МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

Л. В. Перевалова, І. В. Лисенко, А.М. Лисенко, Г. М. Гаряєва

НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ

ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У НАЦІОНАЛЬНОМУ ТА МІЖНАРОДНОМУ СПІВРОБІТНИЦТВІ

Навчально-методичний посібник для студентів денної форми навчання, які навчаються за спеціальністю 035.10

«Філологія (прикладна та комп’ютерна лінгвістика)

Затверджено

редакційно-видавничою радою НТУ «ХПІ»,

протокол № 2 від 28.06.2023 р.

Харків 2023

УДК 004.056+340

Н 83

Р е ц е н з е н т и*:*

*Яковюк І.В.*, доктор юридичних наук, професор кафедри права Європейського Союзу Національного юридичного університету ім. Ярослава Мудрого

*Шаронова Н.В.*, доктор технічних наук, професор, завідувачка кафедри інтелектуальних комп’ютерних систем Національного технічного

університету «Харківський політехнічний інститут»

**Перевалова Л. В. та ін.**

**Н83** Нормативно-правове забезпечення інформаційної безпеки у на- ціональному та міжнародному співробітництві: навч.-метод. посіб. / Л. В. Перевалова, І. В. Лисенко, А.М. Лисенко, Г. М. Гаряєва. – Харків: ФОП Панов А. М., 2023. – 112 с.

**ISBN 978-617-8113-60-5**

Навчально-методичний посібник підготовлено відповідно до навчаль- ного курсу «Нормативно-правове забезпечення інформаційної безпеки у наці- ональному та міжнародному співробітництві». В ньому розглядаються осно- вні законодавчі акти, міжнародні правові документи, які регулюють діяльність органів державної влади у сфері забезпечення інформаційної безпеки. Особ- лива увага приділяється механізмам формування інформаційної безпеки як в Україні, так й у розвинутих країнах світу. Автори розкривають основні форми інформаційного протиборства, визначають завдання інформаційної війни та її моделі, проблеми забезпечення інформаційної безпеки та кібербезпеки, нада- ють характеристику стратегії забезпечення інформаційної безпеки, основним реальним та потенційним загрозам інформаційної безпеки нашої держави

Посібник буде корисним як для студентів, які навчаються за спеціаль- ністю «Філологія (прикладна та комп’ютерна лінгвістика)», так і для виклада- чів.

Бібліогр. 30 назв.

**УДК 004.056+340**

**ISBN 978-617-8113-60-5** © Л. В. Перевалова, І. В. Лисенко,

А. М. Лисенко, Г. М. Гаряєва 2023

# ВСТУП

На сучасному етапі розвитку людської цивілізації для кожної країни світу інформація стає стратегічно важливим ресурсом, від ефективного ви- користання якого залежить безпека держави й перспективи формування та подальшого розвитку демократичного суспільства. Сьогодні інформаційні ресурси активно використовуються в усіх сферах суспільного життя для отримання достовірних даних у різних галузях знань і практичній діяльно- сті.

Одночасно зі зростанням ролі інформації підвищується й важливість її захисту, яка забезпечується шляхом застосування інструментів інформа- ційної безпеки, що набуває особливої актуальності в умовах війни. Захист інформації є надзвичайно важливою складовою національної безпеки дер- жави. Інформаційна безпека є складним, системним, багаторівневим яви- щем, на стан і перспективи розвитку якого мають безпосередній вплив зов- нішні та внутрішні чинники, такі як політична обстановка у світі та внутрі- шньополітична обстановка в державі; наявність потенційних зовнішніх і внутрішніх загроз; стан і рівень інформаційно-комунікаційного розвитку країни.

Забезпечення інформаційної безпеки сприяє забезпеченню досяг- нення успіху при вирішенні завдань у політичній, військово-політичній,

військовій, соціальній, економічній та інших сферах державної діяльності. Інформаційна безпека ставить на меті забезпечення безпеки особистості, держави і суспільства в цілому.

В рамках навчального курсу «Нормативно-правове забезпечення ін- формаційної безпеки у національному та міжнародному співробітництві» студентам надаються знання основних законодавчих актів та міжнародних документів, які забезпечують інформаційну безпеку України та інших країн світу. Визначаються основні поняття інформаційної безпеки держави, зага- льні поняття безпеки інформаційних ресурсів, особливості та основні фо- рми інформаційного протиборства, надається класифікація загроз для інфо- рмаційної безпеки держави, суспільства та особи. Розглянуті способи побу- дови інформаційно-комунікаційних систем і мереж на основі сучасних спо- собів передачі й обробки інформації та способи захисту інформації в інфо- рмаційних системах і мережах. Аналізується політика та система забезпе- чення інформаційної безпеки України. Особлива увага приділяється харак- теристики нормативно-правових актів України та міжнародно-правових до- кументів, які сприяють забезпеченню інформаційної безпеки України.

Таким чином, метою вивчення дисципліни «Нормативно-правове за-

безпечення інформаційної безпеки у національному та міжнародному спів- робітництві» є:

* сприяти засвоєнню правових знань, формування вмінь і навичок за- стосовувати здобуті знання у професійної діяльності;
* формування у майбутніх фахівців розуміння сутності явища інфор- маційна безпека;
* ознайомити їх з основними загрозами інформаційній безпеці та ви- робити уявлення про ефективність інструментів забезпечення інформацій- ної безпеки особистості, держави, суспільства.

У результаті вивчення навчальної дисципліни «Нормативно-правове забезпечення інформаційної безпеки у національному та міжнародному співробітництві» студенти повинні знати та аналізувати:

* міжнародні нормативно-правові документи щодо забезпечення ін- формаційної безпеки;
* чинне законодавство України в сфері інформаційної безпеки. Уміти:
* орієнтуватись у системі джерел законодавства України та міжнаро- дно-правового регулювання;
* аналізувати, узагальнювати та застосовувати норми права України у практичній діяльності, роз’яснювати їх зміст;
* складати та оформлювати документи юридичного характеру;
* підбирати літературу з теми заняття, складати конспекти і тези ви- ступів, знаходити правову інформацію;
* керуватись у практичній діяльності та поведінці правовими знан- нями і переконаннями.

Структура навчальної дисципліни «Нормативно-правове забезпе- чення інформаційної безпеки у національному та міжнародному співробіт- ництві» визначається відповідно до робочого навчального плану.

Видання може бути корисним викладачам і студентам закладів вищої освіти при викладанні та вивченні дисципліни «Нормативно-правове забез- печення інформаційної безпеки у національному та міжнародному співро- бітництві».

**ЗМІСТ ТА СТРУКТУРА**

**навчальної дисципліни**

**«Нормативно-правове забезпечення інформаційної безпеки у національному та міжнародному співробітництві»**

**Тема 1. Поняття інформаційної безпеки держави, суспільства та особи**

Інформаційна безпека (поняття і визначення). Правове забезпечення інформації та інформаційної безпеки. Інформація та види інформації. Ін- формаційні відносини. Інформаційний суверенітет. Інформаційна безпека, її сутність. Види інформаційної безпеки. Інтереси особи, суспільства та держави в інформаційній сфері. Інформаційна сфера та інтереси особи, держави та суспільства.

# Тема 2. Інформаційна безпека та кібербезпека

Кіберпростір: поняття та склад. Проблеми забезпечення інформацій- ної та кібербезпеки. Стратегії забезпечення національної безпеки держави. Закон України «Про національну безпеку». Кіберпростір та його співвідно- шення з інформаційною безпекою. Кібербезпека склад та сутність. Страте- гія забезпечення національної безпеки. Фундаментальні національні інте- реси України.

# Тема 3. Загрози для інформаційної безпеки держави, суспільства, людини

Інформаційна безпека держави та життєво важливі інтереси особис- тості, суспільства та держави. Об’єкти та суб’єкти інформаційної безпеки. Концепція інформаційної безпеки. Поняття загроз інформаційній безпеці. Види загроз інформаційній безпеці та їх джерела. Фактори загроз інформа- ційній безпеці. Класифікація видів загроз інформаційній безпеці України. Внутрішні та зовнішні джерела загроз інформаційній безпеці. України. Принципи забезпечення інформаційної безпеки. Система забезпечення ін- формаційної безпеки держави. Основні форми і способи забезпечення ін- формаційної безпеки держави.

# Тема 4. Принципи, форми та методи забезпечення інформаційної безпеки держави

Основні та специфічні принципи забезпечення інформаційної безпеки держави. Основні форми забезпечення інформаційної безпеки держави: інформаційний патронат, інформаційна кооперація, інфор- маційне протиборство. Методи забезпечення інформаційної безпеки.

# Тема 5. Інформаційне протиборство між країнами. Інформаційна війна

Інформаційне протиборство та його види. Об’єкти впливу інформа- ційного протиборства. Концепція інформаційного протиборства. Ступені інформаційного протиборства. Основні форми інформаційного протибор- ства. Інформаційна війна та її завдання. Особливості інформаційної війни. Концепція інформаційної війни. Органи інформаційної війни. Основні фо- рми та рівні інформаційної війни. Засоби інформаційної війни. Інформа- ційні переваги у сфері інформаційного протиборства.

# Тема 6. Інформаційна зброя в інформаційні війні

Інформаційна зброя та сфера її застосування. Основні об’єкти засто- сування інформаційної зброї. Види інформаційної зброї. Інформаційна зброя воєнного та невоєнного застосування. Особливості застосування ін- формаційної зброї. Засоби ураження комп’ютерних інформаційних систем. Програми з потенційно небезпечними наслідками.

# Тема 7. Основи теорії інформаційної боротьби

Поняття теорії інформаційної боротьби та її мета. Зміст теорії інфор- маційної боротьби. Загальні основи теорії інформаційної боротьби та її структура. Теорія сил та засобів ураження інформації. Теорія захисту ін- формації. Фактори впливу: економічний, воєнний та інформаційний. За- кони та закономірності інформаційної боротьби. Принципи інформаційної боротьби. Заходи інформаційної боротьби: інформаційне забезпечення, ін- формаційний захист, інформаційна протидія. Способи та форми інформа- ційної боротьби.

# Тема 8. Основи безпеки інформаційних ресурсів

Поняття та загальні властивості інформації. Одержувачі інформації. Поняття загроз. Загрози безпеки інформації та інформаційних ресурсів. Джерела загроз безпеці інформації. Класифікація вразливостей безпеки. Моделі порушень інформаційних ресурсів. Порушники, цілі та мета їх дій.

# Тема 9. Забезпечення безпеки інформації та інформаційних ресурсів

Напрями захисту інформації. Правовий захист: конституційне законо- давство, загальні та спеціальні закони, підзаконні акти. Спеціальне зако- нодавство та його значення для забезпечення інформаційної безпеки. Стра- хове забезпечення та його мета. Ліцензія як засіб забезпечення безпеки ін- формації. Комерційна таємниця. Забезпечення захисту та безпеки інформа- ції на підприємстві. Особливості захисту комп’ютерних систем. Служба

захисту інформації. Організаційний захист та його заходи. Інженерно-тех- нічний захист та його засоби.

# Тема 10. Захист інформаційних систем

Джерела інформації. Люди як джерела інформації. Конфіденційна ін- формація: поняття та джерела. Інформаційна система як об’єкт захисту. Структура інформаційної системи. Рівні захисту інформаційних систем: локальний, мережевий, на рівні користувачів. Основні принципи захисту інформаційних систем. Інформаційні ресурси та їх властивості. Корпора- тивні інформаційні системи (КІС).

# Тема 11. Інформаційна безпека України

Національна безпека та її структура. Принципи забезпечення націона- льної безпеки. Інформаційна безпека та її місце в національній безпеки Ук- раїни. Сутність інформаційної безпеки. Мета та завдання забезпечення ін- формаційної безпеки України. Основні реальні та потенційні загрози ін- формаційній безпеці України. Загрози інформаційної безпеки: зовнішні та внутрішні загрози. Стан та перспективи розвитку інформаційної безпеки. Система та політика забезпечення інформаційної безпеки.

# Розділ 1. ПОНЯТТЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ, СУСПІЛЬСТВА ТА ОСОБИ

* 1. Інформаційна безпека (поняття і визначення).
  2. Інформаційна безпека, її сутність.
  3. Інтереси особи, суспільства та держави в інформаційній сфері.

# Інформаційна безпека (поняття і визначення)

З кожним роком інформаційні системи ускладняються, інформаційна безпека й політика набувають усе більш глобальний характер, виходячи на перший план. У XXI ст. виникло багато проблем, пов’язаних з інформацій- ною безпекою. Процеси глобалізації дуже гостро дали про себе знати й, крім позитивних елементів, виникли серйозні негативні явища, до яких сві- това спільнота виявилася неготовою. Тому інформаційна безпека у сучас- ному суспільстві відіграє величезну роль, оскільки суспільство вступає в епоху інформаційних війн, при яких цінність інформації зростає в багато разів. При цьому інформація – це не тільки товар, а й інструмент маніпуля- ції суспільством, думкою громадян, створенню конфліктів. Отже, як лю- дина потребує захисту від інформації, так і інформація потребує захисту від людини. Особливо зростає роль інформаційної безпеки у сфері високих те- хнологій, бо саме цифрова інформація стає одночасно і сировиною, і про- дуктом, яку виробляють, обробляють, продають та, на жаль, частіше

крадуть. Здебільшого нині визначають інформаційну безпеку через комп’ютерну безпеку. Дійсно, величезні обсяги інформації, що містяться на електронних носіях дедалі відіграють усе більшу роль у сучасному світі. Але ця інформація дуже вразлива, що зумовлене її великими обсягами, ба- гатозначністю, можливістю «інформаційних диверсій», анонімністю дос- тупу. Захист інформації, що розміщена в середовищі комп’ютера – це наба- гато складніше, ніж збереження таємниці звичайного поштового листу- вання. Враховуючи це, можна зробити висновок, що проблеми інформацій- ної безпеки надзвичайно актуальні й потребують поглибленого вивчення.

Нормативно-правовий підхід до розуміння інформаційної безпеки представлений в законах та інших нормативних актах України, які регулю- ють відносини у сфері інформаційної безпеки.

Базові засади інформаційної безпеки нашої держави закладено у стат- тях 17, 19, 31, 32, 34, 50, 57 та 64 Конституції України.

Передусім варто вказати, що зміст інформаційної безпеки передбачає широкий комплекс компонентних частин та на сьогодні не має чіткого юри- дичного визначення у законодавстві. В Законі України «Про Концепцію На- ціональної програми інформатизації» від 4 лютого 1998 р. офіційно визнано інформаційну безпеку як невід’ємну частину політичної, економічної, обо- ронної та інших складових національної безпеки. Законом України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007- 2015 роки» було вперше законодавчо закріплено поняття інформаційна без- пека як стан захищеності життєво важливих інтересів людини, суспільства і держави. Також інформаційна безпека розкривається у Доктрині інфор- маційної безпеки України від 25 лютого 2017 р. [12] як невід’ємна складова кожної зі сфер національної безпеки і як важлива самостійна сфера забез- печення національної безпеки. Саме ж поняття інформаційної безпеки за- стосовується у Законі України «Про національну безпеку України» від 21 червня 2018 р., але жодним чином не визначено, що саме мається на увазі під інформаційною безпекою та забезпеченням інформаційної безпеки.

Дослідження такого складного явища, як інформаційна безпека, може

бути успішним лише за умови наявності розробленого понятійного апарату. Головною складовою цього апарату є система понять, завдяки яким розк- риваються сутнісні моменти досліджуваного явища.

Розглянемо основні поняття, визначення і терміни.

# Інформація:

1. документовані або публічно проголошені відомості про події та явища, що відбуваються в суспільстві, державі та навколишньому природному се- редовищі;
2. відомості про осіб, предмети, технології, засоби, ресурси, події та явища, що відбуваються в усіх сферах діяльності держави, життя суспільства, та навколишньому природному середовищі, незалежно від форми їх

представлення, будь-які знання про предмети, факти, поняття і т. ін. про- блемної сфери, якими обмінюються користувачі системи оброблення да- них.

Основним Законом, регулюючим питання інформації в Україні є Закон

«Про інформацію», який регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інфор- мації.

Закон України «Про інформацію» закріплює право громадян України на інформацію, закладає правові основи інформаційної діяльності. Закон стверджує інформаційний суверенітет України і визначає правові форми міжнародного співробітництва в галузі інформації, встановлює загальні правові основи одержання, використання, поширення та зберігання інфор- мації, закріплює право особи на інформацію в усіх сферах суспільного і державного життя України, а також систему інформації, її джерела, визна- чає статус учасників інформаційних відносин, регулює доступ до інформа- ції та забезпечує її охорону, захищає особу та суспільство від неправдивої інформації.

Відповідно до цього Закону кожна людина має право на інформацію,

що передбачає можливість вільного одержання, використання, поширення, зберігання та захисту інформації, необхідної для реалізації своїх прав, сво- бод і законних інтересів.

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

Держава приділяє багато уваги охороні права на інформацію. Так ст.7 встановлює:

* 1. Право на інформацію охороняється законом. Держава гарантує всім суб'єктам інформаційних відносин рівні права і можливості доступу до ін- формації.
  2. Ніхто не може обмежувати права особи у виборі форм і джерел оде- ржання інформації, за винятком випадків, передбачених законом.

Суб’єкт інформаційних відносин може вимагати усунення будь-яких порушень його права на інформацію.

* 1. Забороняється вилучення і знищення друкованих видань, експонатів, інформаційних банків, документів з архівних, бібліотечних, музейних фон- дів, крім встановлених законом випадків або на підставі рішення суду.
  2. Право на інформацію, створену в процесі діяльності фізичної чи юри- дичної особи, суб'єкта владних повноважень або за рахунок фізичної чи юридичної особи, Державного бюджету України, місцевого бюджету, охо- роняється в порядку, визначеному законом.

Розділ II Закону присвячено **інформаційній діяльності**, під якою розу- міється сукупність дій, спрямованих на задоволення інформаційних потреб громадян, юридичних осіб і держави.

Визначено основні напрями та види інформаційної діяльності – одер- жання, використання, поширення та зберігання інформації.

У розділі III Закону наведені галузі, види, джерела інформації та режим доступу до неї.

Основними галузями інформації визначені: політична, економічна, ду- ховна, науково-технічна, соціальна, екологічна, міжнародна.

Основними видами інформації є: статистична; адміністративна інфор- мація (дані); масова інформація; інформація про діяльність державних ор- ганів влади та органів місцевого і регіонального самоврядування; правова інформація; інформація про особу; інформація довідково-енциклопедич- ного характеру; соціологічна інформація.

За режимом доступу інформація поділяється на **відкриту інформацію та інформацію з обмеженим доступом**. Держава здійснює контроль за ре- жимом доступу до інформації. Державний контроль за додержанням вста- новленого режиму здійснюється спеціальними органами, які визначають Верховна Рада України і Кабінет Міністрів України.

**Доступ до відкритої інформації** забезпечується шляхом:

систематичної публікації її в офіційних друкованих виданнях (бюлете- нях, збірниках);

поширення її засобами масової комунікації;

безпосереднього її надання заінтересованим громадянам, державним органам та юридичним особам.

Обмеження права на одержання відкритої інформації забороняється за- коном.

