

УДК 342.9

*Валентин Михайлович Петрик*

## **“ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ” ЯК НОВІТНЯ НАВЧАЛЬНА ДИСЦИПЛІНА: ОСОБЛИВОСТІ ВИКЛАДАННЯ ТА НАВЧАЛЬНО-МЕТОДИЧНОГО ЗАБЕЗПЕЧЕННЯ**

Постійне зростання впливу інформаційної сфери характерне для сучасного етапу розвитку суспільства. До структури цієї сфери входять: сукупність інформації, інформаційних зв'язків та інформаційних систем, об'єктів, які готують інформацію, зберігають, розповсюджують і використовують її, а також система регулювання інформаційних відносин. Сформувалася дуже важлива залежність національної безпеки держави від такої її важливої складової як інформаційна безпека, яка постійно зростатиме у міру розвитку інформаційних технологій і процесу глобалізації. Зазначене зумовлює важливість вивчення навчальної дисципліни “Інформаційна безпека держави”.

На сьогодні є значна кількість навчальних дисциплін та спецкурсів з інформаційної безпеки, де здебільшого розглянуто інформаційно-технічні аспекти, правові й загальні положення зазначеної проблематики. Слід відмітити, що з метою підвищення ефективності захисту людини, суспільства та держави від негативних інформаційних впливів необхідно розробляти відповідні навчальні дисципліни і навчальну літературу (посібники, підручники) для підготовки висококваліфікованих фахівців (державних службовців, політологів, правознавців, соціологів, психологів, журналістів, представників силових відомств та ін.), а також формування критичного мислення широких верств населення. Тому тема і зміст навчальної дисципліни “Інформаційна безпека держави” є вкрай *актуальними*.

**Мета** вивчення навчальної дисципліни “Інформаційна безпека держави” полягає у набутті студентом та курсантом компетенцій, знань, умінь і навичок для подальшого використання у своїй практичній діяльності по забезпеченню інформаційної безпеки України з урахуванням досягнень науково-технічного прогресу та міжнародного досвіду.

**Завдання** вивчення навчальної дисципліни:

- розширити і систематизувати знання щодо загроз національній безпеці в інформаційній сфері;

- набути знання щодо історії та сучасності проведення акцій інформаційного впливу, спеціальних інформаційних операцій, інформаційних війн;
- здобути знання про нормативно-правове регулювання інформаційної безпеки та систему суб'єктів забезпечення інформаційної безпеки України;
- сформувати критичне мислення для набуття навичок із захисту від маніпулятивного впливу;
- розвинути вміння щодо управління інформаційною безпекою держави.

**Предметом** навчальної дисципліни є зміст інформаційної безпеки, можливі та потенційні загрози національній безпеці в інформаційній сфері і основи забезпечення інформаційної безпеки держави. **Об'єкт** навчальної дисципліни — інформаційна безпека як невід'ємна складова національної безпеки.

**Значення і місце** навчальної дисципліни у підготовці фахівців: навчальна дисципліна “Інформаційна безпека держави” відіграє важливу роль у підготовці фахівців освітньо-кваліфікаційного рівня “бакалавр” за напрямками “Управління інформаційною безпекою” та “Організація захисту інформації з обмеженим доступом”, курсантів НА СВ України для ефективного забезпечення інформаційної складової національної безпеки.

**Перелік знань** навчальної дисципліни “Інформаційна безпека держави”. Необхідно **знати**: базові поняття щодо інформаційної безпеки держави, суспільства і особи; види та сучасні технології інформаційних впливів; сутність форми і види інформаційного протиборства; етапи, ознаки, суб'єкти та методи проведення спеціальних інформаційних операцій; завдання, об'єкти посягань, форми проведення інформаційної війни; історію і особливості сучасного стану інформаційно-психологічного протиборства, склад злочинів у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж і мереж електрозв'язку; особли-

вості впливу на інформаційний простір України засобів масової інформації та неурядових організацій; сучасні піар-технології як механізм впливу на інформаційну сферу нашої держави; духовно-релігійну складову національної безпеки України; інформаційні аспекти економічного протиборства та тероризму; сучасний досвід США, ФРН, Франції, РФ і КНР щодо забезпечення інформаційної безпеки та проведення інформаційно-психологічного протиборства; нормативно-правове регулювання забезпечення інформаційної безпеки України; державну систему забезпечення інформаційної безпеки України і суб'єкти, які її утворюють.

