ЗМІСТ

Інформаційна безпека

Подивитись анотацію та купити на **jurkniga.ua**

Анотація

У підручнику розкрито концептуальні засади інформаційної безпеки, національні інтереси в інформаційній сфері, стратегія формування та розвитку єдиного інформаційного простору України, загрози безпеці держави та її громадянам в інформаційній сфері, технології інформаційного та інформаційно-психологічного впливу й захисту від цих впливів, система забезпечення інформаційної безпеки України, особливості функціонування та функції її субєктів. Підручник затверджено для викладання навчальних дисциплін "Інформаційна безпека" та "Інформаційна безпека держави".

Окремі розділи підручника можуть використовуватися при викладанні навчальних дисциплін "Інформаційне протиборство", "Забезпечення інформаційної безпеки держави", "Організаційно-правові основи забезпечення інформаційної безпеки" та "Кібербезпека".

Він розрахований на студентів і викладачів вищих навчальних закладів гуманітарної спрямованості, насамперед для підготовки державних службовців, правознавців, психологів, журналістів, політологів та кримінологів. Це видання також буде корисним для аспірантів, науковців, практикуючих психологів, представників спецслужб та інших силових відомств.

Національна академія Служби безпеки України

ОСТРОУХОВ В. В., ПРИСЯЖНЮК М. М.,
ФАРМАГЕЙ О. І., ЧЕХОВСЬКА М. М. та ін.

ІНФОРМАЦІЙНА БЕЗПЕКА

Підручник

Київ
Видавництво Ліра-К
2021

УДК 351.746.1:159.964

Затверджено вченою радою Національної академії СБ України,
(протокол № 11 від 8 грудня 2020 року)

РЕЦЕНЗЕНТИ:
Ю. В. РОМАНЕНКО − д. соціол. н., проф., В. О. ХОРОШКО − д. т. н., проф.,
О. В. ШМОТКІН − д. ю. н., проф., О. Ф. БАНТИШЕВ − к. ю. н., проф.

НАУКОВІ КОНСУЛЬТАНТИ:
М. П. СТРЕЛЬБИЦЬКИЙ − д. ю. н., проф., Н. Г. ІВАНОВА, д. психол. н., проф.

Інформаційна безпека. Підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова – К.: Видавництво Ліра-К, 2021. – 412 с.

ISBN 978-617-520-081-0

У підручнику розкрито концептуальні засади інформаційної безпеки, національні інтереси в інформаційній сфері, стратегія формування та розвитку єдиного інформаційного простору України, загрози безпеці держави та її громадянам в інформаційній сфері, технології інформаційного та інформаційно-психологічного впливу й захисту від цих впливів, система забезпечення інформаційної безпеки України, особливості функціонування та функції її суб'єктів.

Підручник затверджено для викладання навчальних дисциплін "Інформаційна безпека" та "Інформаційна безпека держави". Окремі розділи підручника можуть використовуватися при викладанні навчальних дисциплін "Інформаційне протиборство", "Забезпечення інформаційної безпеки держави", "Організаційно-правові основи забезпечення інформаційної безпеки" та "Кібербезпека". Він розрахований на студентів і викладачів вищих навчальних закладів гуманітарної спрямованості, насамперед для підготовки державних службовців, правознавців, психологів, журналістів, політологів та кримінологів. Це видання також буде корисним для аспірантів, науковців, практикуючих психологів, представників спецслужб та інших силових відомств.

УДК 351.746.1:159.964

Внесок авторів:
Остроухов В. В. – вступ, загальна редакція, підрозділи 4.4, 4.6; Петрик В. М. – підрозділи 1.1, 1.2, 3.1.1, 3.1.2, 5.2; Фармагей О. І. – підрозділи 1.3, 1.4; Присяжнюк М. М. – розділ 2, підрозділи 3.1, 3.1.3, 4.1, 4.3, 4.5, 5.1, 5.3, 7.1, Іменний покажчик, Тематичний покажчик, Робоча програма навчальної дисципліни; Карпович О. М. – підрозділи 4.1.1, 4.1.2, 4.2; Чеховська М. М. – розділ 6; Мельник Д. С. – підрозділи 4.3.1, 7.2., 7.3.