**Інформація з обмеженим доступом** за своїм правовим режимом поді- ляється на ***конфіденційну і таємну***.

**Конфіденційна інформація** – це відомості, які знаходяться у воло- дінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов. Громадяни, юридичні особи, які володіють інформацією професійного, ді- лового, виробничого, банківського, комерційного та іншого характеру, оде- ржаною на власні кошти, або такою, яка є предметом їх професійного, ді- лового, виробничого, банківського, комерційного та іншого інтересу і не порушує передбаченої законом таємниці, самостійно визначають режим до- ступу до неї, включаючи належність її до категорії конфіденційної, та вста- новлюють для неї систему (способи) захисту. Виняток становить інформа- ція комерційного та банківського характеру, а також інформація, правовий режим якої встановлено Верховною Радою України за поданням Кабінету Міністрів України (з питань статистики, екології, банківських операцій,

податків тощо), та інформація, приховування якої являє загрозу життю і здоров’ю людей.

**До таємної інформації** належить інформація, що містить відомості, які становлять *державну та іншу передбачену законом таємницю (військова, комерційна, банківська, професійна, лікарська, адвокатська таємниця тощо*), розголошення якої завдає шкоди особі, суспільству і державі.

**Інформація, що становить військову таємницю** – це вид таємної ін- формації, який охоплює відомості в сфері оборони, державної безпеки та охорони правопорядку, розголошення якої може завдати шкоди інтересам державної безпеки, бойової готовності Збройних Сил України та інших вій- ськових формувань, їхніх окремих підрозділів, якщо ці відомості не нале- жать до державної таємниці згідно з законодавством України.

**Інформація, що становить комерційну таємницю** – це відомості на- уково-технічного, технічного, виробничого, фінансово-економічного або іншого характеру (в тому числі секрети виробництва – так зване ноу-хау), що мають дійсну або потенційну комерційну цінність у силу її невідомості третім особам, до якої немає вільного доступу на законній підставі й у від- ношенні якої власником такої інформації введений режим комерційної та- ємниці.

Порядок обігу таємної інформації, що не становить державної таємниці, та її захист визначається відповідними державними органами за умов доде- ржання вимог Закону України «Про інформацію».

**Інформація з обмеженим досту**пом може бути поширена без згоди її власника, якщо вона є суспільно значимою, тобто якщо вона є предметом громадського інтересу і якщо право громадськості знати цю інформацію переважає право її власника на її захист.

Особливим видом таємної інформації є **державна таємниця**. Вона охо- плює відомості у сфері оборони, економіки, зовнішніх відносин, державної безпеки і органів правопорядку, розголошення яких може завдати шкоди життєво важливим інтересам України і які визначені у порядку, встановле- ному законом, державною таємницею та підлягає охороні з боку держави. Віднесення інформації до категорії відомостей, що становлять державну та- ємницю, порядок її захисту та обігу, доступ до неї визначається Законом України «Про державну таємницю», яким закладено правову основу ство- рення та функціонування системи охорони державної таємниці в Україні.

Ступень таємності інформації визначається наданим грифом таємності

«Таємно», «Цілком таємно» та «Особливої важливості». Гриф надається на певний термін, який залежить від ступеня таємності: для грифу «таємно» – 5 років, «цілком таємно» – 10 років, «особливої важливості» – 30 років.

У розділі IV Закону визначені учасники інформаційних відноси, їх права та обов’язки. Основними учасниками цих відносин є: автори, спожи- вачі, поширювачі, зберігачі (охоронці) інформації. Кожний учасник

інформаційних відносин для забезпечення його прав, свобод і законних ін- тересів має право на одержання інформації про: діяльність органів держав- ної влади; діяльність народних депутатів; діяльність органів місцевого і ре- гіонального самоврядування та місцевої адміністрації; те, що стосується його особисто.

Розділ V Закону присвячений охороні інформації, відповідальності за порушення законодавства про інформацію. Держава гарантує всім учасни- кам інформаційних відносин рівні права і можливості доступу до інформа- ції. Стаття 45-1 забороняє цензуру та втручання в професійну діяльність жу- рналістів і засобів масової інформації з боку органів державної влади або органів місцевого самоврядування, їх посадових осіб. Інформація не може бути використана для закликів до повалення конституційного ладу, пору- шення територіальної цілісності України, пропаганди війни, насильства, жорстокості, розпалювання расової, національної, релігійної ворожнечі, посягання на права і свободи людини. Не підлягають розголошенню відо- мості, що стосуються лікарської таємниці, грошових вкладів, прибутків від підприємницької діяльності, усиновлення (удочеріння), листування, теле- фонних розмов і телеграфних повідомлень, крім випадків, передбачених за- коном. Порушення законодавства України про інформацію тягне за собою дисциплінарну, цивільно-правову, адміністративну або кримінальну відпо- відальність згідно з законодавством України.

Розділ VI Закону присвячено міжнародній інформаційній діяльності,

співробітництві з іншими державами, зарубіжними і міжнародними органі- заціями в галузі інформації. Міжнародне співробітництво в галузі інформа- ції з питань, що становлять взаємний інтерес, здійснюється на основі між- народних договорів, укладених Україною та юридичними особами, які зай- маються інформаційною діяльністю.

Відносини, які виникають у всіх сферах життя й діяльності держави, суспільства і людини при одержанні, використанні, поширенні та збері- ганні інформації є **інформаційними відносинами**. Як й будь які суспільні відносини вони мають власні структуру: суб’єктів, як приймають участь у цих відносинах та об’єкт, з приводу якого вони вступають у інформаційні відносини.

**Суб’єктами інформаційних відносин** є:

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

**Об’єктом інформаційних відносин** є інформація. Об’єктами інформа- ційної безпеки можуть бути: інформаційні системи різного масштабу й різ- ного призначення. До соціальних об’єктів інформаційної безпеки звичайно відносять особу, суспільство, державу.

Здатність держави контролювати й регулювати потоки інформації поза межами своєї держави складає **інформаційний суверенітет**, метою якого є дотримання законів України, прав і свобод громадян, забезпечення націо- нальної безпеки держави.

Важливим поняттям для усвідомлення інформаційної безпеки є визна- чення інформаційного простору.

# Інформаційний простір (національний):

1. інформаційне середовище, в якому здійснюються інформаційні процеси та інформаційні відносини щодо створення, збирання, відображення, реєст- рації, накопичення, збереження, захисту та поширення інформації, інфор- маційних продуктів і ресурсів, на яке поширюється юрисдикція держави;
2. сукупність національних інформаційних ресурсів та інформаційної ін- фраструктури, які дозволяють на основі єдиних принципів і загальних пра- вил забезпечувати інформаційну взаємодію громадян, суспільства і дер- жави з їх рівним правом доступу до відкритих інформаційних ресурсів та максимально повним задоволенням інформаційних потреб суб’єктів дер- жави на всій її території з додержанням балансу інтересів на входження у світовий інформаційний простір і забезпечення інформаційної безпеки від- повідно до Конституції України та міжнародних правових норм.

# Інформаційна безпека, її сутність

***Інформаційна безпека*** – захищеність (стан захищеності) основних ін- тересів особи, суспільства і держави у сфері інформації, включаючи інфор- маційну й телекомунікаційну інфраструктуру і власне інформацію та її па- раметри, такі як повнота, об’єктивність, доступність і конфіденційність. Ін- формаційна безпека є складовою національної безпеки. Але особливістю інформаційної безпеки є те, що вона, як невід’ємна частина, входить до ін- ших складових національної безпеки: економічної, воєнної, політичної без- пеки тощо.

Поняття інформаційної безпеки держави, суспільства та особи, зале- жно від його використання, розглядається в декількох ракурсах. У найзага- льнішому випадку інформаційна безпека – це стан захищеності інформа- ційного середовища суспільства, який забезпечує його формування, вико- ристання і розвиток в інтересах громадян, організацій, держави.

Більш розгорнуте формулювання інформаційної безпеки – це стан за- хищеності потреб в інформації особи, суспільства й держави, за якого за- безпечується їхнє існування та прогресивний розвиток незалежно від наяв- ності внутрішніх і зовнішніх інформаційних загроз.

Треба відзначити, що задоволення потреб в інформації приводить до оволодіння відомостями про навколишній світ та процеси, що протікають у ньому, тобто інформованості особи, суспільства та держави. Стан інфор- мованості визначає ступінь адекватності сприйняття суб’єктами

навколишньої дійсності і, як наслідок, обґрунтованість рішень та дій, що приймаються.

Дослідження сутності інформаційної безпеки має враховувати той факт, що сутність є внутрішнім змістом предмета, який виражається у стій- кій єдності всіх різноманітних і суперечливих формах буття.

Базовою характеристикою інформаційної безпеки слід вважати імові- рність появи загрози підвищеного ризику реалізації загрози або небезпеки для індивіда, суспільства та держави.

Критерієм ефективності забезпечення інформаційної безпеки є висо- кий рівень безпеки при мінімумі відповідних витрат.

Отже, можна говорити про структуру поняття інформаційної безпеки. **Основним її елементом** є життєво важливі інтереси соціальної системи, які співвідносяться із зовнішніми чинниками у вигляді інтересів наднаціональ- них або інших національно-державних структур у межах міжнародного співтовариства. **Зсередини національно-державного утворення** його життєво важливі інтереси перебувають у взаємодії з інтересами елементів, які складають це утворення. У ролі останніх виступають соціальні групи, еліта, організації, партії, релігійні та етнічні утворення, рухи тощо. Сукуп- ність внутрішніх і зовнішніх інформаційних загроз створюють передумови для порушення безпечного функціонування системи державного управ- ління.

Вагомість інформаційно-комунікаційних процесів у сучасному світі

дає підстави розглядати забезпечення інформаційної безпеки як одне з гло- бальних і пріоритетних завдань органів державного управління, вирішенню якого мають бути підпорядковані політична, економічна, воєнна, культурна та інші види діяльності системи державного управління.

В інформаційному праві інформаційна безпека – це одна зі сторін ро- згляду інформаційних відносин у межах інформаційного законодавства з позицій захисту життєво важливих інтересів особи, суспільства, держави та акцентування уваги на загрозах цим інтересам і на механізмах усунення або запобігання таким загрозам правовими методами.

Таким чином, визначаючи поняття інформаційної безпеки, можна ви- окремити декілька підходів окреслення сутності цього феномену, а саме ро- зуміння інформаційної безпеки як:

1. Стану захищеності інформаційного простору.
2. Процесу управління загрозами та небезпеками, що забезпечує інфо- рмаційний суверенітет держави.
3. Стану захищеності національних інтересів держави в інформацій- ному середовищі.
4. Захищеності встановлених законом правил, за якими відбуваються інформаційні процеси в державі.
5. До суспільних відносин, пов’язаних із захистом життєво важливих інтересів людини і громадянина, суспільства та держави від реальних та по- тенційних загроз в інформаційному просторі.
6. Важливої функції держави.
7. Невід’ємної частини політичної, економічної, оборонної та інших складових національної безпеки.

Види інформаційної безпеки:

- особи;

* суспільства;
* держави.

**Інформаційна безпека особи** – це стан захищеності психіки та здо- ров’я людини від деструктивного інформаційного впливу, який призводить до неадекватного сприйняття нею дійсності та (або) погіршення її фізич- ного стану.

**Інформаційна безпека суспільства** – можливість безперешкодної реалізації суспільством та окремими його членами своїх конституційних прав, пов’язаних із можливістю вільного одержання, створення й поши- рення інформації, а також ступінь їхнього захисту від деструктивного інфо- рмаційного впливу. Необхідний рівень інформаційної безпеки забезпечу- ється сукупністю політичних, економічних, організаційних заходів, спря- мованих на попередження, виявлення й нейтралізацію тих обставин, фак- торів і дій, які можуть завдати збитків чи зашкодити реалізації інформацій- них прав, потреб та інтересів країни та її громадян.

Слід зазначити, що інформаційна безпека особи та суспільства між собою тісно пов’язані. Інформаційна безпека суспільства та його окремих осіб залежить від рівня:

- інтелектуальності, спеціальної теоретичної й практичної підготовки;

* критичного мислення, морального та духовного вдосконалення;
* гармонійного розвитку особи в суспільстві;
* технічних засобів захисту.

**Інформаційна безпека де**р**жави** – це стан її захищеності, при якій спеціальні інформаційні операції, акти зовнішньої інформаційної агресії, інформаційний тероризм, незаконне зняття інформації за допомогою спеці- альних технічних засобів, комп’ютерні злочини та інший деструктивний ін- формаційний вплив не завдає суттєвої шкоди національним інтересам.

* 1. **Інтереси особи, суспільства та держави в інформаційній сфері Інформаційна сфера** – це сфера діяльності суб’єктів, пов’язана із

створенням, перетворенням і споживанням інформації.

Інформаційна сфера умовно поділяється на *три основні предметні ча- стини:*

* + - створення і поширення вихідної та похідної інформації;
* формування інформаційних ресурсів, підготовки інформаційних продуктів,
* надання інформаційних послуг; споживання інформації;
* та дві забезпечувальні предметні частини:
  + - створення і застосування інформаційних систем, інформаційних те- хнологій і
* засобів їхнього забезпечення; створення й застосування засобів і механізмів інформаційної безпеки.

В чому ж знаходять свій прояв інтереси учасників інформаційних ві- дносин?

# Інтереси особи в інформаційній сфері полягають:

* + - у реалізації конституційних прав людини та громадянина на доступ до інформації, на використання інформації в інтересах здійснення не забо- роненої законом діяльності, фізичного, духовного та інтелектуального роз- витку;
    - у захисті інформації, що забезпечує особисту безпеку.

# Інтереси суспільства в інформаційній сфері полягають:

* + - у забезпеченні інтересів особи в цій сфері;
* у зміцненні демократії;
* у створенні правової соціальної держави;
* у досягненні та підтриманні суспільного спокою;
* у духовному відновленні держави.

**Інтереси держави в інформаційній сфері** полягають у створенні умов:

* + - для гармонійного розвитку державної інформаційної інфраструк-

тури;

* для реалізації конституційних прав і свобод людини та громадянина

в галузі одержання інформації та користування нею з метою забезпечення непорушності конституційного ладу, суверенітету та територіальної ціліс- ності держави, політичної, економічної та соціальної стабільності, у безу- мовному забезпеченні законності та правопорядку, розвитку рівноправного та взаємовигідного міжнародного співробітництва.

# Питання для самоконтролю

* 1. Які основні підходи до визначення поняття «інформаційна без- пека» Ви знаєте?
  2. Визначить основні ознаки інформаційної безпеки.
  3. У чому полягають інтереси особи, суспільства та держави в інфор- маційній сфері?
  4. Надайте характеристику об’єктам та суб’єктам інформаційної без- пеки.
  5. Розкрийте види інформаційної безпеки.
  6. Що таке інформація?
  7. Що таке джерело інформації?
  8. Які існують носії інформації?
  9. Що розуміють під інформаційними ресурсами?
  10. Що таке загроза інформаційній безпеці?

# Розділ 2. ІНФОРМАЦІЙНА БЕЗПЕКА ТА КІБЕРБЕЗПЕКА

* 1. Кіберпростір: поняття та склад.
  2. Проблеми забезпечення інформаційної та кібербезпеки.
  3. Стратегії забезпечення національної безпеки держави. Закон України

«Про національну безпеку».

# Кіберпростір: поняття та склад

Поступове й доволі умовне поєднання віртуального і реального прос- торів за допомогою ІТ-систем і мережних технологій різного функціональ- ного призначення, які в процесах обробки, передавання та зберігання інфо- рмації використовують електромагнітний спектр і діють як єдине ціле, а та- кож відповідного програмного забезпечення призвело, зрештою, до форму- вання кіберпростору – високорозвиненої моделі об’єктивної реальності, в якій відомості щодо осіб, предметів, фактів, подій, явищ і процесів:

* подаються в деякому математичному, символьному (як сигнали, знаки, звуки, рухомі або нерухомі зображення) або в будь-якому іншому вигляді;
* розміщуються в пам’яті будь-якого фізичного пристрою, спеціально при- значеного для зберігання, обробки й передавання інформації;
* перебувають у постійному русі по сукупності ІТ- систем і мереж.

Уперше термін «кіберпростір» було використано в *Конвенції про зло- чинність у сфері комп’ютерної інформації від 23 листопада 2001 року*. Сфера його дії на той час перебувала під впливом загальних механізмів пра- вового регулювання суспільних відносин, обмежуючись специфічними об’єктами й інтересами суб’єктів правовідносин, а також комп’ютерними мережами, за допомогою яких можна брати участь у відповідних правовід- носинах.

Нині кіберпростір має чимало визначень. Серед інших варто також відзначити й такі визначення поняття кіберпростір:

поліморфний віртуальний простір, що генерує інформаційна система як у формі складних світів, так і у простих реалізаціях (типу електронної пошти, глобальної навігації тощо);

комунікаційне середовище, утворене системою зв’язків між об’єктами кіберінфраструктури – комп’ютерами, комп’ютерними мере- жами, програмним забезпеченням та інформаційними ресурсами, викорис- товуване для забезпечення певних інформаційних потреб;

штучне електронне середовище існування інформаційних об’єктів у цифровій формі, утворене в результаті функціонування кібернетичних комп’ютерних систем управління й обробки інформації, що забезпечує ко- ристувачам доступ до обчислювальних та інформаційних ресурсів систем, вироблення електронних інформаційних продуктів, а також обмін елект- ронними повідомленнями, даючи змогу із застосуванням електронних ін- формаційних образів у режимі реального часу вступати у відносини (взає- модіяти) щодо спільного використання обчислювальних та інформаційних ресурсів системи (надання інформаційних послуг, ведення електронної ко- мерції тощо);

простір, сформований інформаційно-комунікаційними системами, в якому відбуваються процеси перетворення (створення, зберігання, об- міну, обробки та знищення) інформації, поданої у вигляді електронних комп’ютерних даних;

об’єкти інформаційної інфраструктури, що керуються інформацій- ними (автоматизованими) системами управління та інформації, що в них циркулює;

середовище, утворене організованою сукупністю інформаційних про- цесів на основі взаємопоєднаних за єдиними принципами та правилами ін- формаційних, телекомунікаційних та інформаційно-телекомунікаційних систем.

Найбільш відмітними ознаками кіберпростору як субстанції, ство- ренню якої сприяли передусім такі чинники: зміна характеру діяльності лю- дини з ухвалення рішень; упровадження електронно-цифрових форм ство- рення, обробки, зберігання та переміщення інформації, перехід від паперо- вого діловодства до електронного тощо; абсолютна більшість фахівців вва- жає його неперевершені можливості зі створення незліченних зв’язків між окремими індивідами і соціальними групами та з надання різнопланових інформаційних послуг.