**Перелік вмінь навчальної дисципліни "Інформаційна безпека держави".** Необхідно *вміти*: узагальнювати теоретичні уявлення щодо сутності інформаційної безпеки; виявляти існуючі та потенційні загрози національній безпеці України в інформаційній сфері; виявляти приховані та шкідливі інформаційно-психологічні впливи; здійснювати порівняльний аналіз форм, методів, засобів та технологій проведення інформаційних війн, акцій інформаційного впливу і спеціальних інформаційних операцій; здійснювати прогнози щодо можливих небезпек інформаційному простору держави; надати кримінологічну характеристику злочинам у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж і мереж електронного зв'язку; виявляти ступінь впливу на національну безпеку ЗМІ, громадських та релігійних організацій; використовувати світовий досвід щодо забезпечення інформаційної безпеки для його творчого впровадження на українських теренах; аналізувати сучасний стан нормативного регулювання та державної системи забезпечення інформаційної безпеки нашої держави, а також розробляти пропозиції щодо їх вдосконалення; проводити аналітичні дослідження у сфері інформаційної безпеки України; використовувати піар-технології для захисту національної безпеки в інформаційній сфері.

*Організаційні форми, методи та засоби забезпечення високої фундаментальної, професійної і практичної спрямованості та диференційованого підходу навчання студентів, курсантів:* для ефективної організації навчальних занять використовуються такі форми роботи, як розповідь, учбова лекція, семінар, дискусія, робота з книгою, постановки завдань, планування процесом виконання, ілюстрування, демонстрування, регулювання і контроль, аналіз підсумків практичної роботи.

Також використовуються такі методи як, індуктивний, дедуктивний, продуктивний, дослідницький, стимулювання. Індуктивний метод навчання полягає в тому, що викладач спершу викладає факти, проводить дослідди, поступово підводить студентів, курсантів до узагальнень, визначення понять. Дедуктивний метод навчання полягає в тому, що ви-

кладач повідомляє загальне положення, закон, а потім роблячи висновки поступово підводить до конкретних висновків, ставить конкретні завдання. Продуктивний метод навчання пов'язаний з опануванням нових знань в процесі творчої роботи. Дослідницький метод навчання застосовується для засвоєння досвіду творчої діяльності, глибоких знань. Методи стимулювання спеціально спрямовані на формування позитивних мотивів навчання, стимулюють пізнавальну активність, водночас сприяють збагаченню курсантів, студентів новою інформацією.

Засоби навчання виступають тим інструментарієм, за допомогою якого він впливає на розум, почуття і волю студентів, курсантів для активізації їхньої пізнавальної діяльності й інтенсифікації процесу навчання. Підручники та посібники служать студенту, курсанту повторення та закріплення знань, самостійної підготовки до семінарських занять. Схеми використовуються під час читання лекцій із сутності інформаційної безпеки та про загальнодержавну систему забезпечення інформаційної безпеки України. Кінофрагменти з використанням мультимедійного обладнання застосовуються для ілюстративного супроводження лекції. Під час проведення практичних занять навчальні фільми демонструються тільки після ґрунтовного засвоєння студентами, курсантами теоретичного матеріалу. Одні навчальні фільми показують з метою їх аналізу для встановлення особливостей проведення акцій інформаційного впливу, спеціальних інформаційних операцій, інформаційних війн, еволюції ІПП. Інші навчальні фільми є тенденційними з використанням дезінформування та інших маніпулятивних технологій, які необхідно студентам, курсантам виявити і охарактеризувати, що формує навички критичного мислення студента, курсанта.

Навчальна дисципліна викладається за кредитно-модульною системою. При проведенні занять за кредитно-модульною системою реалізуються вимоги модульного структурування змісту застосування 100-бальної рейтингової системи оцінювання рівня навчальних здобутків студентів. Поточне оцінювання здійснюється усним (фронтальним та індивідуальним) опитуванням й письмовим контролем знань.

Практична та професійна спрямованість дисципліни зумовлена набуттям знань і вмінь щодо управління інформаційною безпекою. Насамперед, це знання та вміння, які дозволяють виявляти загрози національній безпеці в інформаційній сфері, аналізувати сучасний стан системи забезпечення інформаційної безпеки України і розробляти пропозиції щодо її вдосконалення.

**Взаємозв'язок з суміжними дисциплінами:** вивчення навчальної дисципліни "Інформаційна безпека держави" поглиблює знання студентів, отримані під час вивчення двох дисциплін "Основи інформаційної безпеки" й

“Основи національної безпеки”, а курсанти дисципліни “Основи національної безпеки”. Дисципліна “Інформаційна безпека держави” дає фундаментальні знання для вивчення навчальної дисципліни “Забезпечення інформаційної безпеки” при підготовці фахівців освітньо-кваліфікаційного рівня “бакалавр” за напрямом “Управління інформаційною безпекою”, а також навчальної дисципліни “Основи інформаційного протидіювання” при підготовці фахівців освітньо-кваліфікаційного рівня “спеціаліст” за напрямом “Організація захисту інформації з обмеженим доступом”.