ISBN 978-617-520-081-0

© Остроухов В.В., Присяжнюк М.М.,
Фармагей О.І., Чеховська М.М. та ін., 2021
© Видавництво Ліра-К, 2021

ЗМІСТ

ВСТУП…… 5

РОЗДІЛ 1. Концептуальні засади інформаційної безпеки …….. 7
1.1. Базові поняття щодо інформації та інформаційної безпеки…… 7
1.2. Інформаційний вплив та його різновиди……..…… 13
1.3. Визначення об'єктів інформаційного впливу……... 18
1.4. Інформаційна безпека як складова національної безпеки держави……. 29

РОЗДІЛ 2. Інтереси держави в інформаційній сфері……... 37
2.1. Загальна характеристика інтересів держави у сфері інформаційної безпеки…… 37
2.2. Інформаційна політика держави..…….. 44
2.3. Політико-правові аспекти формування інформаційного суспільства держави…….. 61
2.4. Стратегія формування та розвитку єдиного інформаційного простору України…… 76

РОЗДІЛ 3. Загрози безпеці держави в інформаційній сфері…….. 90
3.1. Поняття та види загроз безпеці держави в інформаційній сфері 90
3.1.1. Інформаційні війни як джерело загроз безпеці держави в інформаційній сфері……. 91
3.1.2. Спеціальні інформаційні операції в міжнародній політиці..... 98
3.1.3. Інформаційна зброя як засіб ведення інформаційного протиборства……. 110

РОЗДІЛ 4. Загрози людині та суспільству в інформаційній сфері…..... 127
4.1. Поняття і сутність маніпулювання свідомістю людини……. 127
4.1.1. Способи та технології маніпулювання свідомістю людини…. 131
4.1.2. Технології масового маніпулятивного впливу…….. 133
4.2. Поняття та напрями реалізації сугестивних технологій маніпулятивного впливу……. 159
4.3. Реалізація маніпулятивних технологій в засобах масової інформації ……..... 171
4.3.1. Фактори впливу на діяльність засобів масової інформації..... 179
4.4. Вплив на людину певних фізичних факторів інформаційного середовища……..... 185
4.5. Вікна Овертона в аспекті інформаційної безпеки…… 197
4.6. Інформаційно-психологічна безпека особи..... 201

РОЗДІЛ 5. Загрози інформаційній безпеці в інформаційно-комунікаційних мережах……. 212
5.1. Інтернет як арена сугестивного маніпулятивного впливу...…..... 212
5.2. Соціальна інженерія в аспекті маніпулятивного впливу……. 228

5.3. Комп'ютерна злочинність та кібертероризм як загрози інформаційній безпеці……..……..... 242

РОЗДІЛ 6. Захист від загроз маніпулятивного впливу……. 254
6.1. Базові стратегії та механізми психологічного захисту…… 256
6.2. Як розпізнати загрозу маніпулювання й протидіяти йому…….. 259

РОЗДІЛ 7. Система забезпечення інформаційної безпеки України….. 267
7.1. Стан інформаційної безпеки держави..... 267
7.2. Структура загальнодержавної системи забезпечення інформаційної безпеки України, завдання та функції її суб'єктів..... 272
7.3. Діяльність спеціальних служб України у сфері забезпечення інформаційної безпеки держави……. 351

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ 380

ІМЕННИЙ ПОКАЖЧИК…… 386

ТЕМАТИЧНИЙ ПОКАЖЧИК…….. 391

ДОДАТКИ..... 394
Додаток1.
Робоча програма навчальної дисципліни "Інформаційна безпека"... 394

ВСТУП

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.

Останнім часом визначальної ваги набуває інформаційна безпека. Рівень інформаційного потенціалу все більшою мірою обумовлює оперативність прийняття державних 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. 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.

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 є невід’ємною складовою державної політики національної безпеки і являє собою офіційно прийняту систему поглядів та практичну діяльність органів державної влади і управління, спрямовану на забезпечення такого стану захищеності інтересів людини, суспільства та держави, при якому досягається інформаційний розвиток (інтелектуальний, соціально-політичний, технічний, морально-етичний), за якого сторонні інформаційні впливи не завдають їм суттєвої шкоди.