З урахуванням характерних особливостей кіберпростору як сфери вчинення заздалегідь спланованих деструктивних дій на кшталт проник- нення в ІТС один одного, блокування або виведення з ладу найбільш ураз- ливих елементів цих систем, дезорганізації оборонних автоматизованих си- стем управління протилежної сторони, систем управління її транспортом і енергетикою, економікою й фінансовою системою тощо (поряд із назем- ною, морською й повітряно-космічною сферами) і своєрідної сполучної ланки між такими поняттями, як Інтернет і кібернетика, усе це, у свою чергу, дає змогу:

виокремити в цьому просторі систему певних відношень між суб’єктами та об’єктами інформаційної й кібернетичної інфраструктури;

охарактеризувати злочини, втручання і загрози, пов’язані з особливо- стями існування та передавання інформації;

розглядати кіберпростір із позицій власне віртуального і реального (електронного, комунікаційного, кібернетичного, інформаційного, особли- вого психологічного) тлумачення як додатковий вимір бойового простору, розрізняючи при цьому фізичний (інфраструктура, кабелі та роутери), се- мантичний (дані) і синтаксичний (протоколи передавання даних) рівні тощо.

# Проблеми забезпечення інформаційної та кібербезпеки

Сучасний стан справ зумовлює небачені досі глибинні зміни у став- ленні більшості держав світу до безпеки власного інформаційного та кібе- рпростору, а отже, і до посиленого захисту інформації, засобів її обробки та кіберсередовища, в якому ця інформація циркулює, тобто до вжиття заходів із забезпечення інформаційної та кібербезпеки.

Таким чином, якщо **кібербезпека** – це система збору даних; органи та канали управління; канали інтерактивної взаємодії, то **інформаційна без- пека** – це інформаційні потоки; бази даних; персонал.

При цьому інформаційну безпеку в найзагальнішому розумінні мо- жна визначити як такий стан захищеності інформаційного простору дер- жави, за якого неможливо завдати збитку властивостям об’єкта безпеки, що стосуються інформації та інформаційної інфраструктури, і який гарантує безперешкодне використання й розвиток національної інфосфери в інтере- сах оборони.

Спектр інтересів ІБ щодо інформації, інформаційних систем та інфо- рмаційних технологій як об’єктів безпеки можна поділити на такі основні категорії: доступність – можливість за прийнятний час отримати певну ін- формаційну послугу; цілісність – актуальність і несуперечливість інформа- ції, її захищеність від руйнування та несанкціонованого змінювання; кон- фіденційність – захищеність від несанкціонованого ознайомлення.

Кібербезпеку можна визначити як стан захищеності кіберпростору держави загалом або окремих об’єктів її інфраструктури від ризику сторон- нього кібервпливу, за якого забезпечується їхній сталий розвиток, а також своєчасне виявлення, запобігання й нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним і/або національним інтересам.

Складовими кібербезпеки є: кібернетичні впливи, розвідка інформа- ційно-телекомуніційних систем протиборчих сторін, захист власної інфор- маційної системи.

Головні проблеми забезпечення кібернетичної безпеки постають із та- ких причин: відсутності чіткого усвідомлення ролі та значення кібербезпе- кової складової  в системі забезпечення національної безпеки держави; дефініційної, термінологічної та нормативно-правової неврегульованості у сфері кібербезпеки; залежності держави від програмних і технічних

продуктів іноземного виробництва; відсутності належної координації діяльності відповідних відомств, а отже, і  неузгодженості дій зі створення окремих елементів системи кібербезпеки; дефіциту щодо методичного за- безпечення та кадрового наповнення  відповідних структурних підрозді- лів.

Комплексну сутність кібербезпеки за таких умов складають:

|  |  |  |
| --- | --- | --- |
| І. Аспекти: | ІІ Сфери | ІІІ Рівні |
| Соціальні Технічні  (біологічний) Інформаційні Комунікаційні | Зовнішньополітична Внутрішньополітична Воєнна, економічна Соціальна, екологічна Науково-творча | Нормативно-правовий Соціальний Інфокомунікаційний Соціотехнічний Методичний |

# Стратегії забезпечення національної безпеки держави. Закон України «Про національну безпеку»

Протягом останніх років Україна, як і більшість країн світу, робить певні кроки в розбудові інформаційного суспільства, забезпечення інфор- маційної й кібербезпеки, а також у боротьбі з кіберзлочинністю. Нормати- вно-правову базу в цих сферах діяльності становлять такі документи:

* Конвенція Ради Європи про кіберзлочинність, ратифікована Законом Ук- раїни від 7.09.2005 року № 2824-ІV;
* Закони України: «Про інформацію», «Про національну безпеку України»,

«Про Державну службу спеціального зв’язку та захисту інформації Укра- їни», «Про телекомунікації», «Про захист інформації в інформаційно-теле- комунікаційних системах», «Про доступ до публічної інформації», «Про оборону України», «Про засади внутрішньої і зовнішньої політики», «Про об’єкти підвищеної небезпеки»;

* Укази Президента України, зокрема про Доктрину інформаційної безпеки, Стратегію національної безпеки України та Воєнну доктрину України;
* окремі положення Кримінального кодексу України;
* окремі постанови Кабінету Міністрів України та рішення Ради національ- ної безпеки та оборони України.

В Законі України «Про національну безпеку України» надається ви- значення таким важливим документам, як:

* 1. Стратегія національної безпеки України – документ, що визначає актуальні загрози національній безпеці України та відповідні цілі, завдання, механізми захисту національних інтересів України та є основою для плану- вання й реалізації державної політики у сфері національної безпеки;
  2. Стратегія воєнної безпеки України – документ, у якому виклада- ється система поглядів на причини виникнення, сутність і характер

сучасних воєнних конфліктів, принципи і шляхи запобігання їх виник- ненню, підготовку держави до можливого воєнного конфлікту, а також на застосування воєнної сили для захисту державного суверенітету, територі- альної цілісності, інших життєво важливих національних інтересів;

* 1. Стратегія кібербезпеки України – документ довгострокового пла- нування, що визначає загрози кібербезпеці України, пріоритети та напрями забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, сус- пільства і держави;
  2. Стратегія громадської безпеки та цивільного захисту України – до- кумент довгострокового планування, що розробляється на основі Стратегії національної безпеки України за результатами огляду громадської безпеки та цивільного захисту і визначає напрями державної політики щодо гаран- тування захищеності життєво важливих для держави, суспільства та особи інтересів, прав і свобод людини і громадянина, цілі та очікувані результати їх досягнення з урахуванням актуальних загроз.

Загрози національній безпеці України та відповідні пріоритети держа- вної політики у сферах національної безпеки і оборони визначаються у Стратегії національної безпеки України, Стратегії воєнної безпеки України, Стратегії кібербезпеки України, інших документах з питань національної безпеки і оборони, які схвалюються Радою національної безпеки і оборони України і затверджуються указами Президента України.

Стратегія національної безпеки України була затверджена Указом Президента України 14.09.2020 року.

Стратегія визначає основні пріоритети національних інтересів Укра- їни та забезпечення національної безпеки, цілі та основні напрями держав- ної політики у сфері національної безпеки; поточні та прогнозовані загрози національній безпеці та національним інтересам України з урахуванням зо- внішньополітичних та внутрішніх умов; основні напрями зовнішньополі- тичної та внутрішньополітичної діяльності держави для забезпечення її на- ціональних інтересів і безпеки; напрями та завдання реформування й роз- витку сектору безпеки і оборони; ресурси, необхідні для реалізації Страте- гії.

Стратегія національної безпеки України ґрунтується на таких основ-

них засадах:

стримування - розвиток оборонних і безпекових спроможностей для унеможливлення збройної агресії проти України;

стійкість - здатність суспільства та держави швидко адаптуватися до змін безпекового середовища й підтримувати стале функціонування, зок- рема шляхом мінімізації зовнішніх і внутрішніх уразливостей;

взаємодія - розвиток стратегічних відносин із ключовими іноземними партнерами, насамперед з Європейським Союзом і НАТО та їх державами-

членами, Сполученими Штатами Америки, прагматичне співробітництво з іншими державами та міжнародними організаціями на основі національних інтересів України.

На підставі Конституції України, Закону України «Про національну безпеку України» у Стратегії визначаються пріоритети національних інте- ресів України та забезпечення національної безпеки – це відстоювання не- залежності і державного суверенітету; відновлення територіальної цілісно- сті у межах міжнародно визнаного державного кордону України; суспіль- ний розвиток, насамперед розвиток людського капіталу; захист прав, сво- бод і законних інтересів громадян України; європейська і євроатлантична інтеграція.

Відповідно до Закону «Про національну безпеку України» державна політика у сферах національної безпеки і оборони спрямована на захист:

людини і громадянина - їхніх життя і гідності, конституційних прав і свобод, безпечних умов життєдіяльності;

суспільства - його демократичних цінностей, добробуту та умов для сталого розвитку;

держави - її конституційного ладу, суверенітету, територіальної цілі- сності та недоторканності; території, навколишнього природного середо- вища - від надзвичайних ситуацій.

Основними принципами, що визначають порядок формування держа- вної політики у сферах національної безпеки і оборони, є:

1. верховенство права, підзвітність, законність, прозорість та дотримання засад демократичного цивільного контролю за функціонуванням сектору безпеки і оборони та застосуванням сили;
2. дотримання норм міжнародного права, участь в інтересах України у між- народних зусиллях з підтримання миру і безпеки, міждержавних системах та механізмах міжнародної колективної безпеки;
3. розвиток сектору безпеки і оборони як основного інструменту реалізації державної політики у сферах національної безпеки і оборони.

Фундаментальними національними інтересами України є:

1. державний суверенітет і територіальна цілісність, демократичний кон- ституційний лад, недопущення втручання у внутрішні справи України;
2. сталий розвиток національної економіки, громадянського суспільства і держави для забезпечення зростання рівня та якості життя населення;
3. інтеграція України в європейський політичний, економічний, безпеко- вий, правовий простір, набуття членства в Європейському Союзі та в Орга- нізації Північноатлантичного договору, розвиток рівноправних взаємовигі- дних відносин з іншими державами.

Слід відзначити, що сектор безпеки і оборони підлягає демократич- ному цивільному контролю, який здійснюється Президентом України, Вер- ховною Радою України, Радою національної безпеки і оборони, Кабінетом

Міністрів України, органами виконавчої влади та органами місцевого само- врядування, встановлюється також судовий контроль та громадський на- гляд.

Державна політика у сферах національної безпеки і оборони спрямо- вується на забезпечення воєнної, зовнішньополітичної, державної, еконо- мічної, інформаційної, екологічної безпеки, кібербезпеки України тощо.

# Питання для самоконтролю

* 1. Що таке кіберборотьба?
  2. Які основні особливості їй притаманні?
  3. Дайте визначення поняття «кібернетична безпека».
  4. Визначить істотні ознаки, що характеризують кібербезпеку.
  5. У чому полягають основні причини головних проблем забезпечення кібербезпеки?
  6. Які стратегії затверджені в Законі України «Про національну без- пеку України»?
  7. В чому полягає значення Стратегії національної безпеки України?
  8. На яких засадах ґрунтується Стратегія національної безпеки Укра-

їни?

* 1. В чому полягає головна мета державної політики в сфері націона-

льної безпеки?

* 1. На яких принципах базується державна політики в сфері націона- льної безпеки та оборони?

# Розділ 3. ЗАГРОЗИ ДЛЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ, СУСПІЛЬСТВА, ЛЮДИНИ

* 1. Поняття загроз інформаційній безпеці.
  2. Види загроз інформаційній безпеці.
  3. Фактори загроз інформаційній безпеці.
  4. Джерела загроз інформаційній безпеці.
  5. Етапи розвитку засобів інформаційних комунікацій.

# Поняття загроз інформаційній безпеці

*Загрози інформаційній безпеці – сукупність умов і факторів, що ство- рюють небезпеку життєво важливим інтересам особи, суспільства й дер- жави в інформаційній сфері.*

Основні загрози інформаційній безпеці можна поділити на три групи:

1. загрози впливу неякісної інформації (недостовірної, фальшивої, дезінформації) на особу, суспільство, державу;
2. загрози несанкціонованого і неправомірного впливу сторонніх осіб на інформацію й інформаційні ресурси (на виробництво інформації, інфор- маційні ресурси, на системи їхнього формування і використання);
3. загрози інформаційним правам і свободам особи (праву на вироб- ництво, поширення, пошук, одержання, передавання і використання інфор- мації; праву на інтелектуальну власність на інформацію і речову власність на документовану інформацію; праву на захист честі й гідності тощо).

Аналіз і виявлення загроз інформаційної безпеки є важливою функ- цією забезпечення інформаційної безпеки. Багато в чому вигляд розроблю- ваної системи захисту і склад механізмів її реалізації визначається потен- ційними загрозами, виявленими на цьому етапі. Наприклад, якщо користу- вачі мають доступ в Інтернет, то кількість загроз інформаційній безпеці рі- зко зростає, відповідно, це відбивається на методах і засобах захисту і т. д. Загроза інформаційній безпеці – це потенційна можливість пору- шення режиму інформаційної безпеки. Навмисна реалізація загрози нази- вається атакою на інформаційну систему. Особи, які навмисно реалізують загрози, є зловмисниками. Найчастіше загроза є наслідком наявності враз- ливих місць у захисті інформаційних систем, наприклад, неконтрольований доступ до персональних комп’ютерів або неліцензійне програмне забезпе- чення (на жаль, навіть ліцензійне програмне забезпечення не позбавлене вразливостей). Історія розвитку інформаційного середовища показує, що нові вразливі місця з’являються постійно. З такою ж регулярністю, але з невеликим відставанням з’являються і засоби захисту. Переважно засоби захисту з’являються у відповідь на виникаючі загрози. Так, наприклад, по- стійно з’являються виправлення до програмного забезпечення фірми Microsoft, що усувають чергові його вразливі місця. Такий підхід до забез- печення безпеки малоефективний, оскільки завжди існує проміжок часу між моментом виявлення загрози та її усуненням. Саме в цей період злов- мисник може завдати непоправної шкоди інформації. У цьому зв’язку більш прийнятним є інший спосіб – спосіб попереджувального захисту, що полягає в розробці механізмів захисту від можливих, передбачуваних і по- тенційних загроз. Але деякі загрози не можна вважати наслідком цілеспря- мованих дій шкідливого характеру. Існують загрози, викликані випадко-

вими помилками або техногенними явищами.

Знання можливих загроз інформаційній безпеці, а також вразливих місць системи захисту, необхідне для того, щоб вибрати найбільш економі- чні й ефективні засоби забезпечення інформаційної безпеки.

# Види загроз інформаційній безпеці

Відповідно виділяють такі види загроз.

## За ступенем гіпотетичної шкоди:

*загроза* – явні чи потенційні дії, які ускладнюють або унеможливлю- ють реалізацію національних інтересів в інформаційній сфері та створюють небезпеку для системи державного управління, життєзабезпечення її систе- моутворюючих елементів;

*небезпека* – безпосередня дестабілізація функціонування системи дер- жавного управління.

## За повторюваністю вчинення:

*повторювані* – такі загрози, які раніше вже мали місце;

*продовжувані* – неодноразове здійснення загроз, що складається з ряду тотожних, які мають спільну мету.

## За сферами походження:

*екзогенні* – джерело дестабілізації системи лежить поза її межами;

*ендогенні* – алгоритм дестабілізації системи перебуває в самій сис-

темі.

## За ймовірністю реалізації:

*імовірні* – такі загрози, які за виконання певного комплексу умов

обов’язково відбудуться. Прикладом може слугувати оголошення атаки ін- формаційних ресурсів суб’єкта забезпечення національної безпеки, яке пе- редує самій атаці;

*неможливі* – такі загрози, які за виконання певного комплексу умов ніколи не відбудуться. Такі загрози зазвичай мають більше декларативний характер, не підкріплений реальною і, навіть, потенційною можливістю здійснити проголошені наміри, вони здебільшого мають залякуючий хара- ктер;

*випадкові* – такі загрози, які за виконання певного комплексу умов ко- жного разу протікають по-різному. Загрози цього рівня доцільно аналізу- вати за допомогою методів дослідження операцій, зокрема теорії ймовірно-

стей і теорії ігор, які вивчають закономірності у випадкових явищах.

## За джерелами походження:

*природного походження* – включають у себе небезпечні геологічні, метеорологічні, гідрологічні морські та прісноводні явища, деградацію ґру- нтів чи надр, природні пожежі, масове ураження сільськогосподарських ро- слин і тварин хворобами чи шкідниками, зміна стану водних ресурсів і біо- сфери тощо;

*техногенного походження* – транспортні аварії (катастрофи), пожежі, неспровоковані вибухи чи їх загроза, раптове руйнування каналів зв’язку, аварії на інженерних мережах і спорудах життєзабезпечення, аварії голов- них серверів органів державного управління тощо;

*антропогенного походження* – вчинення людиною різноманітних дій із руйнування інформаційних систем, ресурсів, програмного забезпечення об’єкта тощо.

*До цієї групи за змістом дій належать*:

А) ненавмисні, викликані помилковими чи ненавмисними діями лю- дини (це, наприклад, може бути помилковий запуск програми, ненавмисне інсталяція закладок тощо);

Б) навмисні (інспіровані), що стали результатом навмисних дій людей (наприклад: навмисна інсталяція програм, які передають інформацію на інші комп’ютери, навмисне введення вірусів тощо).

## За значенням:

*допустимі* – такі загрози, які не можуть призвести до колапсу сис- теми. Прикладом можуть слугувати віруси, які не пошкоджують програми шляхом їх знищення;

*недопустимі* – такі загрози, які: можуть у разі їх реалізації призвести до колапсу і системної дестабілізації системи; можуть призвести до змін, несумісних із подальшим існуванням системи.

## За структурою впливу:

*системні* – загрози, що впливають одразу на всі складові елементи суб’єкта ЗНБ;

*структурні* – загрози, що впливають на окремі структури системи. Ці загрози є також небезпечними, водночас вони стосуються структури окре- мих органів державної влади або їхніх компонентів;

*елементні* – загрози, що впливають на окремі елементи структури си- стеми. Такі загрози носять постійний характер і можуть бути небезпечними лише за умови неефективності або не проведення їх моніторингу.

## За характером реалізації:

*реальні* – активізація алгоритмів дестабілізації є неминучою і не об- межена часовим інтервалом і просторовою дією;

*потенційні* – активізація алгоритмів дестабілізації можлива за певних умов середовища функціонування органу державного управління;

*здійснені* – такі загрози, які втілені в життя;

*уявні* – псевдоактивізація алгоритмів дестабілізації, або ж активізація таких алгоритмів, що за деякими ознаками схожі з алгоритмами дестабілі- зації, але такими не є.

## За ставленням до них:

*об’єктивні* – такі загрози, які підтверджуються сукупністю обставин і фактів, що об’єктивно характеризують навколишнє середовище, крім того, ставлення до них суб’єкта управління не відіграє вирішальної ролі через те, що об’єктивні загрози існують незалежно від волі та свідомості суб’єкта;

*суб’єктивні* – така сукупність чинників об’єктивної дійсності, яка вва- жається загрозою суб’єктом управління системою безпеки.

***За об’єктом впливу:*** на державу; на людину; на суспільство.

Загрози можуть мати або об’єктивну природу, наприклад, зміна умов фізичного середовища (пожежі, повені і т. ін.) чи відмовлення елементів

обчислювальної системи, або суб’єктивну, наприклад, помилки персоналу. Загрози, що мають суб’єктивну природу, можуть бути випадковими або на- вмисними. Отже, на будь-якому об’єкті повинні здійснюватися деякі дії чи фактори, що будуть перешкоджати реалізації конкретних захисних механі- змів і заходів, створюючи тим самим відзначені вище загрози. При цьому вони будуть безпосередньо пов’язані з цими загрозами і будуть, власне ка- жучи, їхніми причинами.