Базовою літературою навчальної дисципліни “Інформаційна безпека держави” є підручники “Інформаційна безпека (соціально-правові аспекти)”, “Історія інформаційно-психологічного протидіювання” [1—2] та навчальні посібники “Сугестивні технології маніпулятивного впливу”, “Інформаційно-психологічна безпека в епоху глобалізації” [3—4].

Підручник “Інформаційна безпека (соціально-правові аспекти)” [1] затверджений



Міністерством освіти і науки України (лист 1.4/18-Г-133.1 від 10 січня 2009 року) написаний авторським колективом, до складу якого входять представники Національної академії СБ України (Є. Д. Скулиш, В. В. Остроухов, В. М. Петрик, Л. Ф. Компанцева, О. А. Штоквиц, Д. С. Мельник, М. М. Галамба) та

інші провідні вітчизняні фахівці з проблем забезпечення інформаційно-психологічної складової національної безпеки (М. М. Присяжнюк, А. М. Кузьменко, Я. М. Жарков, Ю. М. Супрунов).

У першій частині “Небезпеки інформаційного простору для людини” (7 розділів) розкриваються технології маніпулювання свідомістю особистості та особливості протидії їм. Друга частина — “Сутність інформаційно-психологічного протидіювання” (7 розділів) — присвячена теорії, історії і світовому досвіду цього протидіювання. У третій частині “Загрози національній безпеці України в інформаційно-психологічній сфері. Шляхи забезпечення інформаційно-психологічної безпеки” (9 розділів) розглядаються впливи на інформаційну безпеку України ЗМІ, неурядових та релігійних організацій, а також здійснено аналіз сучасного стану державної системи забезпечення інформаційної безпеки України й розробляються шляхи її вдосконалення. Практичне значення має додаток — програма навчального курсу “Інформаційна безпека (соціально-правові аспекти)” (144 ауд. год.), яка дає змогу впроваджувати матеріали підручника в навчальний процес.

Цей підручник використовується у НА СБ України (504 ауд. год.):

1. Для викладання в Навчально-науковому інституті інформаційної безпеки НА СБ України:

– для потоку студентів за спеціальністю “Організація захисту інформації з обмеженим доступом” навчальних дисциплін “Інформаційна безпека держави” (72 ауд. год.) та “Інформаційне протидіювання” (54 ауд. год.).

– при підготовці фахівців освітньо-кваліфікаційного рівня “бакалавр” напряму “Управління інформаційною безпекою” навчальних дисциплін “Вступ до спеціальності” (36 ауд. год.), “Інформаційна безпека держави” (144 ауд. год.), “Забезпечення інформаційної безпеки” (126 ауд. год.).

2. Для викладання курсантам навчальної дисципліни “Інформаційна безпека держави” (36 ауд. год.)

3. Для використання у викладанні слухачам на потоках перепідготовки і підвищення кваліфікації оперативного та керівного складу СБ України (36 ауд. год.).

Підручник “Історія інформаційно-психологічного протидіювання” [2] розроблено авторським колективом, до складу якого входять представники Національної академії СБ України (Є. Д. Скулиш, В. М. Петрик, В. В. Остроухов, Л. Ф. Компанцева) та інші провідні фахівці нашої держави з питань дослідження теорії та історії інформаційного протидіювання (Я. М. Жарков, М. М. Присяжнюк).

У цьому підручнику розкривається еволюція інформаційно-психологічного протидіювання від стародавніх часів до сьогодення. Показано сутність і засоби ведення інформаційного протидіювання (інформаційних війн, спеціальних інформаційних операцій та акцій інформаційного впливу) з використанням інформаційної зброї та інших сучасних технологій інформаційного впливу.

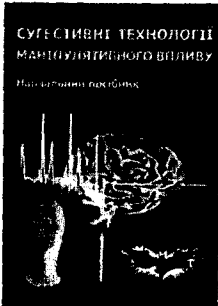
Підручник розраховано на студентів і викладачів вищих навчальних закладів гуманітарної спрямованості, насамперед для підготовки курсантів, істориків, психологів, журналістів та політологів. Цим виданням також можуть користуватися представники Служби безпеки, Служби зовнішньої розвідки, Міністерства оборони України та інших силових відомств.