Інформаційна безпека є, як важливою самостійною сферою забезпечення національної безпеки, так і невід'ємною складовою кожної зі сфер національної безпеки. Інформаційні простір, інформаційні ресурси, інформаційна інфраструктура та технології значною мірою впливають на рівень і темпи соціально-економічного, науково-технічного й культурного розвитку. Тому розвиток України як суверенної, демократичної, правової та економічно стабільної держави можливий за умови забезпечення інформаційної безпеки.

Для сучасного етапу генезису суспільства характерне постійне зростання впливу інформаційної сфери, до складу якої входять: інформація, інформаційні зв'язки та інформаційні системи, об'єкти, які займаються підготовкою, зберіганням, поширенням і використанням інформації, а також система регулювання інформаційних відносин.

Національна безпека держави має стійку залежність від інформаційної безпеки, яка постійно зростає із розвитком інформаційних технологій.

Для ефективного забезпечення національної безпеки в інформаційній сфері необхідні відповідні висококваліфіковані спеціалісти.

Навчальна дисципліна "Інформаційна безпека" відіграє важливу роль у підготовці фахівців освітньо-кваліфікаційних рівнів "бакалавр" та "магістр" за спеціальностями 256 Національна безпека (за окремими сферами забезпечення і видами діяльності), 251 Державна безпека (спеціалізація – управління у сфері забезпечення державної безпеки) та 125 Кібербезпека (управління інформаційною безпекою) Вона викладається після дисципліни "Національна безпека" й забезпечує фундаментальні знання для вивчення курсу "Забезпечення інформаційної безпеки держави" та деяких інших спеціальних і професійно орієнтованих дисциплін.

Під час вивчення дисципліни "Інформаційна безпека" здобувачі вищої освіти отримують теоретичні знання та практичні навички, необхідні для подальшої професійної діяльності в Службі безпеки України, Міністерстві оборони України, Державній службі спеціального зв'язку та захисту інформації України та інших структурах, що забезпечують національну безпеку в інформаційній сфері держави.

Підручник буде корисним для якісного засвоєння навчальної дисципліни "Інформаційна безпека", сприятиме реалізації вимог освітньо-кваліфікаційної характеристики та освітньо-професійної програми підготовки кваліфікованих фахівців, що передбачають оволодіння знаннями і вміннями для вирішення професійно орієнтованих типових завдань.

РОЗДІЛ 1.

КОНЦЕПТУАЛЬНІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Базові поняття щодо інформації та інформаційної безпеки

Інформація (згідно Закону України "Про інформацію") − це будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

Але більш повне визначення: **"інформація"** (лат. informatio – роз'яснення, виклад, тлумачення) – це відомості про осіб, предмети, технології, засоби, ресурси, події та явища, що відбуваються в усіх сферах діяльності держави, життя суспільства й в довкіллі, незалежно від форми їх надання. Відомості можуть бути подані у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб.

Документ – це матеріальний носій, що містить інформацію, основними функціями якого є її збереження та передавання у часі та просторі.

Особистість постійно перебуває під впливом інформації, що поширюється в просторі цілеспрямовано або довільно. До розвитку сучасних кібернетичних систем під простором поширення інформації розуміли атмосферу, стратосферу, космос, водні акваторії океанів і морів. Зараз розуміння інформаційного простору включає додатково кібернетичні та віртуальні системи. Розглядаючи вплив інформаційного простору на особистість, слід враховувати, що він здійснюється також і на суспільство та державу і через них опосередковано на кожного індивідуума. Цей вплив може носити конструктивний (безпечний) і деструктивний (небезпечний) характер.

Основні принципи інформаційних відносин:

- гарантованість права на інформацію;
- відкритість, доступність інформації та свобода обміну нею;
- достовірність і повнота інформації;
- свобода вираження поглядів і переконань;
- правомірність одержання, використання, поширення, зберігання та захисту інформації;
- захищеність особи від втручання в її особисте та сімейне життя..

Суб'єкти інформаційних відносин:

- фізичні особи;
- юридичні особи;
- об'єднання громадян;
- суб'єкти владних повноважень.

Суб'єкт владних повноважень – це орган державної влади, орган місцевого самоврядування, інший суб'єкт, що здійснює владні управлінські функції відповідно до законодавства, у тому числі на виконання делегованих повноважень.