Ці події чи фактори можна охарактеризувати в такий спосіб:

вони об’єктивно існують і можуть реалізуватися в будь-який момент часу на будь-якому об’єкті, де обробляється інформація, що підлягає захи- сту;

вони не зводяться до загроз;

один і той самий процес чи подія в одному випадку призводить до загроз, а в іншому – не являє собою ніякої небезпеки для інформації;

для кожного такого фактору існує можливість явно установити, з якими видами загроз він пов’язаний;

виникає можливість здійснювати конкретні дії по протидії загрозам. Таким чином, виявляється, що загрози виникають унаслідок здійс-

нення цих факторів, тобто є їх результатом. Надалі ці фактори будемо на- зивати дестабілізуючими факторами (ДФ). Як показує подальший аналіз, введення поняття ДФ цілком логічно виправдане і дає змогу одержати дуже просту, зрозумілу й наочну схему для створення моделі загроз.

# 3. 3. Фактори загроз інформаційній безпеці

Фактори загроз за видовою ознакою поділяються на політичні, еконо- мічні та організаційно-технічні.

# Під політичними факторами загроз інформаційній безпеці розуміють:

зміни геополітичної ситуації внаслідок фундаментальних змін у різ- номанітних регіонах світу, зведення до мінімуму ймовірності світової яде- рної війни;

інформаційна експансія розвинених країн, які здійснюють глобальний моніторинг світових політичних, економічних, воєнних, екологічних та ін- ших процесів, та поширюють інформацію з метою здобуття односторонніх переваг;

становлення нової державності в пострадянських країнах на основі принципів демократії, законності, інформаційної відкритості;

знищення колишньої командно-адміністративної системи державного управління, а також системи забезпечення безпеки;

порушення інформаційних зв’язків унаслідок утворення на території колишнього СРСР нових держав;

прагнення пострадянських країн до більш тісного співробітництва із закордонними країнами в процесі проведення реформ на основі максималь- ної відкритості сторін;

низька загальна правова та інформаційна культура сторін. **Основними економічними факторами загроз безпеці інформації є:** перехід на ринкові відносини в економіці, поява на ринку великої кі-

лькості вітчизняних та зарубіжних комерційних структур – виробників та споживачів інформації, засобів інформатизації та захисту інформації, вклю- чення інформаційної продукції в систему товарних відносин;

критичний стан вітчизняних галузей промисловості, які виробляють засоби інформатизації та захисту інформації;

розширення кооперації із зарубіжними країнами в розвитку інформа- ційної інфраструктури.

# Основними організаційно-технічними факторами загроз інфор- маційній безпеці є:

* недостатня нормативно-правова база у сфері інформаційних від- носин, у тому числі в галузі забезпечення інформаційної безпеки;
* недостатнє регулювання державою процесів функціонування та розвитку
* ринку засобів інформатизації, інформаційних продуктів та послуг;
* широке використання у сфері державного управління та кредитно- фінансової сфери незахищених від витоку інформації імпортних технічних та програмних засобів для зберігання, обробки та пере- давання інформації;
* зростання обсягів інформації, яка передається відкритими кана- лами зв’язку;
* загострення криміногенної ситуації, зростання числа комп’ютер- них злочинів, особливо в кредитно-фінансовій сфері.

# 3.4. Джерела загроз інформаційній безпеці

З огляду на визначення загроз інформаційній безпеці, можна виділити декілька основних джерел загроз, які можуть стосуватися інтересів особи, суспільства й держави.

# Джерела загроз інформаційній безпеці особи.

**Інтереси особи, які необхідно охороняти в інформаційному суспі- льстві**, полягають насамперед у реальному забезпеченні конституційних прав і свобод людини і громадянина на доступ до відкритої інформації, на використання інформації в інтересах здійснення не забороненої законом ді- яльності, а також у захисті інформації, що забезпечує особисту безпеку, ду- ховний та інтелектуальний розвиток.

Найбільш небезпечним джерелом загроз цим інтересам вважається суттєве розширення можливості маніпулювання свідомістю людини за ра- хунок формування навколо неї індивідуального «віртуального інформацій- ного простору», а також можливість використання технологій впливу на її психічну діяльність. Важливою особливістю способу життя людини в ін- формаційному суспільстві є суттєве скорочення «інформаційних» відста- ней (часу доступу до необхідної інформації), що веде до появи нових мож- ливостей як із формування особистості, так і з реалізації її потенціалу.

Людство впритул підходить до рубежів, за якими інформаційна ін- фраструктура стає, по суті, основним джерелом інформації для людини, здійснює безпосередній вплив на її психічну діяльність, на формування її соціальної поведінки. Проблема формування розумових потреб і мотивації соціальної поведінки поки не має загального вирішення навіть для індуст- ріального суспільства і ще більше ускладнюється стосовно інформаційного суспільства. Вона є однією з найбільш складних у сучасній психологічній науці. Загалом структура споживчо-мотиваційної сфери особи утворюється базовими потребами, зумовленими його генотипом (в їжі, особистій без- пеці, потреба в продовженні роду, довголітті, а також потребами у спілку- ванні з іншими людьми), похідними потребами, що формуються діючою системою виховання. Способи і форми задоволення цих потреб великою мірою залежать від інформації і знань, що одержуються з навколишнього світу і, зокрема, надходять через інформаційну інфраструктуру. Спрямова- ність використання одержаної інформації і результати, що одержуються, визначаються передусім особою людини та її духовним потенціалом. Скла- дність процедур, що реалізуються в сучасних технологіях доступу до необ- хідних інформаційних ресурсів, критично збільшують залежність окремої людини від інших людей, які розробляють інформаційні технології, визна- чення алгоритмів пошуку необхідної інформації, її попередньої обробки, приведення до виду, зручного для сприйняття, доведення до споживача. По суті, ці люди формують для людини інформаційний фон його життя, визна- чають умови, в яких він живе і діє, вирішує свої життєві проблеми. Саме тому вважається виключно важливим забезпечити безпеку взаємодії лю- дини з інформаційною структурою.

Іншим небезпечним джерелом загроз інтересам особи є використання

на шкоду її інтересам персональних даних, що нагромаджуються різнома- нітними структурами, у тому числі органами державної влади, а також ро- зширення можливості прихованого збирання інформації, що становить його особисту й сімейну таємницю, відомості про її приватне життя. Це зу- мовлено насамперед труднощами реалізації механізмів охорони цих відо- мостей, подальшими досягненнями в мікромініатюризації засобів прихова- ного збирання і передавання інформації.

# Інформаційна безпека людини (в широкому розумінні) перед- бачає:

по-перше, *належний рівень інформаційної культури*, тобто теоретич- ної та практичної підготовки особистості, за якого досягається захищеність і реалізація її життєво важливих інтересів та гармонійний розвиток в умо- вах інформаційного суспільства незалежно від наявності інформаційних за- гроз;

по-друге, *здатність держави створити умови для гармонійного роз- витку й задоволення потреб особи в інформації* незалежно від наявності інформаційних загроз;

по-третє, *гарантування, розвиток і використання інформаційного се- редовища в інтересах особистості*;

по-четверте, *захищеність від різного роду інформаційних загроз*.

# Джерела загроз інформаційній безпеці суспільства.

Інтереси суспільства, що вступило у стадію постіндустріального роз- витку, полягають у захисті життєво важливих інтересів у цій сфері, забез- печення реалізації конституційних прав і свобод людини та громадянина в інтересах зміцнення демократії, досягнення і підтримування суспільної зла- годи, підвищення творчої активності населення.

Одним із джерел загроз інтересам суспільства в інформаційній сфері є безперервне ускладнення інформаційних систем і мереж зв’язку критично важливих інфраструктур забезпечення життя суспільства. Ці загрози мо- жуть проявлятися у вигляді як навмисних, так і ненавмисних помилок, збоїв і відмов техніки і програмного забезпечення, шкідливого впливу зі сторони злочинних структур і кримінальних елементів. Об’єктами реалізації таких структур можуть виступати системи енергетичної, транспортної, трубопро- відної і деяких інших інфраструктур.

Небезпечним джерелом загроз виступає можливість концентрації за- собів масової інформації в руках невеликої групи власників. Ці загрози мо- жуть проявлятися у вигляді маніпуляції суспільною думкою щодо тих чи інших суспільно значущих подій, а також руйнування моральних устоїв су- спільства шляхом нав’язування чужорідних цінностей.

Нарешті, небезпечним джерелом загроз є розширення масштабів віт- чизняної і міжнародної комп’ютерної злочинності. Ці загрози можуть про- являтися у вигляді спроб здійснення шахрайських операції з використанням глобальних або вітчизняних інформаційно-телекомунікаційних систем, від- мивання фінансових коштів, одержаних протиправним шляхом, одержання неправомірного доступу до фінансової, банківської та іншої інформації, яка може бути використаною з корисливою метою.

**Джерела загроз інформаційній безпеці держави** Інтереси держави в інформаційній сфері полягають у створенні умов для гармонійного розви- тку інформаційної інфраструктури держави, реалізації конституційних

прав і свобод людини і громадянина в інтересах зміцнення конституційного ладу, суверенітету і територіальної цілісності країни, встановлення полі- тичної і соціальної стабільності, економічного процвітання, безумовного виконання законів і підтримки міжнародного співробітництва на основі партнерства.

Передусім загрози інтересам держави також можуть проявлятися у вигляді отримання протиправного доступу до відомостей, що складають державну таємницю, до іншої конфіденційної інформації, розкриття якої може нанести збитки. Проте найбільш небезпечними джерелами загроз ін- тересам держави в інформаційному суспільстві може стати неконтрольо- ване поширення інформаційної зброї та розгортання гонки озброєнь у цій галузі, спроби реалізації концепції ведення інформаційних війн.

Серед найбільш серйозних завдань, які можуть вирішуватися за допо- могою сучасної інформаційної зброї, можна виділити такі:

створення атмосфери бездуховності та аморальності, негативного ві- дношення до культурної спадщини противника;

маніпулювання суспільною свідомістю та політичною орієнтацією со- ціальних груп населення держави з метою створення політичної напруги та хаосу;

дестабілізація політичних відносин між партіями, об’єднаннями та рухами з метою провокації конфліктів, розпалювання недовіри, загост- рення політичної боротьби, провокування репресій проти опозиції, прово- кація взаємного знищення;

зниження інформаційного забезпечення влади та управління, інспіра- ція помилкових управлінських рішень;

дезінформація населення про роботу державних органів, підрив їх- нього авторитету, дискредитація органів управління;

провокування соціальних, політичних, національних і релігійних су- тичок;

ініціювання страйків, масових заворушень та інших акцій економіч- ного протесту;

ускладнення прийняття органами важливих рішень;

підрив міжнародного авторитету держави, її співробітництва з ін- шими країнами;

нанесення втрат життєво важливим інтересам держави в політичній, економічній, оборонній та інших сферах.

Руйнівний вплив інформаційних загроз в інформаційному суспільстві може бути більш потужним та ефективним, ніж це уявляється. Особливо небезпечним це є в умовах існування майже монопольного положення ком- паній невеликої кількості країн на ринку інформаційних продуктів, оскі- льки це здатне спровокувати бажання використати наявну перевагу для до- сягнення тієї чи іншої політичної мети.

# 3.5. Етапи розвитку засобів інформаційних комунікацій

Враховуючи вплив на трансформацію ідей інформаційної безпеки, у розвитку засобів інформаційних комунікацій можна виділити декілька ета- пів:

**I етап – до 1816 року** – характеризується використанням природно виникаючих засобів інформаційних комунікацій. У цей період основне за- вдання інформаційної безпеки полягало в захисті відомостей про події, фа- кти, майно, місцезнаходження й інші дані, що мають для людини особисто або співтовариства, до якого вона належала, життєве значення.

1. **етап – починаючи з 1816 року** – пов’язаний із початком викорис- тання штучно створюваних технічних засобів електро- і радіозв’язку. Для забезпечення скритності й перешкодостійкості радіозв’язку необхідно було використовувати досвід першого періоду інформаційної безпеки на ви- щому технологічному рівні, а саме застосування перешкодостійкого коду- вання повідомлення (сигналу) з подальшим декодуванням прийнятого по- відомлення (сигналу).
2. **етап – починаючи з 1935 року** – пов’язаний із появою засобів ра- діолокації й гідроакустики. Основним способом забезпечення інформацій- ної безпеки в цей період було поєднання організаційних і технічних заходів, спрямованих на підвищення захищеності засобів радіолокації від дії на їхні приймальні пристрої активними маскуючими і пасивними імітуючими ра- діоелектронними перешкодами.
3. **етап – починаючи з 1946 року** – пов’язаний із винаходом і впро- вадженням у практичну діяльність електронно-обчислювальних машин (комп’ютерів). Завдання інформаційної безпеки вирішувалися переважно методами і способами обмеження фізичного доступу до устаткування засо- бів добування, переробки і передачі інформації.
4. **етап – починаючи з 1965 року** – зумовлений створенням і розвит- ком локальних інформаційно-комунікаційних мереж. Завдання інформа- ційної безпеки також вирішувалися, в основному, методами і способами фі- зичного захисту засобів добування, переробки і передачі інформації, об’єд- наних у локальну мережу шляхом адміністрування і управління доступом до мережевих ресурсів.
5. **етап – починаючи з 1973 року** – пов’язаний із використанням надмобільних комунікаційних пристроїв із широким спектром завдань. За- грози інформаційній безпеці стали набагато серйознішими. Для забезпе- чення інформаційної безпеки в комп’ютерних системах із безпровідними мережами передачі даних потрібно було розробити нові критерії безпеки. Утворилися співтовариства людей-хакерів, що ставлять собі за мету нане- сення збитку інформаційній безпеці окремих користувачів, організацій і ці- лих країн. Інформаційний ресурс став найважливішим ресурсом держави, а забезпечення його безпеки – найважливішою й обов’язковою складовою

національної безпеки. Формується інформаційне право – нова галузь між- народної правової системи.

1. **етап – починаючи з 1985 року** – пов’язаний зі створенням і роз- витком глобальних інформаційно-комунікаційних мереж із використанням космічних засобів забезпечення. Можна припустити що черговий етап роз- витку інформаційної безпеки, очевидно, буде пов’язаний із широким вико- ристанням надмобільних комунікаційних пристроїв із широким спектром завдань і глобальним охопленням у просторі та часі, забезпечуваним космі- чними інформаційно-комунікаційними системами. Для вирішення завдань інформаційної безпеки на цьому етапі необхідним є створення макросис- теми інформаційної безпеки людства під егідою ведучих міжнародних фо- румів.

# Питання для самоконтролю

* 1. Дайте визначення поняттям «загроза», «небезпека».
  2. Яким чином розрізняються групи загроз інформації?
  3. Визначте види загроз за ймовірністю реалізації, за джерелами по- ходження, за значенням, за структурою та об’єктом впливу, за характером реалізації.
  4. Які основні підходи до визначення дестабілізуючих факторів ви знаєте?
  5. Визначте політичні, економічні, організаційно-технічні фактори загроз.
  6. Охарактеризуйте джерела загроз інформаційній безпеці особи.
  7. Які джерела загроз інформаційній безпеці суспільству існують?
  8. Назвіть джерела загроз інформаційній безпеці держави.
  9. Визначить етапи розвитку засобів інформаційних комунікацій.
  10. Охарактеризуйте кожний етап розвитку засобів інформаційних ко- мунікацій.

# Розділ 4. ПРИНЦИПИ. ФОРМИ ТА МЕТОДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

* 1. Основні принципи забезпечення інформаційної безпеки держави.
  2. Основні форми забезпечення інформаційної безпеки держави.
  3. Методи забезпечення інформаційної безпеки.

# Основні принципи забезпечення інформаційної безпеки держави

Забезпечення інформаційної безпеки держави – це сукупність заходів, призначених для досягнення стану захищеності потреб особи, суспільства й держави в інформації.

Забезпечення інформаційної безпеки досягається в процесі свідомої цілеспрямованої діяльності органів державного управління із запобігання можливого порушення їх нормального функціонування в результаті дії за- гроз та небезпек.

Метою забезпечення інформаційної безпеки є створення нормальних умов функціонування конкретного органу державного управління, а також проведення моніторингу стану інформаційної безпеки для розроблення оп- тимальної моделі функціонування системи забезпечення інформаційної безпеки.

Держава здійснює свої заходи через відповідні органи, а громадяни, суспільні організації й об’єднання, що мають відповідні повноваження, – згідно із законодавством.

В основу забезпечення інформаційної безпеки держави повинні бути покладені такі принципи:

- законність, дотримання балансу інтересів особи, суспільства і дер- жави;

 взаємна відповідальність суб’єктів забезпечення інформаційної без-

пеки;

 інтеграція систем національної і міжнародної безпеки.

Специфічними принципами забезпечення інформаційної безпеки є:

1. *превентивний характер проведення її заходів щодо заходів інших*

*видів безпеки.* Превентивність (лат. praeventio від praevenio – «попере- джую») зумовлена властивою людині послідовністю виконання операцій, що складає будь-яку елементарну дію. Усе починається з приймання (добу- вання) інформації, а закінчується активною дією: реакцією на одержану ін- формацію. Оскільки це справедливо щодо будь-якого виду діяльності, то можна стверджувати, що цей принцип є загальним, і його дія поширюється на всі сфери безпеки особи, суспільства та держави.

1. *адекватна інформованість об’єктів безпеки, у тому числі й між- народних*. Адекватна інформованість об’єктів безпеки означає, що всі вони мають право володіти інформацією про явища і процеси, що їх цікавлять, яке обмежене тільки законодавчо з метою охорони особистої, сімейної, професійної, комерційної та державної таємниці, а також моралі. Права та свободи суспільства в питаннях пошуку, володіння та поширення інформа- ції повинні регулюватися законодавчими актами, які видаються щодо спе- цифіки діяльності суспільних об’єднань та організацій або змісту інформа- ції. Наприклад, адекватна інформованість суспільства про його матеріальні цінності досягається у сфері нормотворчості та правозастосування законо- давства про захист комерційної таємниці. Права та свободи суспільства в духовній сфері повинні захищати законодавчі акти, які визначають порядок освіти та функціонування освітніх, просвітницьких, культурних, релігійних організацій, а також засобів масової інформації. В основі прав і свобод

держави у сфері її інформованості з питань світової політики, економіки, науки, ресурсів, екології, оборони тощо лежать діючі норми та принципи міждержавного права.

Головним слід вважати принцип рівної безпеки. Стосовно до інфор- маційної сфери можна говорити про його трансформацію в принцип адек- ватної інформованості держав світового співтовариства, який передбачає право кожної держави на інформаційну безпеку, забезпечення інформацій- ної безпеки всіх членів співтовариства рівною мірою, врахування інтересів усіх сторін без будь-якої дискримінації, виключення односторонніх пере- ваг, відмова від дій, що наносять шкоду іншій державі. Законодавча база, яка визначає перелік відомостей, що віднесені до державної таємниці, ме- ханізм та порядок її захисту повинні розроблятися, виходячи із наведеного принципу, а також багатосторонніх угод держав, які входять до міжнарод- ної системи інформаційної безпеки. Формування останньої буде, очевидно, справою далекої перспективи, яка ознаменує собою вищий рівень прояву довіри та зацікавленості держав світового співтовариства в забезпеченні ви- конання на практиці принципу адекватної інформованості. Така система повинна стати підсистемою в системі колективної безпеки.

