

ВСТУП

На початок XXI сторіччя припадає революційна фаза розвитку суспільства: на зміну індустріальному суспільству приходить інформаційно-індустріальне суспільство, в якому великого значення набувають системи поширення, зберігання та обробки інформації. Відображаючи реальність, інформація проникає в усі напрямки діяльності держави, суспільства, громадянина.

З появою нових інформаційних технологій, основаних на широкому впровадженні засобів обчислювальної техніки, зв'язку, систем телекомунікації, інформація стає постійним і необхідним атрибутом забезпечення діяльності держави, юридичних осіб, суспільних об'єднань і навіть пересічних громадян. Системи електронного документообігу в державних установах, система електронних платежів, карткова система сплати телефонних дзвінків, телевізор із телетекстом або телефонні та відеотелефонні розмови через Internet уже стали ознаками повсякденного життя.

Іншим аспектом цих процесів є збільшення кількості важливої інформації, яку обробляють в автоматизованих системах, від якості, достовірності і оперативності одержання якої залежить більшість важливих рішень, що приймаються на різних рівнях: від керівника держави до громадянина. Отже, нормальне життя суспільства все більше залежить від правильності функціонування таких інформаційних систем. Більше того, вони стають і найважливішим об'єктом для атаки з боку сил, ворожих для суспільства (або окремої держави). Інформаційна сфера стає не тільки однією з найважливіших сфер міжнародного співробітництва, але й об'єктом суперництва.

Інформаційний вплив на державу, суспільство, громадянина зараз ефективніший і економніший, ніж політичний, економічний і навіть військовий. Країни з більш розвиненою інформаційною інфраструктурою, установлюючи технологічні стандарти й надаючи покупцям свої ресурси, визначають умови формування і діяльності інформаційних структур в інших країнах, суттєво впливають на розвиток їхніх інформаційних сфер. Під час формування державної інформаційної політики і

програми входження в інформаційне суспільство пріоритетним стає розвиток безпеки інформаційної сфери на основі створення державної системи інформаційної безпеки.

Наведено сучасні погляди на стан та забезпечення інформаційної безпеки особистості, суспільства та держави. Причому інформаційна безпека особистості – це насамперед захищеність психіки і свідомості людини від небезпечних інформаційних впливів: маніпулювання свідомістю, дезінформування, спонукання до самогубства, образ тощо. Інформаційна безпека держави (суспільства) характеризується мірою захищеності держави (суспільства) та стійкості основних сфер життєдіяльності (політики, економіки, науки, техносфери, сфери управління, воєнної сфери тощо) відносно небезпечних (дестабілізуючих, деструктивних, що загрожують державним інтересам) інформаційних впливів, причому як з упровадження, так і добування інформації. Інформаційна безпека – це здатність нейтралізувати такі впливи.

У першій частині посібника розглянуто основи інформаційної безпеки держави.

Докладно окреслено місце й роль інформаційної безпеки в загальній системі національної безпеки:

- визначено поняття національної безпеки, основні категорії національної безпеки, фактори й засоби національної безпеки;
- охарактеризовано основні види національної безпеки відповідно до її рівнів (безпека особистості, суспільства, держави) та змісту (безпека політична, економічна, соціальна, воєнна, екологічна, науково-технічна, безпека інформаційної сфери);
- визначено систему забезпечення національної безпеки, функції системи та повноваження суб'єктів національної безпеки.

До основних положень інформаційної безпеки належать:

- визначення поняття інформаційної безпеки як інформаційної безпеки особистості, держави, суспільства та концепції інформаційної безпеки держави як систематизованої сукупності відомостей про інформаційну безпеку держави та шляхи її забезпечення;
- дестабілізуючі фактори, загрози інформаційній безпеці держави та їхні джерела;

- забезпечення інформаційної безпеки держави, методи та засоби забезпечення у формах інформаційного патронату, інформаційної кооперації та у формі інформаційного протиборства.

В окремому розділі розглянуто основи психологічної війни та інформаційно-психологічної безпеки держави:

- основні поняття психологічної війни як складової інформаційної війни на державному та воєнному рівнях становлять види та закономірності психологічних впливів, зміст психологічних впливів, ефективність психологічних впливів, зміст психологічних операцій, засоби психологічних впливів та органи психологічної війни;

- технології психологічної війни, що передбачають вивчення особливостей об'єктів психологічних операцій, форми психологічної війни (вплив усного мовлення, друкованих та образотворчих засобів, радіо та телебачення), методи переконувального та навіювального впливів, а також особливі способи та прийоми, основані на дезінформуванні, маніпулюванні свідомістю та поширенні чуток та міфів;

- забезпечення інформаційно-психологічної безпеки на основі створення державної системи інформаційно-психологічної безпеки, визначення її функцій, структури, сил та засобів, а також напрямів діяльності: ліцензування, сертифікації, експертизи в галузі інформаційно-психологічної діяльності та контролю за її станом.

В останньому розділі першої частини посібника наведено основи державної інформаційної політики, які полягають у визначенні головних напрямів діяльності держави в основних галузях інформаційної сфери, змісту програми входження держави в інформаційне суспільство та політики забезпечення інформаційної безпеки.

В окремому розділі розглянуто основні властивості інформації як предмета захисту, основні характеристики інформаційних систем як об'єктів безпеки та основні проблеми безпеки інформаційних технологій.

У наступному розділі другої частини посібника розглянуто проблему створення ефективних систем інформаційної безпеки на основі сучасних методів менеджменту, основною метою яких

стало б скорочення матеріальних втрат, пов'язаних з порушенням інформаційної безпеки. Наведено основні положення міжнародного стандарту ISO 17799, основна ідея якого – допомогти державним та комерційним організаціям вирішити доволі складне завдання: не лише забезпечити надійний захист інформації, але й організувати ефективний доступ до даних та нормальну роботу з ними.

У завершальній частині посібника розглянуто підходи до забезпечення інформаційної безпеки України.

Проаналізовано інформаційну безпеку України:

- визначено зміст національних інтересів України в інформаційній сфері та методи їх забезпечення;
- наведено систему загроз та їхніх джерел для інформаційної безпеки України;
- окреслено стан інформаційної безпеки в Україні та сформульовано основні завдання з її забезпечення.

Система методів та заходів забезпечення інформаційної безпеки України має містити загальні правові, організаційно-технічні й економічні методи та заходи, а також методи та заходи, які можна застосовувати у різноманітних сферах життєдіяльності держави та суспільства: у сфері економіки, внутрішньої та зовнішньої політики, оборони, духовного життя, у галузі науки і техніки, в загальнодержавних інформаційних і телекомунікаційних системах, у правоохоронній і судовій сферах, в умовах надзвичайних ситуацій.

Невід'ємною частиною інформаційної безпеки України повинне стати міжнародне співробітництво в галузі забезпечення інформаційної безпеки як складової частини політичної, воєнної, економічної, культурної та інших видів взаємодії країн, що входять до світового співтовариства.

У лекційному курсі наведено основні функції та основні елементи організаційних основ системи забезпечення інформаційної безпеки України. Сформульовано основні положення політики інформаційної безпеки України та перелік першочергових заходів щодо її реалізації.