Об'єктом інформаційних відносин є інформація.

Кожен має право на інформацію, що передбачає можливість вільного

одержання, використання, поширення, зберігання та захисту інформації, необхідної для реалізації своїх прав, свобод і законних інтересів.

Реалізація права на інформацію не повинна порушувати громадські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи і законні інтереси інших громадян, права та інтереси юридичних осіб.

Право на інформацію забезпечується:

- створенням механізму реалізації права на інформацію;
- створенням можливостей для вільного доступу до статистичних даних, архівних, бібліотечних і музейних фондів, інших інформаційних банків, баз даних, інформаційних ресурсів;
- обов'язком суб'єктів владних повноважень інформувати громадськість та засоби масової інформації про свою діяльність і прийняті рішення;
- обов'язком суб'єктів владних повноважень визначити спеціальні підрозділи або відповідальних осіб для забезпечення доступу запитувачів до інформації;
- здійсненням державного і громадського контролю за додержанням законодавства про інформацію;
- встановленням відповідальності за порушення законодавства про інформацію.

Право на інформацію 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.

Інформаційна діяльність – це сукупність дій, спрямованих на задоволення інформаційних потреб громадян, юридичних осіб і держави.

Основними *напрямами інформаційної діяльності* є: політичний, економічний, соціальний, духовний, екологічний, науково-технічний, міжнародний тощо. Держава гарантує свободу інформаційної діяльності в цих напрямах всім громадянам та юридичним особам в межах їх прав і свобод, функцій і повноважень.

Основними видами інформаційної діяльності є створення, збирання, одержання, зберігання, використання, поширення, охорона та захист інформації.

Інформаційні ресурси України − це вся інформація, яка належить нашій державі, незалежно від змісту, форм, часу й місця створення, поширення та зберігання. Україна самостійно формує інформаційні ресурси на своїй території та вільно розпоряджається ними, за винятком випадків, передбачених законами і міжнародними договорами. Національні інформаційні ресурси є основою інформаційного суверенітету України.

Одним з найважливіших елементів, що є основою реалізації державою своєї політики в інформаційній сфері, виступає інформаційна інфраструктура. **Інформаційна структура** – невід'ємний елемент, як стратегічних інформаційних ресурсів, що є основою обороноздатності

держави, так і інформаційного ринку, що на сьогоднішній день багато в чому обумовлює економічний потенціал і перспективи розвитку держави.

Так, Законом України "Про національну програму інформатизації" окреслені основні *складові національної інформаційної інфраструктури* (національної інфраструктури інформатизації), що включає:

- міжнародні та міжміські телекомунікаційні і комп'ютерні мережі;
- систему інформаційно-аналітичних центрів різного рівня;
- інформаційні ресурси;
- інформаційні технології;
- систему науково-дослідних установ з проблем інформатизації;
- виробництво та обслуговування технічних засобів інформатизації;
- систему підготовки висококваліфікованих фахівців у сфері інформатизації.

Інформаційний суверенітет − це невід'ємне право людини, суспільства, держави на самовизначення та участь у формуванні, розвитку та здійсненні національної інформаційної політики відповідно до Конституції, чинного законодавства України, міжнародного права в національному інформаційному просторі України.

Інформаційний суверенітет України забезпечується:

- виключним правом власності України на інформаційні ресурси, що формуються за рахунок коштів державного бюджету;
- створенням національних інформаційних систем;
- встановленням режиму доступу інших держав до інформаційних ресурсів України;
- використанням національних інформаційних ресурсів на основі рівноправного співробітництва з іншими державами.

Інформаційний суверенітет України, крім цього, має забезпечуватися проведенням цілісної державної програми відповідно до Конституції та чинного законодавства України і норм міжнародного права шляхом реалізації відповідних доктрин, стратегій, концепцій та програм, що стосуються національної інформаційної політики. Головною передумовою існування інформаційного суверенітету є належний стан інформаційної безпеки держави, суспільства та його громадян.

Під ***інформаційною сферою*** на змістовом рівні слід розуміти безпосередньо інформацію та сферу її обігу. Тобто ***безпека інформаційної сфери*** – це стан захищеності інформації та сфер її створення, накопичення, зберігання, оброблення, розповсюдження і використання.