# Основні форми забезпечення інформаційної безпеки держави

Форми та способи забезпечення інформаційної безпеки утворюють власне інструмент, з допомогою якого сили інформаційної безпеки вирішу- ють увесь комплекс завдань із захисту життєво важливих інтересів особи, суспільства та держави. Тому необхідне чітке юридичне оформлення при розробці нормативних актів, які регулюють діяльність органів інформацій- ної безпеки. Найважливіша вимога до обґрунтування способів, форм і ме- ханізмів їхньої реалізації полягає в абсолютному верховенстві права у будь- якій діяльності, у тому числі й політичній. У свою чергу, кожний суб’єкт інформаційного процесу повинен мати відповідну правову свідомість, бути законослухняним, добре уявляти наслідки своїх дій для інших суб’єктів та міру відповідальності на випадок порушення їхніх життєво важливих інте- ресів. Це є принциповим, оскільки застосування тих чи інших форм і спо- собів залежить від того, чи є інформаційні загрози наслідком ненавмисних або навмисних дій суб’єктів інформаційного процесу. У першому випадку забезпечення інформаційної безпеки здійснюється відповідно у формах ін- формаційного патронату та інформаційної кооперації, у другому – у формі інформаційного протиборства

**Інформаційний патронат** (лат. patronatys від patronys – «захисник»)

– форма забезпечення інформаційної безпеки фізичних і юридичних осіб з боку держави. Він припускає забезпечення органів управління системи ін- формаційної безпеки держави відомостями про дестабілізуючі фактори і за- грози стану інформованості фізичних і юридичних осіб (інформаційне

забезпечення інформаційної безпеки) і власне захист життєво важливих ін- тересів цих осіб від інформаційних загроз або, як ще кажуть, інформацій- ний захист. При цьому інформаційне забезпечення інформаційної безпеки включає збирання (добування) відомостей про дестабілізуючі фактори та інформаційні загрози, їхню обробку, обмін інформацією між органами ке- рування й силами та засобами системи інформаційної безпеки. Його основу становить збирання (добування) необхідних відомостей, здійснюване в процесі розвідувальної, оперативно-розшукової й оперативно-інформацій- ної діяльності.

**Інформаційний захист** досягається шляхом внесення в порядку зако- нодавчої ініціативи законопроектів, здійснення судового захисту, прове- дення оперативних заходів силами і засобами інформаційної безпеки.

**Інформаційна кооперація** – форма забезпечення інформаційної без- пеки між рівноправними суб’єктами інформаційного процесу (фізичними, юридичними, міжнародними), який включає сукупність їхніх взаємоузго- джених дій, спрямованих на одержання відомостей про дестабілізуючі фа- ктори, дестабілізуючі й інформаційні загрози та захист від них доступними законними способами і засобами.

**Інформаційне протиборство** – форма забезпечення інформаційної безпеки при здійсненні навмисних деструктивних дій суб’єктів інформацій- ного процесу. Інформаційне протиборство – суперництво соціальних сис- тем (країн, блоків країн) в інформаційній сфері щодо впливу на ті або інші сфери соціальних відносин і встановлення контролю над джерелами стра- тегічних ресурсів, у результаті якого одна група учасників суперництва отримує переваги, необхідні їм для подальшого розвитку.

Для конкретної особи такими способами і засобами можуть бути:

- судовий захист прав і свобод у використанні інформації;

 адміністративний захист її життєво важливих інтересів у інформо- ваності з боку територіальних або відомчих органів інформаційної без- пеки;

-автономний захист своїх прав і свобод переважно із застосуванням

технічних засобів захисту, особистої, сімейної і професійної таємниці.

Це ж характерно і для суспільних об’єднань, організацій (підпри- ємств). Разом із тим за наявності у них власних органів інформаційної без- пеки, їхні можливості у сфері автономного захисту суттєво розширюються.

# Методи забезпечення інформаційної безпеки

Завдання забезпечення інформаційної безпеки повинно вирішуватися системно, це означає, що різні засоби повинні застосовуватися одночасно і під централізованим управлінням. При цьому всі складові системи повинні

«знати» про існування один одного, взаємодіяти й забезпечувати захист як від зовнішніх, так і від внутрішніх загроз.

Діяльність із забезпечення інформаційної безпеки здійснюється за допо- могою різних способів, засобів і прийомів, які у своїй органічній сукупності складають методи. ***Метод передбачає певну послідовність дій на підставі конкретного плану.*** Методи можуть значно змінюватися й варіюватися за- лежно від типу діяльності, в якій вони використовуються, а також сфери застосування.

Важливими методами аналізу стану забезпечення інформаційної безпеки є **методи опису та класифікації**. Для здійснення ефективного захисту си- стеми державного управління необхідно, по-перше, описати, а лише потім класифікувати різні види загроз та небезпек, ризиків та викликів і відпо- відно сформулювати систему заходів зі здійснення управління ними.

Поширеними **методами аналізу стану забезпечення інформаційної безпеки** є **методи дослідження причинних зв’язків**. За допомогою цих методів виявляються причинні зв’язки між загрозами, ризиками, викликами та небезпеками; здійснюється пошук причин, які стали джерелом і спричи- нили актуалізацію тих чи інших чинників небезпеки, а також розробля- ються заходи з їх нейтралізації. У числі таких методів причинних зв’язків можна назвати такі: **метод схожості, метод відмінності, метод сполу- чення схожості і відмінності, метод змін, що супроводжують, метод за- лишків.**

Вибір методів аналізу стану забезпечення інформаційної безпеки зале- жить від конкретного рівня і сфери організації захисту. Залежно від загрози уможливлюється завдання щодо диференціації як різних рівнів загроз, так і різних рівнів захисту.

Що стосується сфери інформаційної безпеки, то в ній, зазвичай, виділя- ють:

фізичний, На фізичному рівні здійснюється організація і фізичний захист інформаційних ресурсів, інформаційних технологій, що використовуються, і управлінських технологій.

програмно-технічний, На програмно-технічному рівні здійснюється іде- нтифікації та перевірка дійсності користувачів, управління доступом, про- токолювання й аудит, криптографія, екранування, забезпечення високої до- ступності.

управлінський, На рівні управління здійснюється управління, координа- ція і контроль організаційних, технологічних і технічних заходів на всіх рі- внях управління з боку єдиної системи забезпечення інформаційної безпеки органів державного управління.

технологічний, . На технологічному рівні здійснюється реалізації полі- тики інформаційної безпеки за рахунок застосування комплексу сучасних автоматизованих інформаційних технологій.

рівень користувача, На рівні користувача реалізація політики інформа- ційної безпеки спрямована на зменшення рефлексивного впливу на

суб’єктів державного управління, унеможливлення інформаційного впливу з боку соціального середовища.

мережевий, На рівні мережі ця політика реалізується у форматі коорди- нації дій органів державного управління, які пов’язані між собою однією метою.

Процедурний. На процедурному рівні вживаються заходи, що реалізу- ються людьми. Серед них можна виділити такі групи процедурних заходів: управління персоналом, фізичний захист, підтримання працездатності, ре- агування на порушення режиму безпеки, планування реанімаційних робіт. Можна виокремити декілька типів методів забезпечення інформацій-

ної безпеки:

однорівневі методи будуються на підставі одного принципу управління інформаційною безпекою;

багаторівневі методи будуються на основі декількох принципів управ- ління інформаційною безпекою, кожний з яких слугує вирішенню власного завдання. При цьому приватні технології не пов’язані між собою і спрямо- вані лише на конкретні чинники інформаційних загроз;

комплексні методи – багаторівневі технології, які об’єднані в єдину сис- тему координуючими функціями на організаційному рівні з метою забезпе- чення інформаційної безпеки з огляду на аналіз сукупності чинників небе- зпеки, які мають семантичний зв’язок або генеруються з єдиного інформа- ційного центру інформаційного впливу;

інтегровані високоінтелектуальні методи - багаторівневі, багатокомпо- нентні технології, які побудовані на підставі могутніх автоматизованих ін- телектуальних засобів із організаційним управлінням.

Загальні методи забезпечення інформаційної безпеки активно викорис- товуються на будь-якій стадії управління загрозами. До таких стадій нале- жать:

прийняття рішення з визначення області та контексту інформаційної за- грози і складу учасників процесу протидії;

ухвалення загальної стратегії та схеми дій у політичній, економічній і соціальній сферах життєдіяльності;

забезпечення адекватного сприйняття загрози та небезпеки в більш ни- зьких організаційних ланках системи державного управління;

виділення необхідних політичних, економічних, соціальних, адміністра- тивних і організаційних ресурсів, достатніх для реалізації програми від- биття інформаційної загрози та збереження сталого розвитку інформацій- них ресурсів системи державного управління:

трансформації результатів оцінки ризиків у відповідну політику безпеки, включаючи національну.

Специфіка методів, що використовуються, значно залежить від суб’єкта діяльності, об’єкта впливу, а також цілей, що переслідуються. Так,

методи діяльності індивіда у зв’язку з його обмеженою можливістю забез- печення інформаційної безпеки здебільшого зводяться до джерела загрози, апелювання до суспільної думки, а також до держави, яка має вживати рі- шучих заходів із нейтралізації інформаційних загроз. Саме суспільство по- части використовує у своїй діяльності методи соціального регулювання, на- дання допомоги окремим індивідам і суспільним організаціям, яким спри- чинена шкода внаслідок виявлення загрози.

Причому, на жаль, слід констатувати, що в нашій країні не на достат- ньому рівні усвідомлюють небезпеку саме в інформаційній сфері, немає штатних одиниць в органах державного управління із забезпечення інфор- маційної безпеки, не проводиться підготовка відповідних фахівців для ор- ганів державного управління.

Дуже важливим є застосування аналітичних методів пізнання і дослі- дження стану суспільної свідомості у сфері інформаційної безпеки. Напри- клад, усвідомлення важливості забезпечення інформаційної безпеки на рі- вні індивіда, суспільства й організації заважає поширений міф про те, що захист інформації і криптографія те ж саме. Водночас таке розуміння є на- слідком використання застарілих підходів до інформаційної безпеки, коли інформаційна безпека лише ототожнюються із захистом інформації шляхом її шифрування. Нині важливою умовою забезпечення інформаційної без- пеки є не стільки секретність, конфіденційність інформації, скільки її дос- тупність, цілісність, захист від загроз.

Отже, система має відповідно реагувати та гарантувати ефективну ді- яльність у цьому напрямі.

Іншим завданням захисту є забезпечення незмінності інформації під час її зберігання або передачі, тобто забезпечення її цілісності.

Таким чином, конфіденційність інформації, яка забезпечується за до- помогою криптографічних методів, не є головною вимогою при проекту- ванні систем захисту інформації органів державного управління. Вико- нання процедур криптокодування і декодування може уповільнити пере- дачу даних та зменшити доступ до них через те, що працівник органу дер- жавного управління буде позбавлений можливості своєчасного та швид- кого доступу до цих даних та інформації, через функціонування механізму захисту. Саме тому забезпечення конфіденційності інформації має відпові- дати можливості доступу до неї.

Отже, управління у сфері інформаційної безпеки має здійснюватися на підставі принципу доступності та безпеки. Система забезпечення інфор- маційної безпеки насамперед має гарантувати доступність і цілісність ін- формації, а її конфіденційність – у випадку необхідності. Також зазначимо, що вплив хакерів та їхня можливість суттєво вплинути на інформаційні си- стеми дещо перебільшена. Здебільшого були зламані ті системи, які мали поганий захист. Так, наприклад, багато компаній в Україні, які мають

солідний грошовий обіг і достатні фінансові джерела, не мають не те щоб цілісної системи безпеки взагалі, а й навіть окремо функціонуючої підсис- теми забезпечення інформаційної безпеки. Переважно забезпечення інфор- маційної безпеки зводиться до того, що в системних блоках блокується доступ до флоппі-дисків і тим самим унеможливлюється несанкціонований запис інформації. Крім цього, системний адміністратор встановлює спеціа- льні програми-фільтри, що відсіюють можливість доступу до внутрішньої мережі ззовні. Можна перераховувати й інші методи захисту інформації, водночас, нині ототожнення забезпечення інформаційної безпеки із забез- печенням безпеки комп’ютерних систем є просто концептуальною помил- кою. Тому не є дивиною, що на сьогодні більша частина українських банків втратила внаслідок власної недбалості чимало коштів. І характерною рисою українського суспільства є те, що жоден із банків жодного разу не визнав факту вчиненого кіберзлочину проти себе.

У цьому аспекті можна зауважити на ще одну проблему: зневага до

вимог інформаційної безпеки та брак необхідних знань. Здебільшого під час робочого дня працівники, виконуючи свої службові обов’язки, відкри- вають паралельні вікна в Інтернеті, та самі, не усвідомлюючи того, відкри- вають доступ не лише до інформації, що в цей час обробляється, а загалом до комп’ютерної мережі всієї системи органів державного управління, по- чинаючи від Кабінету Міністрів України, закінчуючи місцевими органами виконавчої влади. Таким чином, один із найкращих засобів захисту інфор- мації від нападу – не допускати його. Втім не треба плекати надію на ство- рення абсолютної системи інформаційної безпеки, оскільки, як зазначалося вище, ми стоїмо на тій позиції, що загроза та небезпека є атрибутивними компонентами системи інформаційної безпеки, отже, їх існування та реалі- зація, а також негативні наслідки є природним компонентом системи інфо- рмаційної безпеки. Саме вони дають змогу побачити недоліки в системі уп- равління інформаційною безпекою, і водночас слугують імпульсом до вдо- сконалення, тобто до розвитку.

Треба зауважити, що важливим методом забезпечення інформаційної

безпеки є метод розвитку. Захист інформації не обмежується технічними методами, на що зазначає велике коло дослідників. Для ефективного забез- печення інформаційної безпеки важливим є різноманітні моделі та методи оцінки загроз та небезпек. їх варіативність занадто лабільна та залежить як від рівня розвитку тієї чи іншої цивілізації, так і від контексту оцінки, що проводиться, наявності всебічних даних по факторам загроз, алгоритму ви- рахування коефіцієнта ймовірності настання та розміру негативних наслід- ків. Наявність конкретних даних із цього питання дозволяє досить точно визначити ступінь впливу інформаційної зброї, рівень загроз та небезпек.

Основним методом аналізу інформаційних ризиків є кількісний та якісний аналіз, факторний аналіз та інші. Мета якісної оцінки ризиків –

ранжувати інформаційні загрози та небезпеки за різними критеріями, сис- тема яких дозволить сформувати ефективну систему впливу на них.

Важливим методом забезпечення інформаційної безпеки є також метод критичних сценаріїв. У зазначених сценаріях аналізуються ситуації, коли уявний супротивник паралізує систему державного управління і, відпо- відно, знижує здатність підтримувати державне управління в межах опти- мальних параметрів. Причому аналіз подій у світі дає всі підстави ствер- джувати, що інформаційні війни стають органічною частиною політики на- ціональної безпеки багатьох розвинених країн.

Також можна зазначити на метод моделювання, за допомогою якого можна проводити навчання з інформаційної безпеки. Позитивний досвід цього є у США, де на базі однієї з відомих корпорацій постійно провадяться оперативно-дослідницькі навчання, щоб моделювати різні форми інформа- ційних атак у ході інформаційної війни.

Серед методів забезпечення інформаційної безпеки важливе значення має метод дихотомії. Для протидії загрозам інформаційній безпеці вжива- ються необхідні заходи як у напрямку надання певного впливу на джерело загрози, так і в напрямку укріплення об’єкта безпеки. Відповідно виділяють дві предметні області протидії. Одна з них утворюється сукупністю джерел загроз, а інша – сукупністю заходів із забезпечення інформаційної безпеки органу державного управління. Вплив на джерело загрози інформаційної безпеки спрямований на зміну чинників та умов, здатних нанести шкоду об’єкту безпеки. Метою захисту є переконання супротивника в недоцільно- сті здійснення загроз. Що стосується органів державного управління, то джерело загроз може бути спрямовано на зміну міждержавних відносин, укріплення довіри між державами, створення умов, за яких здійснення не- безпечних дій щодо об’єкта безпеки стає невигідним унаслідок виникнення небажаних наслідків або неможливим. Основним предметом за такого ви- падку є інформація, яка є у супротивника у вигляді відомостей, знань, оці- нок. У свою чергу, інформація, що надходить від супротивника і становить собою загрозу, може бути піддана впливу для зміни її здатності завдавати шкоду, нейтралізації, трансформації або ліквідації її небезпечних властиво- стей. Вплив на інформаційну інфраструктуру важливий у тому випадку, коли загрозу може становити середовище поширення небезпечної інформа- ції.

Методи впливу на інформацію у формі повідомлень можна поділити

також на електронні та неелектронні.

Електронні методи впливу застосовуються в тих випадках, коли пові- домлення закріплюються на електромагнітних носіях, що призначені для оброблення за допомогою засобів обчислювальної техніки. Вони поляга- ють у знищенні, викривленні, копіюванні повідомлень, які зберігаються на

цих пристроях. Такі дії можуть бути вчинені лише за допомогою технічного та програмного забезпечення.

Неелектронні методи за своєю суттю мають той самий зміст, але реа- лізуються без використання засобів обчислювальної техніки для впливу на повідомлення, закріплення на інших, передусім паперових, носіях інформа- ції.

# Питання для самоконтролю

1. Надайте визначення поняття «забезпечення інформаційної безпеки держави».
2. Охарактеризуйте основні принципи забезпечення інформаційної безпеки держави.
3. Що таке превентивність?
4. Як можна тлумачити поняття адекватної інформованості?
5. Що таке інформаційний патронат?
6. Що таке інформаційна кооперація?
7. Дати визначення поняття «інформаційне протиборство».
8. Які існують способи забезпечення інформаційної безпеки для кон- кретної особи?
9. Які існують методи забезпечення інформаційної безпеки та методи впливу на інформацію?
10. Надайте характеристику рівням сфери інформаційної безпеки.

# Розділ 5. ІНФОРМАЦІЙНЕ ПРОТИБОРСТВО МІЖ КРАЇНАМИ. ІНФОРМАЦІЙНА ВІЙНА

* 1. Основні форми інформаційного протиборства.
  2. Інформаційна війна та її завдання.
  3. Концепція інформаційної війни.
  4. Органи інформаційної війни.
  5. Основні форми інформаційної війни.

# Основні форми інформаційного протиборства

***Інформаційне протиборство*** – суперництво соціальних систем (країн, блоків країн) в інформаційній сфері щодо впливу на ті або інші сфери соціальних відносин і встановлення контролю над джерелами стра- тегічних ресурсів, у результаті якого одна група учасників суперництва отримує переваги, необхідні їм для подальшого розвитку.

Інформаційне протиборство в наукових колах також розрізняють у широкому й вузькому розумінні.

