділ 3

1. Дайте визначення інформаційної безпеки.

Відповідь на питання викладено в підрозділі 3.1 даного підручника.

2. Чим характеризуються інформаційна безпека суспільства, держави і особистості?

Відповідь на питання викладено в підрозділі 3.1 даного підручника.

3. Дайте визначення інформаційної загрози.

Відповідь на питання викладено в підрозділі 3.1 даного підручника.

4. Наведіть перелік загроз національним інтересам в інформаційній сфері.

Загрози національним інтересам в інформаційній сфері сформульовані в Законі України «Про основи національної безпеки України» в статті 7. Дивись також інформаційні загрози в підрозділі 3.1 даного підручника.

5. Дайте визначення і сформулюйте завдання інформаційної боротьби.

Відповідь на питання викладено в підрозділі 3.2 даного підручника.

6. Дайте загальну характеристику класифікації інформаційних ресурсів.

Відповідь на питання викладено в підрозділі 3.3 даного підручника.

7. Які властивості притаманні інформаційній зброї?

Відповідь на питання викладено в підрозділі 3.4.1 даного підручника.

8. Які існують різновиди класифікації інформаційної зброї?

Відповідь на питання викладено в підрозділі 3.4.4 даного підручника.

9. Дайте визначення і розкрийте сутність інформаційних технологій.

Відповідь на питання викладено в підрозділі 3.5.2 даного підручника.

10. Наведіть класифікацію загроз інформаційним технологіям в управлінні і розкрийте їх сутність.

Відповідь на питання викладено в підрозділі 3.5.2 даного підручника.

Розділ 4.

1. Дайте визначення понять свідомість, суспільна свідомість.

Відповідь на питання викладено в підрозділі 4.1.1 та у глосарію до 4 розділу даного підручника.

2. Дайте характеристику моделей впливу на суспільство.

Відповідь на питання викладено в підрозділі 4.1.2 даного підручника.

3. Сформулюйте тези конструювання релігійної комунікації.

Відповідь на питання викладено в підрозділі 4.2 даного підручника.

4. Дайте стислу характеристику основних форм інформаційного пропагандистського впливу.

Відповідь на питання викладено в підрозділі 4.3.1, також у глосарію до 4 розділу даного підручника наведено визначення пропаганди.

5. Які форми використовують для здійснення інформаційного впливу використовують ПР-технології?

Відповідь на питання викладено в підрозділі 4.3.2, також у глосарію до 4 розділу даного підручника наведено визначення ПР-технології.

6. Дайте стислу характеристику нейролінгвістичному програмуванню.

Відповідь на питання викладено в підрозділі 4.3.3, також у глосарію до 4 розділу даного підручника наведено визначення нейролінгвістичного програмування.

7. Назвіть найбільш розповсюджені інформаційні загрози суспільству та чинники їх ескалації.

Відповідь на питання викладено в підрозділі 4.2 даного підручника.

8. Назвіть сучасні засоби впливу на суспільство й дайте їм стислу характеристику.

Відповідь на питання викладено в підрозділі 4.4 даного підручника.

Розділ 5

1. Розкрийте сутність інформаційно-психологічного маніпулювання в східній культурі.

Досвід інформаційно-психологічного маніпулювання в східній культурі визначається стратагемами, сутність яких викладена в підрозділі 5.1.

2. Розкрийте сутність інформаційно-психологічного маніпулювання в західній культурі.

В доповіді необхідно відзначити, що Західна культура має незначний досвід. Здебільшого за починений і адаптований до до західних цінностей східний досвід. Потім дайте характеристику трудам Аристотеля, Карнегі з точки зору інформаційно-психологічних маніпуляцій (матеріал викладено в підрозділі 5.1).

3. Охарактеризуйте зв'язок між соціальною та інформаційною стійкістю особистості.

Відповідь на питання викладено в підрозділі 5.5.1 даного підручника. Відповідь розпочніть з викладення сутності поняття самоорганізація, далі дайте характеристику соціальної стійкості суспільства і після цього переходьте до характеристики соціально-стійкої особистості. Вкажіть, яким чином інформаційний процес впливає на соціальну стійкість особистості. Під час відповіді користуйтесь рисунком 5.3.

4. У чому полягає сутність рефлексивного управління особистістю?

Відповідь на питання викладено в підрозділі 5.3 даного підручника. Під час відповіді акцентуйте увагу на можливостях використання технології рефлексивного управління в інтересах вирішення завдань інформаційної боротьби.

5. Назвіть основні права та свободи в інформаційній сфері, що закріплюються Конституцією України.

Відповідь на питання викладено в підрозділі 5.4 даного підручника. Під час відповіді акцентуйте увагу на зв'язок прав і свобод людини в інформаційній сфері з іншими правами і свободами людини, що закріплені Конституцією України.

6. Якими рисами повинні володіти люди, для того щоб швидко адаптуватися в сучасному світі?

Відповідь на питання викладено в підрозділі 5.5.1 даного підручника. Під час відповіді акцентуйте увагу на складових морально-семантично-фільтра (рис.5.1), поясніть, яким чином ці складові впливають на формування особистості.

7. Назвіть прийоми безпеки ділового спілкування.

Відповідь на питання викладено в підрозділі 5.5.2 даного підручника. Під час відповіді розкрийте сутність аргументації і контраргументації. Придумайте власні приклади ведення аргументації і контраргументації за шаблонами поданими в п. 5.5.2.