Безпека інформації – захищеність інформації в організації або технічній системі від несанкціонованого доступу (ознайомлення, крадіжки, зміни, знищення).

Держстандартом України прийняте таке 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 обробляють інформацію з обмеженим доступом в недержавних структурах, здійснюється відповідними службами.

Захист інформації – це сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї.

Доктрина інформаційної безпеки України, затверджена Указом Президента України від 25 лютого 2017 року № 47/2017, вводить такі терміни:

стратегічні комунікації – скоординоване і належне використання комунікативних можливостей держави – публічної дипломатії, зв'язків із громадськістю, військових зв'язків, інформаційних та психологічних операцій, заходів, спрямованих на просування цілей держави;

урядові комунікації – комплекс заходів, що передбачають діалог уповноважених представників Кабінету Міністрів України з цільовою аудиторією з метою роз'яснення урядової позиції та/або політики з певних проблемних питань;

кризові комунікації – комплекс заходів, що реалізуються державними органами України у кризовій ситуації і передбачають їх діалог із цільовою аудиторією з питань, що стосуються кризової ситуації;

стратегічний наратив – спеціально підготовлений текст, призначений для вербального викладення у процесі стратегічних комунікацій з метою інформаційного впливу на цільову аудиторію.

Законом України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки" було введено термін **"Інформаційна безпека"**, як стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання, порушення цілісності, конфіденційності та доступності інформації.

Проте, це визначення сформульоване не за суттєвими ознаками і в ньому присутня лише пасивна складова "ступінь захищеності", але відсутня активна складова "інформаційний розвиток" (технічний, інтелектуальний, соціально-політичний, морально-етичний тощо).

До того ж у Законі "Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки", як і в інших законодавчих актах нашої держави, відсутні визначення різновидів інформаційної безпеки. Крім цього, цей закон втратив свою чинність.

Тому пропонуються авторські визначення "інформаційної безпеки", а також "інформаційної безпеки особи, суспільства, держави".

Інформаційна безпека (ІБ) – це стан захищеності життєво важливих інтересів особи, суспільства та держави, при якому досягається інформаційний розвиток (технічний, інтелектуальний, соціально-політичний, морально-етичний тощо), за якого сторонні інформаційні впливи не завдають їм суттєвої шкоди.

Інформаційна безпека особи – це стан захищеності психіки та здоров'я людини від деструктивного інформаційного впливу, який призводить до неадекватного сприйняття нею дійсності та (або) погіршення її фізичного стану.

Необхідний рівень ІБ особи забезпечується:

- рівнем підготовки людини, при якому досягається захищеність і реалізація її життєво важливих інтересів і гармонійний розвиток незалежно від наявності інформаційних загроз;
- здатністю держави створити умови для гармонійного розвитку й задоволення потреб людини в інформації, незалежно від наявності інформаційних загроз;
- гарантуванням розвитку і використання інформаційного середовища в інтересах людини;
- захищеністю від різного роду інформаційних загроз.

Інформаційна безпека суспільства – це можливість безперешкодної реалізації суспільством й окремими його членами своїх конституційних прав, пов'язаних із вільним одержанням, обробленням, створенням і поширенням інформації, а також ступінь їх захисту від деструктивного інформаційного впливу.

Необхідний рівень ІБ суспільства забезпечується сукупністю політичних, економічних, організаційних заходів, спрямованих на попередження, виявлення й нейтралізацію тих обставин, факторів і дій, які можуть завдати збитків чи зашкодити реалізації інформаційних прав, потреб та інтересів країни і її громадян.

Варто відмітити, що ІБ особи та суспільства тісно пов'язані між собою. ІБ суспільства та окремих осіб *залежить від рівня:*

- інтелектуальності, спеціальної теоретичної й практичної підготовки;
- критичного мислення, морального та духовного вдосконалення;
- гармонійного розвитку особистості в суспільстві;
- технічних засобів захисту.

Інформаційна безпека держави – це стан її захищеності та інформаційного розвитку, при якому акції інформаційного впливу, спеціальні інформаційні операції, інформаційні війни, інформаційний тероризм, незаконне зняття інформації за допомогою спеціальних технічних засобів та комп'ютерна злочинність не завдають суттєвої шкоди національним інтересам (Рис.1.1.1).