Інформаційне протиборство (у широкому розумінні) – це форма боро- тьби, що становить сукупність спеціальних (політичних, економічних,

дипломатичних, технологічних, військових та інших) методів, способів і за- собів вигідного впливу на інформаційну сферу об’єкта зацікавленості та за- хисту власної інформаційної сфери в інтересах досягнення поставлених ці- лей.

Інформаційне протиборство (у вузькому розумінні – у військовій, обо- ронній сферах) – це комплекс заходів інформаційного характеру, здійсню- ваних з метою захоплення й утримання стратегічної ініціативи, досягнення інформаційної переваги над противником і створення сприятливого пропа- гандистського підґрунтя при підготовці й веденні бойової й іншої діяльно- сті збройних сил.

***Види інформаційного протиборства***: інформаційно-технічне й ін- формаційно-психологічне. Головними об’єктами впливу інформаційно-те- хнічного протиборства є системи телекомунікації і зв’язку, радіоелектронні засоби тощо. Об’єктом інформаційно-психологічного протиборства зали- шаються свідомість і психіка населення й особового складу збройних сил, спецслужб противника та системи формування суспільної думки і прий- няття стратегічних рішень.

Концепція інформаційного протиборства передбачає його ведення на воєнному та державному рівнях. На державному рівні метою інформацій- ного протиборства є послаблення позицій конкуруючих держав, підрив їх- ніх національно-державних основ, порушення системи національного уп- равління за рахунок інформаційного впливу на політичну, дипломатичну, економічну та соціальну сфери життєдіяльності країни, проведення психо- логічних операцій, підривних та інших деморалізуючих пропагандистських акцій. Воно спрямовано на забезпечення національних інтересів держави, упередження міжнародних конфліктів, терористичних акцій, забезпечення інформаційної безпеки країни та розглядається як вид стратегічного проти- борства країн.

За інтенсивністю, масштабами та засобами, які використовуються, ви- діляють такі ступені інформаційного протиборства: інформаційна експан-

сія, інформаційна агресія та інформаційна війна.

*Інформаційна експансія* – діяльність із досягнення національних інте- ресів методом безконфліктного проникнення в інформаційну сферу з ме- тою: поступової, плавної, непомітної для суспільства зміни системи соціа- льних відносин за зразком системи джерела експансії; витіснення положень національної ідеології і національної системи цінностей і заміщення їхніми власними цінностями й ідеологічними установками; збільшення ступеня свого впливу та присутності, встановлення контролю над стратегічними ін- формаційними ресурсами, інформаційно-телекомунікаційною структурою і національними ЗМІ; нарощування присутності власних ЗМІ в інформацій- ній сфері об’єкта проникнення і т. ін.

*Інформаційна агресія* – незаконні дії однієї зі сторін в інформаційній сфері, спрямовані на нанесення супротивнику конкретної, відчутної шкоди в окремих областях його діяльності шляхом обмеженого та локального по своїх масштабах застосування сили.

Ознаки інформаційної агресії: виключення із засобів інформаційної дії самих небезпечних видів, що не дозволяють надійно контролювати роз- міри, завданого збитку; обмеження розмірів простору, об’єктів інформацій- ної інфраструктури та соціальних груп, що піддаються ураженню інформа- ційною дією (агресія зачіпає інформаційний простір держави не цілком, а тільки його частину); обмеження за метою (переслідує локальну, приватну мету) і часу (зазвичай агресія припиняється після повного досягнення агре- сором усієї поставленої конкретної мети й рідко набуває затяжного харак- теру), а також по силах і засобах, що залучаються.

# Інформаційна війна та її завдання

*Інформаційна війна* – найвищий ступінь інформаційного протиборс- тва, спрямований на розв’язання суспільно-політичних, ідеологічних, а та- кож національних, територіальних та інших конфліктів між державами, на- ціями, класами й соціальними групами шляхом широкомасштабної реаліза- ції народами, засобів і методів інформаційного насильства (інформаційної зброї). Можна вважати, що в інформаційній сфері агресія переростає у війну в тому випадку, якщо одна зі сторін конфлікту починає широко за- стосовувати проти своїх супротивників інформаційну зброю. Цей критерій дозволяє виділити з усього різноманіття процесів і явищ, що відбуваються в інформаційному суспільстві, такі, які становлять для його нормального (мирного) розвитку найбільшу небезпеку. Нині відсутні міжнародні та на- ціональні правові норми, які дозволяють у мирний час (за відсутності офі- ційного оголошення війни з боку агресора) юридично кваліфікувати ворожі дії іноземної держави в інформаційній сфері, що супроводжуються нане- сенням збитку інформаційній або іншій безпеці країни, як акції інформа- ційної агресії або інформаційної війни. Крім того, відсутні чіткі, однозна- чні, закріплені юридично критерії оцінки отриманого в результаті інформа- ційної агресії або інформаційної війни матеріального, морального, іншого збитку. Це дозволяє в мирний час активно використовувати самий небезпе- чний і агресивний арсенал сил і засобів інформаційної війни – як основний засіб досягнення політичної мети.

Інформаційна війна ведеться не тільки у фізичному просторі, де пере-

бувають фізичні інформаційні системи і засоби, але й у деякій віртуальній зоні (віртуальному або кібернетичному просторі). Інформаційна війна роз- ширює простір ведення війн, глибинами у світовому океані.

До особливостей інформаційної війни відноситься те, що вона ве- деться як під час фактичних бойових дій, так і у мирний час і у кризових

ситуаціях без офіційного оголошення. Початок інформаційної війни немо- жливо визначити однозначно. В інформаційній війні відсутня лінія фронту; проведення противником операцій інформаційної війни практично немож- ливо виявити, а якщо факти проведення таких операцій виявляються, то вони залишаються анонімними.

Будь-які міжнародні юридичні й моральні норми ведення інформацій- ної війни відсутні. Та чи інша країна може стати об’єктом інформаційної дії, не знаючи про це. Невисока вартість технічних засобів, які можуть бути використані в інформаційній війні, суттєво розширюють коло можливих її учасників. Ними можуть бути окремі країни та їхні органи розвідки, зло- чинні, терористичні й наркобізнесові угруповання, комерційні фірми і на- віть особи, які діють без злочинних намірів.

# Завданнями інформаційної війни є:

* створення атмосфери бездуховності, негативного ставлення до ку- льтури та історичної спадщини в суспільстві конкурента чи ворога;
* маніпулювання громадською думкою й політичною орієнтацією на-

селення держави з метою створення політичного напруження та стану, бли- зького до хаосу;

* дестабілізація політичних відносин між партіями, об’єднаннями й

рухами для розпалення конфліктів, стимулювання недовіри, підозри, заго- стрення ворожнечі, боротьби за владу;

- провокування та застосування репресій із боку влади щодо опозиції;

* зниження рівня інформаційного забезпечення органів влади й уп- равління, інспірація помилкових управлінських рішень;
* уведення населення в оману щодо роботи державних органів влади, підрив їхнього авторитету, дискредитація їхніх дій.

# Концепція інформаційної війни

***Концепція інформаційної війни*** – це система поглядів на інформа- ційну війну та шляхи її ведення.

За останніми оцінками, концепція інформаційної війни повинна пе- редбачати:

* + - заглушення (у воєнний час) елементів інфраструктури державного і воєнного управління (ураження центрів командування й управління);
    - електромагнітний вплив на елементи інформаційних і телекомуніка- ційних систем (радіоелектронна боротьба);
    - одержання розвідувальної інформації шляхом перехоплення і деко- дування (дешифрування) інформаційних потоків, що передаються кана- лами зв’язку, а також побічним випромінюванням і за рахунок спеціально впроваджених у приміщення технічних засобів і електронних пристроїв пе- рехоплення інформації (радіоелектронна розвідка);
    - здійснення несанкціонованого доступу до інформаційних ресурсів (шляхом використання програмно-апаратних засобів зламу систем захисту інформаційних і телекомунікаційних мереж противника) із наступним їх- нім спотворенням, знищенням або викраденням чи порушенням нормаль- ного функціонування цих систем (так звана «хакерна війна»);
    - формування й масове поширення інформаційними каналами проти- вника або глобальними мережами інформаційної взаємодії дезінформації або тенденційної інформації для впливу на оцінки, наміри й орієнтацію на- селення та осіб, що приймають рішення (психологічна війна);
    - одержання необхідної інформації шляхом перехоплення й обробки відкритої інформації, що передається незахищеними каналами зв’язку або циркулює в інформаційних системах, а також опублікованої в засобах ма- сової інформації.

# Органи інформаційної війни

***Органи інформаційної війни*** – це органи керування інформаційною війною та люди (фахівці, офіцери, підрозділи) для її ведення.

До органів інформаційної війни можуть належати: органи плану- вання й координації з питань інформаційної війни, які розробляють системи планування діяльності з усіх питань, що пов’язані з інформаційною війною; органи стратегічного рівня з відслідковування ознак початку інформаційної війни, які збирають і аналізують розвідувальну інформацію, визнають ознаки початку інформаційних атак (акцій); органи проведення операцій із захисту від інформаційної зброї, які здійснюють попередження про інфор- маційні атаки тактичного рівня і займаються ліквідацією наслідків інфор- маційного нападу; підрозділи розробки конструкцій та архітектури авто- матизованих систем управління, що здійснюють розробку єдиної архітек- тури й технічних стандартів у галузі засобів і систем захисту від інформа- ційної зброї; групи незалежних експертів, що здійснюють аналіз уразливо- сті АСУ, у тому числі через здійснення експериментальних атак на АСУ та їхні окремі елементи.

# Основні форми інформаційної війни

Усі форми інформаційної війни зводяться до впливу на інформаційну інфраструктуру противника, його інформаційні системи та інформаційні ресурси із проведенням будь-яких дій, що мають за мету спотворення інфо- рмації, що він одержує, позбавлення його можливостей одержання нової інформації або фізичне знищення його інформаційних засобів, а також до захисту інформації власних збройних сил від аналогічних дій противника. Спеціалісти пропонують ведення інформаційної війни на державному та воєнному рівнях. Якщо в мирний час метою інформаційної війни на держа- вному рівні є схилення воєнно-політичного керівництва противника до

прийняття вигідних для протилежної сторони рішень, то у воєнний час – повний параліч інформаційної інфраструктури противника при забезпе- ченні стійкого функціонування своєї. У цьому випадку на державному рівні основне завдання інформаційної війни полягає в забезпеченні гарантованої безпеки та стійкості національної інформаційної інфраструктури держави, намаганні завоювання інформаційної переваги над противником.

*На державному рівні інформаційна війна* ведеться з використанням політичних, дипломатичних, економічних, інформаційно-психологічних, інформаційно-технічних і воєнних способів.

Основною формою інформаційної війни на державному рівні є спеці- альна інформаційна операція, яка може носити одночасно і наступальний, і оборонний характер, відповідає передбаченій мірі ризику та очікуваному потенційному ефекту, спрямована на забезпечення національних інтересів і національної безпеки держави. Операції цього типу можуть проводитися проти будь-яких держав, у тому числі й тих, що не є потенційними против- никами. Визначення мети операції, завдань, часу та місця проведення пот- ребує безпосереднього затвердження воєнно-політичним керівництвом держави.

Для погодження запланованих дій і заходів у галузі інформаційного протиборства при керівництві державою створюють спеціальний міжвідо- мчий орган із забезпечення інформаційної безпеки та об’єднаний центр ін- формаційних операцій.

Їхніми завданнями є:

* організація цілеспрямованого інформаційно-психологічного впливу на воєнно-політичне керівництво союзних держав та держав, що є потенцій- ними противниками;
* розробка єдиної національної стратегії ведення інформаційної війни;
* координація дій усіх органів, сил та засобів, що беруть участь у інформа- ційній війні;
* організація та проведення спеціальної інформаційної операції.

*На воєнному рівні інформаційна війна* планується вестись всебічно за- безпеченими силами та засобами, що виділяються для боротьби із силами бойового управління противника. Метою даної боротьби є «обезголов- лення» противника, позбавлення його надійної системи управління, захоп- лення ініціативи та примус противника реагувати на ситуацію, що склалася, бажаним для командування чином при забезпеченні високої стійкості, без- перервності та оперативності функціонування своїх систем управління вій- ськами (силами).

Інформаційна війна на воєнному рівні ведеться на основі викорис- тання інформаційно-насичених засобів розвідки, зв’язку, автоматизації, ра- діоелектронної та психологічної війни, високоточної зброї та звичайних за- собів ураження, а також із застосуванням спеціально створеної

інформаційної зброї, проведення комп’ютерних атак та захисту своїх комп’ютерних мереж.

Для ведення інформаційної війни у збройних силах створюються спе- ціальні бойові формування та органи управління ними. Цим формуванням приписується виконання таких функцій: підготовка й забезпечення плану- вання інформаційних дій, координація зусиль у ході інформаційної опера- ції; здійснення доступу до інформації противника та досягнення контролю над нею; використання у випадку необхідності інформаційної зброї, участь в операціях із введення воєнно-політичного керівництва в оману; приду- шення або дезорганізація частини інформаційної інфраструктури против- ника з одночасним надійним захистом аналогічної структури своїх зброй- них сил та держави.

Основними формами інформаційної війни на воєнному рівні (ведення боротьби із системами бойового управління противника) є *наступальні та оборонні інформаційні операції.*

*Наступальна інформаційна операція* має за мету завоювання інфор- маційної переваги над противником. У цій операції головні зусилля спря- мовуються на дезорганізацію його систем управління військами і зброєю, а частина сил та засобів забезпечують стійкість власного управління. При цьому всі заходи, які проводяться в межах інформаційної боротьби, повинні забезпечувати сприятливі умови для бойових дій своїх військ (сил).

*Оборонна інформаційна операція* проводиться в умовах великої інфо- рмаційної переваги противника і має за мету зниження цієї переваги. У та- кій операції головні зусилля сил і засобів спрямовуються на забезпечення інформаційної безпеки органів управління об’єднань і з’єднань, на захист інформації в системах керування. Частина сил і засобів спрямовуються на дезорганізацію управління військами і зброєю противника. Інформаційні операції повинні проводитися в умовах комплексного, погодженого в часі використання сил та засобів, які залучаються для боротьби із системами бо- йового управління противника: оперативної безпеки, радіоелектронної війни, воєнної дезінформації, психологічної війни, комп’ютерної атаки та захисту мереж та фізичного знищення.

Наступальні та оборонні операції можуть вестися одночасно або пос-

лідовно як у мирний, так і у воєнний час.

*За контекстом оперативна безпека* являє собою не бажаний стан, а комплекс заходів із виявлення критичної інформації, проведення аналізу дій своїх збройних сил із метою:

* виявлення демаскуючих ознак своїх військ (сил) і критичних елеме- нтів інформації, яка могла стати відомою противникові;
* вибору заходів, які зменшують уразливість своїх збройних сил та збройних сил союзників; протидії всім видам розвідки противника.

Крім цього оперативна безпека включає в себе: інформаційну без- пеку; безпеку систем управління, зв’язку та автоматизації; безпеку об’єктів і бойової техніки; фізичну безпеку особового складу.

***Радіоелектронна війна*** включає комплекс заходів із застосуванням засобів електромагнітного випромінювання, спрямованих на зменшення ефективності або запобігання застосування противником електромагніт- ного спектра, а також на забезпечення ефективного використання електро- магнітного спектра своїми військами.

Радіоелектронна війна є основоположним елементом впливу як на си- стеми управління противника в оперативній і тактичній ланках, так і зага- лом на інформаційну інфраструктуру противника. Вона включає три осно- вних елементи:

* радіоелектронне забезпечення;
* радіоелектронна атака;
* боротьба з електронною протидією або радіоелектронна контрпротидія.

***Радіоелектронне забезпечення*** передбачає проведення заходів по- шуку, перехоплення випромінювання в електромагнітному спектрі та ви- значення місцеположення джерел випромінювання для оцінки ступеню мо- жливої загрози і прийняття рішення командирами всіх рангів, а також ви- конання додаткових функцій, таких як ухилення від загрози з боку против- ника і високоточна цілевказівка системам озброєння.

***Радіоелектронна атака*** передбачає активний вплив на радіоелект- ронні засоби противника. За видом впливу атаки поділяється на два компо- ненти: неруйнівні впливи, які включають електронне придушення й елект- ронну дезінформацію; руйнівні впливи на основі застосування протира- діолокаційних ракет, зброї спрямованої енергії (лазерної, надвисокочасто- тної) і т. ін.

***Радіоелектронна контрпротидія*** являє собою сукупність заходів, спрямованих на підвищення живучості та зменшення втрат своїх сил і за- собів від впливу керованої зброї і засобів радіоелектронної протидії проти- вника. Необхідні умови для досягнення інформаційної переваги Інформа- ційна перевага є одним із центральних понять у сфері інформаційного про- тиборства. Воно являє собою здатність складної саморегулюючої системи управління та інформаційного забезпечення держави або воєнного відомс- тва забезпечити стійкий безперервний процес своєчасного одержання дос- товірної інформації та доведення її до відповідних споживачів при одноча- сному отриманні можливості використання у своїх інтересах такої ж сис- теми ймовірного противника або пониження ефективності роботи (виве- дення з ладу) останньої. При цьому під саморегулюючою системою розу- міють особовий склад та компоненти збирання, обробки, аналізу, кореляції, зберігання в пам’яті ЕОМ, відображення на дисплеях, запису на магнітних та інших носіях інформації, систематичного своєчасного оновлення та

уточнення, розподілу за мірою пріоритетності, передавання інформації спо- живачам та здійснення іншого впливу на інформацію.

# Питання для самоконтролю

1. Дайте визначення поняття «інформаційне протиборство».
2. Визначить рівні проведення інформаційного протиборства.
3. Які відокремлюють основні ступені інформаційного протиборства?
4. Що відноситься до органів інформаційної війни?
5. Охарактеризуйте основні форми інформаційної війни.
6. Що являє собою оперативна безпека?

# Розділ 6. ІНФОРМАЦІЙНА ЗБРОЯ В ІНФОРМАЦІЙНІЙ ВІЙНІ

* 1. Інформаційна зброя та сфера її застосування.
  2. Основні об’єкти застосування інформаційної зброї.
  3. Види інформаційної зброї.

1. 4. Особливості застосування інформаційної зброї.

# Інформаційна зброя в інформаційній війні

***До інформаційної зброї відноситься*** широкий клас засобів і способів інформаційного впливу на противника: від дезінформації і пропаганди до засобів радіоелектронної боротьби.

Інформаційну зброю від звичайних засобів ураження відрізняє:

1. скритність – можливість досягнення мети без видимої підготовки та ого- лошення війни;
2. масштабність – можливість наносити непоправні збитки не визначаючи державних кордонів і суверенітетів, без звичного обмеження простору в усіх середовищах життєдіяльності людини;
3. універсальність – можливість багатоваріантного використання як воєн- ними, так і цивільними структурами країни, що нападає, як проти воєнних, так і цивільних об’єктів країни ураження.