Навчальний посібник “Сугестивні технології маніпулятивного впливу” [3] розроблено авторським колективом, до складу якого входять представники Національної академії СБ України (В. М. Петрик, Є. Д. Скулиш, В. В. Остроухов, Л. Ф. Компанцева) та інші провідні фахівці нашої держави з питань дослідження сугестивних технологій маніпулятивного впливу та протидії їх дест-



руктивним проявам (О. Д. Бойко, М. М. Присяжнюк).

У цьому посібнику наводяться основні поняття, розкриваються сутність та засоби маніпулювання свідомістю. Досліджуються особливості маніпулятивного впливу з використанням нейролінгвістичного програмування, піару та інших сучасних сугестивних технологій. Практичне значення має дода-ток — програма навчального курсу “Сугес-тивні технології маніпулятивного впливу”



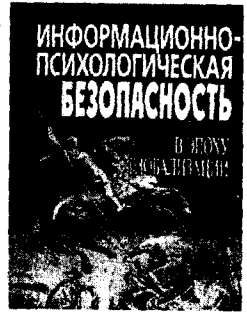
(56 ауд. год.), яка надає можливість впровадження матеріалів посібника в навчальний процес. Об'єктом навчального курсу є маніпулятивний вплив на психіку людини. Предметом — сугестивні технології маніпулятивного впливу (нейролінгвістичне програмування, сугес-тивні технології маніпулятивного впливу)

(нейролінгвістичне програмування, сугес-тивні технології маніпулятивного впливу) в Інтернеті, чорний піар і чорна риторика) та базові стратегії й механізми захисту від маніпулювання.

У навчальному посібнику “Інформаційно-психологічна безпека в епоху глобалізації” [4] розглядається широкий спектр загроз безпеці держави, суспільства і окремої особи в інформаційній сфері, а також сучасні технології маніпуляції свідомістю. Посібник призначено для студентів і викладачів вищих навчальних закладів гуманітарної спрямованості, насамперед при підготовці державних управлінців, політологів, право-

знавців, психологів, соціологів і журналістів. Так само становить інтерес для відповідних фахівців збройних сил, державних і недержавних спецслужб.

Таким чином, український науковий дискурс поповнився новими ґрунтовними підручниками, що є свідченням розвитку й становлення галузі інформаційної безпеки. Нагальною потребою на сьогодні залишається розробка підручника “Інформаційна безпека держави” та впровадження його матеріалів у навчальний процес вищих навчальних закладів (за єдиною навчальною програмою) із залученням всіх провідних фахівців України у цій галузі.



## Література

1. Інформаційна безпека (соціально-правові аспекти) : [підручник] / [В. В. Остроухов, В. М. Петрик, М. М. Присяжнюк та ін.] ; за ред. Є. Д. Скулиша. — К. : КНТ, 2010. — 776 с. 2. Історія інформаційно-психологічного протистояння : [підручник] / [В. М. Петрик, М. М. Присяжнюк, Я. М. Жарков, Є. Д. Скулиш, Л. Ф. Компанцева, В. В. Остроухов] ; за заг. ред. Є. Д. Скулиша. — К. : Наук.-вид. відділ НА СБ України, 2011. — 212 с. 3. Сугестивні технології маніпулятивного впливу : [навч. посібник] / [В. М. Петрик, М. М. Присяжнюк, Л. Ф. Компанцева та ін.] ; за заг. ред. Є. Д. Скулиша. — К. : Наук.-вид. відділ НА СБ України, 2010. — 248 с. 4. Информационно-психологическая безопасность в эпоху глобализации : [учеб. пособие] / [В. М. Петрик, В. В. Остроухов, А. А. Штоквиш и др.] ; под. ред. В. В. Остроухова. — К., 2008. — 544 с.

В статье рассматриваются особенности внедрения в учебный процесс Национальной академии Службы безопасности Украины дисциплины “Информационная безопасность государства”, а также анализируется уровень обеспечения этой дисциплины соответствующими учебниками и учебными пособиями, которые являются творческой разработкой ведущих специалистов в области информационной безопасности в Украине.

**Ключевые слова:** информационная безопасность государства, информационно-психологическое противоборство, сугестивные технологии.

Peculiarities of introduction of the course “Information Security of the State” in educational process of the National Academy of the Security Service of Ukraine are examined in the article. The amount of available textbooks and learning aids for this course, which were created by the leading specialists in the sphere of information security of Ukraine, is analyzed.

**Key words:** information security of the state, information-and-psychological contention, suggestive methods.