Необхідний рівень ІБ держави забезпечується створенням умов для гармонійного розвитку інформаційної інфраструктури держави, реалізації конституційних прав і свобод людини в інтересах держави: зміцнення конституційного ладу, суверенітету і територіальної цілісності країни, встановлення політичної і соціальної стабільності, економічного розвитку, безумовного виконання законів та міжнародного співробітництва.

Рис.1.1.1 Структура інформаційної безпеки держави

Акція інформаційного впливу – одноразова дія інформаційно-психологічного та інформаційно-технічного впливу, яка передбачає спланований вплив на свідомість і поведінку людей шляхом поширення упередженої, неповної чи недостовірної інформації та (або) інформаційно-технічну інфраструктуру об'єкта (об'єктів).

Інформаційний тероризм – небезпечні діяння з інформаційного впливу на соціальні групи й окремих осіб, державні органи влади та управління, пов'язані з поширенням інформації, яка містить погрози переслідуванням, розправою, вбивствами, а також викривлення об'єктивної інформації, що спричиняє виникнення кризових ситуацій у державі, нагнітання страху й напруження в суспільстві.

Комп'ютерна злочинність – це відносно масове соціальне явище, яке полягає в суспільно небезпечних діяннях, коли електронно-обчислювальні машини, мережі, системи та представлена в них інформація є знаряддям або предметом злочинних діянь.

Об'єктами інформаційної безпеки можуть бути:

- свідомість (особи, групи осіб, суспільства);
- інформаційно-телекомунікаційна інфраструктура (суб'єкти та засоби створення, поширення інформації й передання даних);
- інформаційні ресурси (інформація конфіденційна, з обмеженим доступом, особиста і така, що є власністю держави).

1.2. Інформаційний вплив та його різновиди

Інформаційний вплив – це організоване цілеспрямоване застосування спеціальних інформаційних засобів і технологій для внесення деструктивних змін у свідомість особистості, соціальних груп чи населення (корекція

поведінки), в інформаційно-технічну інфраструктуру об'єкта впливу та (чи) фізичний стан людини.

Інформаційний вплив варто поділяти на *інформаційно-технічний* та *інформаційно-психологічний*.

Інформаційно-технічний вплив (ІТВ) – це вплив на інформаційно-технічну інфраструктуру об'єкта з метою забезпечення реалізації необхідних змін у її функціонуванні (зупинка роботи, несанкціонований доступ до інформації та її перекручення (спотворення), програмування на певні помилки, зниження швидкості оброблення інформації тощо), а також вплив на фізичний стан людини. ІТВ становить загрозу безпеці інформаційно-технічної інфраструктури й фізичному стану людини.

Безпека інформаційно-технічної інфраструктури – це стан захищеності, який забезпечує її ефективне використання та захист від можливого ІТВ.

Безпека інформаційно-технічної інфраструктури поділяється на безпеку:

- машинно-технічних засобів (автоматизованих систем та мереж);
- програмного забезпечення;
- режиму захисту від несанкціонованого витоку інформації.

Інформаційно-психологічний вплив (ІПсВ) – це вплив на свідомість та підсвідомість особистості й населення з метою внесення змін у їхню поведінку і світогляд. Базовими методами ІПсВ є *переконання й навіювання.*

Переконання звернене до власного критичного сприйняття дійсності об'єктом впливу. Воно має певні алгоритми впливу:

- логіка переконання має бути доступною інтелекту об'єкта впливу;
- переконання варто здійснювати, спираючись на факти, відомі об'єкту;
- переконлива інформація повинна містити узагальнювальні пропозиції;
- переконання має містити логічно несуперечливі конструкти;
- факти, що доносяться до об'єкта впливу, повинні мати відповідне емоційне забарвлення.

Навіювання, навпаки, спрямовується на суб'єктів, які некритично сприймають інформацію. Його особливостями є:

- цілеспрямованість і плановість застосування;
- конкретність визначення об'єкта навіювання (селективний вплив на певні групи населення з урахуванням їхніх основних соціально-психологічних, національних й інших особливостей);
- некритичне сприйняття інформації об'єктом навіювання (навіювання засноване на ефекті сприйняття інформації як інструкції до дії без її логічного аналізу);
- визначеність, конкретність поведінки, що ініціюється (об'єкту необхідно дати інструкцію щодо його конкретних реакцій і вчинків, які відповідають меті впливу).