Сфера застосування інформаційної зброї включає як воєнну галузь, так і економічну, банківську, соціальну та інші галузі потенційного вико- ристання з метою: дезорганізації діяльності управлінських структур, тран- спортних потоків та засобів комунікації; блокування діяльності окремих підприємств та банків, а також цільових галузей промисловості шляхом порушення багатоланкових технологічних зв’язків та системи взаєморозра- хунків, проведення валютно-фінансових махінацій і т. ін.; ініціювання ве- ликих техногенних катастроф на території противника в результаті пору- шення штатного управління технологічними процесами та об’єктами, які мають справу із значними кількостями небезпечних речовин та високими концентраціями енергії; масового розповсюдження та впровадження

у свідомість людей певних уявлень, звичок та поведінкових стереотипів; виклику невдоволення або паніки серед населення, а також провокування деструктивних дій різноманітних соціальних груп.

# Основні об’єкти застосування інформаційної зброї

*Основними об’єктами застосування інформаційної зброї* як к у мир- ний, так і у воєнний періоди можуть виступати:

* + - комп’ютерні та телекомунікаційні системи, які використовуються державними організаціями при виконанні своїх управлінських функцій;
    - воєнна інформаційна інфраструктура, яка виконує завдання управ- ління військами та бойовими засобами збирання та обробки інформації в інтересах збройних сил;
    - інформаційні та управлінські структури банків, транспортних та промислових підприємств;
    - засоби масової інформації, і передусім електронні (радіо, телеба- чення і т. ін.).

# Види інформаційної зброї

Існують різні критерії поділу інформаційної зброї.

За галузями застосування інформаційну зброю можна розділити на *ін- формаційну зброю воєнного та невоєнного (загального) застосування*. Ін- формаційна зброя, застосування якої можливе у воєнних умовах (радіоеле- ктронна боротьба), включає в себе засоби з такими функціями:

* + - ураження звичайними боєприпасами за цілевказівками засобів ра- діо- та радіотехнічної розвідки з частковим самонаведенням на кінцевій ді- лянці;
    - ураження високоточними боєприпасами нового покоління – інте- лектуальними боєприпасами із самостійним пошуком цілі та самонаведен-

ням на її вразливі елементи; радіопридушення засобів зв’язку маскуваль- ними завадами;

* + - створення завад імітації, які ускладнюють входження у зв’язок, си- нхронізацію в каналах передавання даних, що ініціюють функції переза- питу та дублювання повідомлень;
    - придушення за допомогою засобів силової радіоелектронної боро- тьби (за допомогою потужного електромагнітного випромінювання, яке створює завади за рахунок паразитних каналів прийому);
    - силовий вплив імпульсом високої напруги через мережі живлення;
    - порушення властивостей середовища розповсюдження радіохвиль;
    - за допомогою спеціальних методів впливу на системи зв’язку;
    - засоби генерації природної мови конкретної людини.

*Особливу небезпеку інформаційна зброя представляє сьогодні для ін- формаційних комп’ютерних систем* органів державної влади, управління

військами та зброєю, фінансами та банками, економікою держави, а також для людей при інформаційно-психологічному впливі на них з метою зміни та управління їхньою індивідуальною та колективною поведінкою. При цьому за своєю результативністю інформаційна зброя прирівнюється до зброї масового ураження.

До інформаційної зброї, застосування якої можливе як у воєнний, так і у мирний час, можуть бути віднесені засоби ураження інформаційних комп’ютерних систем та засоби ураження людей (їхньої психіки).

*Засоби ураження інформаційних комп’ютерних систем* являють со- бою сукупність спеціально організованої інформації та інформаційних тех- нологій, яка дозволяє цілеспрямовано змінювати (знищувати, спотворю- вати), копіювати, блокувати інформацію, долати системи захисту, обмежу- вати допуск законних користувачів, здійснювати дезінформацію, порушу- вати функціонування носіїв інформації, дезорганізовувати роботу техніч- них засобів комп’ютерних систем та інформаційно-обчислювальних ме- реж, що застосовується в ході інформаційної війни (боротьби) для досяг- нення поставлених цілей.

За метою використання така інформаційна зброя поділяється на *ін- формаційну зброю атаки та інформаційну зброю забезпечення*.

***Інформаційна зброя атаки*** – це інформаційна зброя, за допомогою якої здійснюється вплив на інформацію, що зберігається, обробляється й передається в інформаційно-обчислювальних мережах (ІОМ) і (або) пору- шуються інформаційні технології, що застосовуються в ІОМ. У складі ін- формаційної зброї атаки виділяють чотири основних види засобів інформа- ційних впливів:

засоби порушення конфіденційності інформації; засоби порушення цілісності інформації;

засоби порушення доступності інформації; засоби психологічного впливу на абонентів ІОМ.

Застосування інформаційної зброї атаки спрямоване на зрив вико- нання ІОМ цільових завдань.

***Інформаційна зброя забезпечення*** – це інформаційна зброя, за допо- могою якої здійснюється вплив на засоби захисту інформації об’єкта атаки, наприклад, інформаційно-обчислювальну систему.

До складу інформаційної зброї забезпечення входять засоби комп’ютерної розвідки та засоби подолання системи захисту інформаційно- обчислювальної системи. Успішне застосування інформаційної зброї забез- печення дозволяє здійснювати деструктивні впливи на інформацію, що збе- рігається, обробляється й передається в мережах обміну інформацією, з ви- користанням інформаційної зброї атаки.

За способом реалізації інформаційну зброю поділяють на три великих класи: 1) інформаційна алгоритмічна (математична) зброя; 2) інформаційна програмна зброя; 3) інформаційна апаратна зброя.

*Інформаційна алгоритмічна (математична) зброя* – це вид інформа- ційної зброї до якої, зазвичай, відносять: алгоритми, що використовують сполучення санкціонованих дій для здійснення несанкціонованого доступу до інформаційних ресурсів; алгоритми застосування санкціонованого (ле- гального) програмного забезпечення і програмні засоби несанкціонованого доступу для здійснення незаконного доступу до інформаційних ресурсів.

*До інформаційної програмної зброї* відносять програми з потенційно небезпечними наслідками своєї роботи для інформаційних ресурсів мережі обміну інформацією.

Програми з потенційно небезпечними наслідками – це окремі про- грами (набори інструкцій) які мають спроможність виконувати будь-яку не- пусту множину таких функцій: приховування ознак своєї присутності в програмно-апаратному середовищі  мережі обміну інформацією; здат- ність до самодублювання, асоціювання себе з іншими програмами і (або) перенесення своїх фрагментів в інші ділянки оперативної або зовнішньої пам’яті; руйнування (спотворення довільним чином) кодів програм в опе- ративній пам’яті; збереження фрагментів інформації з оперативної пам’яті в деякій ділянці  зовнішньої пам’яті прямого доступу (локальної або від- даленої); спотворення довільним чином, блокування і (або) підміна масивів інформації, що виводиться у зовнішню пам’ять або в канал зв’язку, утворе- них у результаті роботи прикладних програм, або масивів даних, що уже містяться у зовнішній пам’яті; придушення інформаційного обміну в теле- комунікаційних мережах, фальсифікування інформації в каналах держав- ного й воєнного управління; нейтралізація роботи тестових програм і сис- тем захисту інформаційних ресурсів.

Програми з потенційно небезпечними наслідками умовно поділяють на такі класи: (бойові) комп’ютерні віруси; засоби несанкціонованого до-

ступу; програмні закладки.

***Комп’ютерні віруси*** (від лат. virus – «отрута»)] – це спеціальні про- грами, які здатні самочинно розмножуватися, створюючи свої копії, і по- ширюватися, модифікуючи (заражаючи) інші програми шляхом приєд- нання до них для наступного одержання управління та відтворення нових копій.

Після запуску заражених програм вірус може виконувати різні неба- жані дії, що порушують цілісність інформації та (або) режим роботи засобів обчислювальної техніки: псування файлів та каталогів; модифікування програмного забезпечення; спотворення результатів обчислень; засмічу- вання або стирання пам’яті; створення завад при роботі комп’ютера, на- приклад, різних аудіо- та відеоефектів.

Комп’ютерні віруси можуть розмножуватися, впроваджуватися в про- грами, передаватися лініями зв’язку, мережами обміну інформацією, виво- дити з ладу системи керування і т. ін.

***Засоби несанкціонованого доступу*** відносяться до класу програм із потенційно небезпечними наслідками, для яких обов’язковим є виконання таких функцій: руйнування або зміна кодів програм в оперативній пам’яті; нейтралізація роботи тестових програм і систем захисту інфор- маційних ресурсів. До засобів несанкціонованого доступу відноситься будь-яке позаштатне програмне забезпечення, яке противник може викори- стати для порушення цілісності операційної системи або обчислювального середовища. Часто цей тип програмного забезпечення використовується для аналізу систем захисту з метою їхнього подолання й реалізації несанк- ціонованого доступу до інформаційних ресурсів мереж обміну інформа- цією. Відмінною ознакою (відносно програмних закладок) засобів несанк- ціонованого доступу є наявність функцій подолання захисту.

***Програмні закладки.*** Відмінною ознакою є відсутність функцій подо- лання захисту. Виділяють декілька видів програмних закладок:

* троянські програми;
* логічні бомби;
* логічні люки;
* програмні пастки;
* програмні черв’яки.

***Інформаційна апаратна зброя*** включає апаратні засоби, призначені для виконання функцій інформаційної зброї. Прикладом інформаційної апаратної зброї можуть бути апаратні закладки, які впроваджуються в ПК, що готуються на експорт, та їхнє периферійне обладнання. Апаратні закла- дки маскуються під звичайні пристрої мікроелектроніки й застосовуються для збирання, обробки та передавання конфіденційної інформації. Інфор- маційна зброя, що відноситься до різних класів, може застосовуватися спі- льно, а також деякі види інформаційної зброї можуть мати риси декількох класів.

***Засоби ураження (впливу) на людей та їхню психіку*** розрізняють залежно від мети їхнього застосування в психологічній війні. До таких ці- лей зазвичай відносять: створення інформації, яку одержує політичне кері- вництво, командування та особовий склад збройних сил противника, та нав’язування їм фальшивої або беззмістовної інформації; психологічна об- робка військ та населення; ідеологічні диверсії та дезінформування; орга- нізація масових демонстрацій під фальшивими лозунгами; пропаганда та розповсюдження фальшивих чуток; змінювання та керування індивідуаль- ною та колективною поведінкою.

Поряд із використанням традиційних засобів (друковані та електронні засоби масової інформації) йде активна розробка та апробація спеціальних

засобів впливу на людину як через ЗМІ, так і через комп’ютерні мережі: засоби інформаційно-психологічного впливу, психогенного впливу, психо- аналітичного впливу, нейролінгвістичного впливу, психотронного впливу та психотропного впливу.

# Особливості застосування інформаційної зброї

*До особливостей застосування інформаційної зброї відносяться:*

* низька вартість – на відміну від традиційних воєнних технологій, розробка інформаційної зброї не потребує значних фінансових ресурсів – достатньо мати досвід роботи в інформаційних системах і доступ у глобальні та ві- домчі мережі;
* відсутність традиційних кордонів – відмінності між суспільним і особис- тим, воєнною і кримінальною поведінкою, а також географічні кордони, які історично складалися між націями, розмиваються зростаючою взаємо- пов’язаністю інформаційних інфраструктур;
* нові можливості для керування суспільною думкою – сучасні інформа- ційні технології надають широкі можливості для маніпулювання свідомі- стю людей і ускладнюють державі роботу з політичної підтримки ініціатив у галузі забезпечення безпеки;
* нові завдання перед органами розвідки – неправильне розуміння ролі, мо- жливостей і цілей інформаційної зброї знижує ефективність традиційної ро- звідувальної діяльності;
* необхідні нові форми розвідки, що концентруються на інформаційній стратегічній зброї;
* складність оцінки загроз і формування системи попередження – нині ще немає систем попередження, які дозволили б їй відрізнити стратегічну атаку з використанням інформаційної зброї від інших форм діяльності в ін- формаційному просторі, включаючи шпигунство й випадкові помилки;
* труднощі при створенні й підтримці коаліцій – коаліції тільки збільшують уразливість їхніх учасників від інформаційної поразки;
* вразливість власних територій – оскільки інформаційні технології не об- межені в географічному плані, то інформаційною зброєю можуть уража- тися цілі як на віддаленому театрі воєнних дій, так і всередині країни.

# Питання для самоконтролю

* 1. Яким чином відрізняється інформаційна зброя від звичайних засобів ураження?
  2. Назвіть сферу застосування інформаційної зброї.
  3. Охарактеризуйте основні об’єкти застосування інформаційної зброї.
  4. Що таке комп’ютерні віруси?
  5. Які існують види програмних закладок?
  6. Назвіть та охарактеризуйте засоби несанкціонованого доступу.
  7. Які виділяють особливості застосування інформаційної зброї?

# Розділ 7. ОСНОВИ ТЕОРІЇ ІНФОРМАЦІЙНОЇ БОРОТЬБИ

* + 1. Зміст теорії інформаційної боротьби.
    2. Закони та закономірності інформаційної боротьби.
    3. Принципи інформаційної боротьби.
    4. Заходи інформаційної боротьби.
    5. Способи та форми інформаційної боротьби.

# Зміст теорії інформаційної боротьби

Інформаційна боротьба – це боротьба з використанням спеціальних способів і засобів для впливу на інформаційну сферу (середовище) конфро- нтуючої сторони, а також для захисту власної інформаційної сфери в інте- ресах досягнення поставленої мети.

Інформаційна боротьба може бути як самостійним видом, так і скла- довою частиною будь-якого іншого різновиду боротьби (збройної, ідеоло- гічної, економічної і т. ін.). Вона ведеться постійно як у мирний, так і у во- єнний час. Масштаби інформаційної боротьби настільки великі, що її під- готовка й ведення повинні носити плановий, систематичний характер, за- снований на глибоких знаннях законів і закономірностей інформаційної бо- ротьби.

Метою інформаційної боротьби – є забезпечення необхідного ступеня власної інформаційної безпеки й максимальне зменшення рівня інформа- ційної безпеки конфронтуючої сторони. Досягнення мети інформаційної боротьби здійснюється шляхом вирішення багатьох завдань, основними з яких є ураження об’єктів інформаційної сфери конфронтуючої сторони і захист власної інформації. Мета й завдання інформаційної боротьби визна- чають її зміст, а також і структуру теорії інформаційної боротьби.

На зміст інформаційної боротьби великий вплив справляє багато факто- рів, серед яких виділяють політичний, *економічний, духовний, власне воєн- ний та інформаційний.*

**Політичний фактор** відіграє найважливішу роль у формуванні змісту інформаційної боротьби. Він визначає:

* її мету та завдання;
* причини виникнення та шляхи запобігання;
* способи й особливості ведення;
* розмах та тривалість;
* забезпечення матеріальними та фінансовими ресурсами.

**Економічний фактор** здійснює великий вплив на зміст і розвиток інфо- рмаційної боротьби. Від економіки залежить рівень інформатизації

суспільства та держави, а значить, і ефективність ведення інформаційної боротьби як у мирний, так і у воєнний час. Економічний розвиток на базі науково-технічного прогресу створює необхідні передумови для розробки ефективних способів виконання завдань інформаційної боротьби.

**Воєнний фактор** лежить в основі розвитку інформаційної боротьби. По- ложення воєнної доктрини держави, воєнні концепції протилежної сто- рони, стан та перспективи розвитку засобів інформаційної боротьби, істо- ричний досвід та нагромаджені знання в цій галузі – саме ця база є голов- ною при розробці фундаментальних положень теорії інформаційної боро- тьби та визначенні напрямків її розвитку.

**Інформаційний фактор** нерозривно пов’язаний з інформаційною боро- тьбою, оскільки остання ведеться в інформаційному середовищі та зале- жить від рівня інформатизації сторін. Цей фактор визначає розмах боро- тьби, порядок і способи її ведення, вибір напрямку ударів, структуру сил та засобів, можливості їхнього маневру при проведенні впливу на інформа- ційне середовище противника.

Загальні основи теорії інформаційної боротьби – найважливіші спільні вихідні положення теорії інформаційної боротьби. У загальних основах ви- значаються:

* апарат понять інформаційної боротьби;
* напрямки й методи досліджень інформаційної боротьби;
* тенденції розвитку інформатизації і її роль у різноманітних галузях життя суспільства;
* роль і місце інформаційної боротьби в мирний і воєнний час;
* об’єкт, предмет, цілі, завдання і структура теорії інформаційної боротьби;
* категорії, закони, закономірності та принципи інформаційної боротьби.

Оскільки основними завданнями інформаційної боротьби є ураження об’єктів інформаційного середовища противника та захист власної інфор- мації, то структура теорії інформаційної боротьби повинна включати:

* теорію ураження інформації,
* теорію захисту інформації,
* теорія сил і засобів ураження інформації.

***Теорія ураження інформації*** як складова частина теорії інформацій- ної боротьби включає загальні положення й теорію сил і засобів ураження інформації. Загальні положення визначають предмет, завдання і зміст теорії ураження інформації, форми та способи ураження інформації, основні фа- ктори, що впливають на зміст і ефективність ураження інформації.

***Теорія сил і засобів ураження інформації*** визначає та вивчає показ- ники оцінки ефективності ураження інформації, математичну модель ура- ження інформації, стан підготовки і вирішення завдань ураження інформа- ції.

***Теорія захисту інформації*** включає загальні положення, що визнача- ють: предмет, завдання і зміст теорії; об’єкти і елементи захисту інформа- ції; основні фактори, що впливають на зміст і ефективність захисту інфор- мації, а також визначає та вивчає загрози інформації й методологічні ос- нови її захисту, систему показників оцінки ефективності захисту інформа- ції, загальну математичну модель захисту інформації, організаційно-техні- чні і правові основи захисту інформації.

# Закони та закономірності інформаційної боротьби

Закони інформаційної боротьби визначаються як суттєві, необхідні ві- дношення, що характеризують впорядкованість будови і функціонування, тенденції зміни й розвитку тих чи інших явищ інформаційної боротьби.

Закони інформаційної боротьби являють собою більш менш точне ві- дображення у свідомості людей тих об’єктивних зв’язків і відносин, які іс- нують і діють в інформаційному просторі. Якщо вони пізнані, відображені, описані, то стають основою для практичної діяльності з підготовки і ве- дення інформаційної боротьби.

Особливостями законів (закономірностей) війни, а також інформацій- ної боротьби є наступне:

1. вони проявляються тільки через діяльність людей;
2. мають універсальний характер кількість і якість засобів інформа- ційної боротьби, а також особового складу зумовлюють форми та способи інформаційної боротьби та її ефективність. Винайдення нових засобів ін- формаційної боротьби та їхнє впровадження в практику неминуче призво- дить до виникнення нових форм і способів інформаційної боротьби.

*У сфері інформаційної боротьби можна визначити такі закономір- ності*: обумовленість масштабів та спрямованості характером створення воєнно-політичної та економічної ситуації, а також цілями воєнної полі- тики держави, суспільних та економічних структур, які беруть участь в ін- формаційній боротьбі; відповідність змісту та масштабів створення до ха- рактеру та особливостей суспільного та державного устрою; залежність масштабу та якості створення від матеріальних та духовних можливостей держави (інших суспільних та економічних структур).

# Принципи інформаційної боротьби

Принципи інформаційної боротьби – це науково обґрунтовані поло- ження, правила, рекомендації з підготовки і ведення інформаційної боро- тьби, керівництва її силами й засобами. Вони створюються на основі зако- нів і закономірностей, а також досвіду, набутого в результаті практичної діяльності в галузі інформаційної боротьби. Вони не тільки відображають об’єктивну сутність, але і приписують, як слід діяти в конкретних умовах.