Навіювання (сугестія) – це процес прихованого впливу на психіку людини, пов'язаний зі зниженням свідомості й критичності при сприйнятті

навіяного змісту, який не вимагає ні розгорнутого особистого аналізу, ні оцінки спонукання до певних дій. Суть навіювання полягає у впливі на відчуття людини, а через них – на її волю й розум.

Навіювання є основним способом маніпулювання свідомістю, прямим вторгненням у психічне життя людей. При цьому маніпулятивний вплив організується так, щоб думка, уявлення, образ безпосередньо входили у сферу свідомості та закріплювалися в ній як дані безперечні й уже доведені. Це стає можливим при підміні активного відношення психіки до предмета комунікації навмисно створеною пасивністю сприйняття, що так властиво релігійним виданням (розсіювання уваги поданням великої кількості інформації, активна форма її подання, штучне перебільшення престижу джерел).

ІПсВ спрямовується на індивідуальну або суспільну свідомість інформаційно-психологічними чи іншими засобами, що зумовлює трансформацію психіки, зміну поглядів, думок, взаємин, ціннісних орієнтацій, мотивів, стереотипів особи з метою вплинути на її діяльність і поведінку. Кінцевою його метою виступає досягнення певної реакції, поведінки (дії або бездіяльності) особистості, яка відповідає цілям ІПсВ.

Процес сприйняття індивідом ІПсВ, спрямованого на емоційну сферу свідомості, специфічний. Загалом, він більше згорнутий, ніж, наприклад, процес сприйняття пропагандистського впливу: в ньому функціонують тільки сприйняття й запам’ятовування, діяльність мислення виражена досить слабко. Інформацію особистість сприймає або не сприймає, сприймає цілком чи частково, але у формуванні певних висновків практично не бере участі. Процес ІПсВ на емоційну сферу свідомості включає довільне сприйняття та запам’ятовування й характеризується дуже зниженим рівнем усвідомлення змісту впливу. Осмислення отриманої інформації відбувається пізніше, при більш високій пізнавальній активності індивіда.

Потужність і ефективність маніпулятивного впливу залежить від наявності певних переваг у маніпулятора над адресатом. Раніше вже наголошувалося на прихованому від адресата характері маніпулятивного впливу, що відразу створює переваги маніпулятору. Є й інші переваги, які дають змогу маніпулятору використовувати специфічні прийоми впливу та підсилюють його ефект.

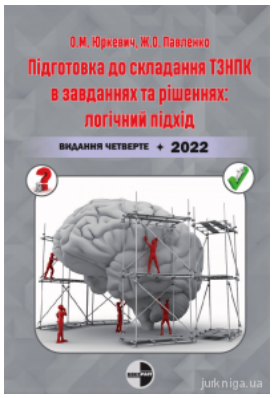
Рівень ефективності ІПсВ залежить від таких умов:

- *змісту матеріалу:* його складності, конкретності, суспільної важливості тощо. Наприклад, за рівних умов чим простіша інформація, тим більше шансів, що дії, на які вона спонукає, можуть виконуватися автоматично, особливо коли не суперечать переконанням об’єкта. Тобто, чим конкретніший заклик до дії, тим вищий ступінь автоматизму реакції на неї;
- *психічного стану*, що характеризується наявністю високого рівня автоматизму відповідної реакції. Страх, пригніченість, апатія сприяють некритичному й підсвідомому сприйняттю впливу. Ступінь автоматизму у відповіді особи пов’язаний із рівнем усвідомленості та критичності сприйняття інформації. Якщо вплив сприймається підсвідомо й некритично, то відповідь аудиторії може бути автоматичною;

Книги, які можуть вас зацікавити

Пропаганда

Кримінальний кодекс України



Підготовка до складання ТЗНПК в завданнях та рішеннях: логічний підхід

Закон України "Про оперативно-розшукову діяльність". Алерта

Перейти до галузі права
Інформаційне право

ЮРКНИГА
від теорії до практики

Перейти на сайт →