Зміст і масштаби завдань інформаційної боротьби передбачають наявність цілої множини принципів інформаційної боротьби.

## До принципів інформаційної боротьби відносяться:

* принцип відповідності (підпорядкованості) цілей і завдань інформацій- ної боротьби політичним цілям;
* принцип необхідності зосередження сил та засобів інформаційної боро- тьби у вирішальному місці у вирішальний момент;
* принцип завчасної підготовки сил і засобів інформаційної боротьби;
* принцип постійної готовності сил і засобів інформаційної боротьби до захисту власної інформації й до руйнівного впливу на інформаційне се- редовище противника;
* принцип високої активності й рішучості дій;
* принцип узгодженого спільного застосування всіх сил і засобів інформа- ційної боротьби;
* принцип безперервності інформаційної боротьби;
* принцип відповідності (підпорядкованості) цілей і завдань інформацій- ної боротьби політичним цілям;
* принцип необхідності зосередження сил та засобів інформаційної боро- тьби у вирішальному місці у вирішальний момент;
* принцип завчасної підготовки сил і засобів інформаційної боротьби;
* принцип постійної готовності сил і засобів інформаційної боротьби до захисту власної інформації й до руйнівного впливу на інформаційне се- редовище противника;
* принцип високої активності й рішучості дій;
* принцип узгодженого спільного застосування всіх сил і засобів інформа- ційної боротьби;
* принцип безперервності інформаційної боротьби;
* принцип ведення інформаційної боротьби з напруженням, необхідним для вирішення поставлених завдань;
* принцип своєчасного маневру силами й засобами інформаційної боро- тьби;
* принцип раптовості, застосування несподіваних для противника способів виконання завдань;
* принцип врахування духовного фактора в інтересах виконання поставле- них завдань;
* принцип всебічного забезпечення, підтримки боєздатності та своєчасно- сті відновлення сил і засобів інформаційної війни;
* принцип твердості й безперервності управління силами і засобами інфо- рмаційної боротьби, непохитності в досягненні поставленої мети, вико- нанні прийнятих рішень і поставлених завдань.

# Заходи інформаційної боротьби

Інформаційна боротьба включає комплекс заходів інформаційного за- безпечення, інформаційного захисту й інформаційної протидії.

***Інформаційне забезпечення*** в умовах інформаційної боротьби – це комплекс заходів добування інформації про противника в умовах протибор- ства, збирання інформації про свої сили і засоби, обробка інформації й об- мін нею між органами керування з метою організації і ведення бойових дій. Результативність інформаційного забезпечення залежить від багатьох фак- торів і умов, які, зрештою, здійснюють вплив на два основних елементи: інформування органу керування і сприйняття одержаної ним інформації.

***Інформування*** – акт передавання органу керування певної поточної інформації. Залежно від змісту інформації, інформування можна класифі- кувати таким чином:

1. правильне інформування;
2. правильне дезінформування;
3. трансінформування;
4. трансдезінформування.

Види інформування мають певні особливості.

***Правильне інформування*** – це передавання органу керування неспотворе- ної інформації про істинну ситуацію.

***Правильне дезінформування*** – це передавання органу керування неспотво- реної інформації про неправдиву ситуацію.

***Трансінформування*** – це передавання органу керування трансінформації (інформація про істинну ситуацію, трансформована в інформацію про не- правдиву ситуацію).

***Трансдезінформування*** – це передавання органу керування трансдезінфор- мації (інформація про неправдиву ситуацію, перетворена в інформацію про правдиву ситуацію).

*Сприйняття інформації* – процес формування в органі керування уя- влення про ситуацію, включаючи її кількісні та якісні параметри. Найбільш суттєві характеристики при цьому – розпізнавальні ознаки істинних і не- правдивих елементів ситуації. Ступінь відповідності уявлень органу керу- вання про ці характеристики їхнім вихідним величинам створює переду- мови для виникнення різноманітних ситуацій інформаційної боротьби. Ці передумови реалізуються залежно від того, наскільки інформація, що пос- тупає, співвідноситься з образами істинних і неправдивих елементів ситуа- ції, які зберігаються в інформаційному кадастрі.

*Інформаційне рішення* – це одиничний акт сприйняття органом керу- вання поточної інформації про ситуацію та її віднесення до будь-якої відо- мості інформаційного кадастру.

*Інформаційний кадастр* – сукупність відомостей, необхідних для прийняття рішення органом керування. Інформаційний кадастр може мати

вигляд двомірної матриці, стовпці якої відповідають тематичним розділам кадастру, а рядки – їхнім характеристикам. Процес прийняття інформацій- ного рішення передує всім іншим етапам процесу мислення людини або етапам обробки інформації в сучасних інформаційних системах.

***Інформаційна протидія*** – сукупність заходів інформаційної боро- тьби, спрямованих на протидію інформаційному забезпеченню протибор- чої сторони. Вона включає блокування добування, обробки й обміну інфо- рмацією та впровадження дезінформації на всіх етапах інформаційного за- безпечення. Завдання інформаційної протидії вирішуються шляхом маску- вання, контррозвідки, радіоелектронного придушення й руйнування інфор- маційних систем противника.

***Інформаційний захист*** – це сукупність заходів захисту від інформа- ційної протидії противника, які включають дії з деблокування інформації, необхідної для вирішення завдань управління, і блокування дезінформації, що поширюється й упроваджується в систему управління. Він досягається проведенням контрольної розвідки, перевіркою інформації, захистом від вогневого ураження (захоплення) елементів інформаційних систем, а також радіоелектронним захистом. Інформаційний захист підвищує ефективність інформаційного забезпечення в умовах інформаційної протидії противника. **Радіоелектронний захист** – це сукупність заходів забезпечення стій-

кої роботи засобів управління й розвідки в умовах ведення противником радіоелектронної боротьби, застосування розвідувально-ударних комплек- сів, самонавідної зброї та усунення взаємного впливу радіоелектронних за- собів.

# Способи та форми інформаційної боротьби

Способи інформаційної боротьби визначають порядок і прийоми за- стосування сил і засобів інформаційної боротьби для захоплення й утри- мання інформаційної переваги над противником при підготовці і прове- денні бойових дій.

Способи інформаційної боротьби включають:

1. вид і послідовність інформаційних впливів на противника;
2. об’єкти впливу;
3. склад сил і засобів, що виділяються для ведення інформаційної боро- тьби, їхнє оперативне шикування (бойовий порядок).

Усі способи інформаційної боротьби можна поділити на три основні категорії:

1. силові,
2. інтелектуальні,
3. комбіновані.

За аналогією зі збройною боротьбою виділяють дві основні групи спосо- бів:

1. наступальні
2. оборонні.

***Силові способи інформаційної боротьби*** засновані на ураженні об’єктів інформаційної боротьби різноманітними видами зброї (звичайної, радіоелектронної, інформаційної). Застосування силових способів дозволяє досягти інформаційної переваги в кількості інформації, необхідної для ви- рішення завдань управління військами (силами).

***Інтелектуальні способи інформаційної боротьби*** реалізують реф- лексне управління противником. Застосування таких способів дозволяє до- сягти інформаційної переваги в якості інформації, яка використовується для управління військами (силами).

***Комбіновані способи*** інформаційної боротьби забезпечують досяг- нення інформаційної переваги як за кількістю, так і за якістю інформації.

## Наступальні способи інформаційної боротьби реалізують:

* блокування інформації,
* відвернення уваги,
* сковування сил противника,
* вимотування противника,
* інсценування,
* дезінтеграцію,
* замирення,
* залякування противника,
* провокування противника,
* перевантаження противника,
* навіювання на противника і тиск на противника.

***Спосіб блокування інформації*** полягає в тому, що на етапі підготовки й у ході бойових дій шляхом виконання комплексу заходів інформаційної протидії повністю або частково припиняється добування (збирання) інфор- мації про ситуацію й обмін інформацією в системах управління військами і зброєю противника. Для реалізації цього способу застосовується вогневе, радіоелектронне й інформаційне ураження (придушення) елементів систем управління військами (силами) і зброєю противника.

***Спосіб відвернення уваги*** полягає в тому, що на етапі підготовки бо- йових дій шляхом проведення комплексу заходів інформаційної протидії намагаються створити реальну або удавану загрозу для одного з найбільш уразливих місць противника і тим самим переконати його у своїх намірах діяти на одному з можливих напрямів з метою відволікти головні сили про- тивника на вирішення другорядних завдань.

***Спосіб сковування сил противника*** є різновидом способу відвер- нення уваги. При його застосуванні у противника створюється переконання в наявності загрози для одного з уразливих місць, запобігання якій потребує виділення частини сил.

***Спосіб вимотування противника*** полягає в проведенні комплексу заходів інформаційної протидії з метою примусити противника здійсню- вати невигідні й марні дії і, як наслідок, вступити в бій із розтраченими ре- сурсами та зниженою боєздатністю. При цьому можуть проводитися обме- жені бойові або відволікаючі дії.

***Спосіб інсценування*** полягає в тому, що на етапі підготовки до бойо- вих дій противникові нав’язується уява про наявність удаваної загрози для одного з його уразливих місць, запобігання якій не потребує виділення сил та засобів. Це робиться з метою, щоб противник помітив обман і його пи- льність була б приспана. Якщо виникає справжня загроза, він також сприйме її як фальшиву і зможе діяти відповідно до реальної ситуації.

***Спосіб дезінтеграції*** використовується для вирішення політичних за- вдань у міждержавних конфліктах. Реалізація способу полягає в проведенні комплексу заходів інформаційної протидії, що дозволяє нав’язати против- никові уяву про необхідність діяти всупереч коаліційним інтересам. З цією метою може використовуватися дезінформування громадської думки, а та- кож формування фальшивих уявлень про воєнно-політичну ситуацію у го- лів держав, що беруть участь у конфлікті. Крім того, можуть проводитися заходи, які сприяють загостренню реально наявних або штучно створюва- них суперечностей у стані ворога з метою зменшити його воєнну й еконо- мічну могутність.

До форм ведення інформаційної боротьби відносяться: *інформаційна*

*операція, інформаційна битва, інформаційна дія (акція), інформаційний удар.*

***Інформаційна операція*** (від лат. Operatio – «дія») – це сукупність уз- годжених за метою, завданнями, місцем і часом дій (акцій), ударів і битв, що проводяться за єдиним задумом і планом для вирішення завдань інфор- маційної боротьби (завоювання й утримання інформаційної переваги над противником або зниження його інформаційної переваги) на театрі воєнних дій, стратегічному або оперативному напрямах.

Мета інформаційної операції досягається вирішенням таких завдань:

1. інформаційним впливом на противника,
2. інформаційним захистом,
3. ефективним використанням інформаційних ресурсів власного угру- повання військ (сил).

Інформаційна операція поділяється на наступні види:

1. Наступальна інформаційна операція, метою якої є завоювання інформа- ційної переваги над противником.
2. Оборонна інформаційна операція, її мета знизити переваги противника.

***Інформаційна битва*** являє собою сукупність узгоджених і взаємо- пов’язаних за метою, завданнями, місцем і часом інформаційних дій та уда- рів, об’єднаних загальним задумом, які здійснюються спеціально

виділеними силами і засобами та спрямовані для вирішення одного опера- тивного завдання інформаційної боротьби. Залежно від масштабу й виду інформаційної операції в ній може бути одна або декілька інформаційних битв, що здійснюються одночасно або послідовно.

**Інформаційні дії (акції)** – це сукупність узгоджених за метою, за- вданнями, місцем і часом заходів, що проводяться силами і засобами, залу- ченими для ведення інформаційної боротьби, протягом певного часу в пев- ному районі (напрямку). Під час інформаційних дій можуть здійснюватися інформаційні удари. Для ефективного проведення заходів інформаційної боротьби інформаційні впливи на противника необхідно починати ще у ми- рний час, нерідко заздалегідь до початку воєнних (бойових) дій. Такі інфо- рмаційні впливи зазвичай називають інформаційними акціями, оскільки вони виходять за межі власне інформаційної боротьби у сфері інформацій- ного протиборства геополітичних суб’єктів.

Інформаційні дії (акції) можна класифікувати за різними критеріями:

І. За видами:

* 1. наступальні
  2. оборонні

ІІ. За масштабом:

1. стратегічні
2. оперативно-стратегічні
3. оперативні
4. оперативно-тактичні
5. тактичні

ІІІ. За об’єктами впливу:

1. інформаційні системи
2. морально-психологічний стан особового складу та їхня комбінація.

До **наступальних інформаційних дій** *належать інформаційний вплив (інформаційна акція) та інформаційна блокада.*

До **оборонних** – *дії (акції) з інформаційного захисту.*

***Під інформаційним ударом*** розуміють короткочасний потужний уз- годжений інформаційний вплив сил і засобів на найбільш важливий еле- мент (елементи) системи управління (керування) противника для досяг- нення рішучих цілей із завоювання інформаційної переваги (зниження ін- формаційної переваги противника). Інформаційні удари можна класифіку- вати за **масштабом** (*стратегічні, оперативно-стратегічні, оперативні, оперативно-тактичні, тактичні*), **типами** (*радіоелектронні, радіоелект- ронно-вогневі, комп’ютерні, спеціальні й комбіновані*) і **ступенем зосере- дження сил і засобів** (*вибіркові, зосереджено масовані й масовані*).

# Питання для самоконтролю

* 1. Надайте визначення інформаційної боротьби.
  2. В чому полягає мета інформаційної боротьби?
  3. Які фактори впливають на зміст інформаційної боротьби?
  4. Які існують заходи інформаційної боротьби?
  5. Охарактеризувати принципи інформаційної боротьби.
  6. Надайте визначення метода оцінки ефективності інформаційної бо- ротьби.
  7. Які існують форми ведення інформаційної боротьби?
  8. Які існують способи інформаційної боротьби?
  9. Що таке радіоелектронно-вогневий удар?
  10. Формула для обчислення числового значення критерію ефектив- ності інформаційної боротьби.

# Розділ 8. ОСНОВИ БЕЗПЕКИ ІНФОРМАЦІЙНИХ РЕСУРСІВ

* 1. Поняття та загальні властивості інформації. Поняття загроз.
  2. Загрози безпеки інформації та інформаційних ресурсів.
  3. Джерела загроз безпеці інформації.
  4. Класифікація вразливостей безпеки.
  5. Моделі порушень інформаційних ресурсів.

# Поняття та загальні властивості інформації. Поняття загроз.

***Інформація*** – це зафіксоване на носії уявлення про предмети, про- цеси, події, явища та ін. Під фіксацією розуміють закріплення чого-небудь у певному положенні або вигляді. Найпростішим прикладом є письмове за- кріплення відомостей, думок. Інформація для свого функціонування зав- жди вимагає наявності носія. При цьому носієм інформації може виступати поле або речовина, іноді людина.

У процесі інформаційних відносин носії можуть бути або носіями- джерелами, або носіями-одержувачами залежно від напряму переміщення інформації.

Одержувачі сприймають інформацію через той чи інший сенсор (датчик, вимірювальний перетворювач). Процес сприйняття є досить складним. Сприйняття може включати:

* виявлення об’єкта в полі сприйняття;
* розрізнення окремих ознак усередині об’єкта;
* виділення в ньому інформативного змісту, адекватного меті дії;
* формування образу сприйняття.

У Законі України «Про інформацію» під джерелами інформації розу- міються передбачені, або встановлені Законом носії інформації: документи або інші носії інформації, які є матеріальними об’єктами, що зберігають ін- формацію.

Уявлення - це образ та/або суть предмета, процесу, події, природного явища тощо, сприйняті датчиками приладів або безпосередньо органами чуття, а також створені відтворювальною і/або творчою уявою людини чи елементами штучного інтелекту різних пристроїв. При цьому уява – це пси- хічна діяльність, що полягає у створенні уявлень і уявних ситуацій, яка за- галом не сприймалася людиною в реальній дійсності (творча уява) або від- творюють колишні враження і спогади, що спираються на життєвий досвід (відтворювальна уява).

Розрізняють ***відтворювальну й творчу*** уяву, але насправді ці обидва компоненти тісно взаємодіють між собою в процесі створення уявлень.

Інформація має деякі істотні з погляду її захисту властивості. Ці вла- стивості для користувача або власника інформації можна розглядати як де- які бажані стани інформації (носіїв інформації). Такими властивостями є:

* + - конфіденційність – властивість інформації бути захищеною від несан- кціонованого ознайомлення;
    - цілісність – властивість інформації бути захищеною від несанкціонова- ного спотворення, руйнування або знищення;
    - доступність – властивість інформації бути захищеною від несанкціоно- ваного блокування.

# Загрози безпеки інформації та інформаційних ресурсів

Події, які потенційно можуть порушити одну з названих властивостей інформації, відповідно, називають загрозами порушення конфіденційності, цілісності та доступності інформації.

*Загрози порушення конфіденційності* спрямовані на розголошення ін- формації з обмеженим доступом.

*Загрози порушення працездатності (доступності)* спрямовані на створення ситуацій, коли в результаті навмисних дій знижується працезда- тність обчислювальної системи, або її ресурси стають недоступними.

*Загрози порушення цілісності* полягають у спотворенні або зміні неа- вторизованим користувачем інформації, що зберігається або передається. Цілісність інформації може бути порушена як зловмисником, так і в резуль- таті об’єктивних впливів зі сторони середовища експлуатації системи.

Порушення інформаційної безпеки можливе лише у випадках перемі- щення інформації. Наприклад, під час несанкціонованого ознайомлення (читання) документа з паперового носія відбувається переміщення (копію- вання) інформації в мозок людини, яка стає носієм-одержувачем цієї інфо- рмації.

У процесі переміщення інформації може відбуватися зміна її носія. Наприклад, носіями інформації під час її переміщення можуть виступати: матеріальні середовища (повітря, вода, метал та ін.); сенсори або датчики;

перетворювачі та інші об’єкти живої й неживої природи, що виконують фу- нкцію проміжних носіїв інформації.

Загрози конфіденційності спрямовані на заборонене режимом дос- тупу переміщення інформації від носія-джерела до носія-одержувача. Інфо- рмація зберігає конфіденційність, якщо додержується насамперед режимна адекватність носіїв інформації. Поняття «режимна адекватність» склада- ється з термінів:

* + - режим – це сукупність норм для досягнення якої-небудь мети. Напри- клад, для захисту інформації. Тут обов’язково враховується режим доступу до інформації як передбачений правовими нормами порядок отримання, ви- користання, поширення і зберігання інформації;
    - адекватність (від лат. Adaequatus – прирівняний, рівний) – це відпові- дність, правильність, точність.

Смислове значення складових поняття «режимна адекватність носіїв інформації» є таким: це відповідність режимів доступу носіїв інформації (джерела та одержувача) під час їх взаємодії.

Загрози цілісності інформації спрямовані на заборонену режимом до- ступу (порядком отримання, використання, поширення та зберігання інфо- рмації) її зміну або спотворення, що призводить до порушення її якості або повного знищення. Цілісність інформації може бути порушена сумісно, а також унаслідок об’єктивного впливу з боку середовища, що оточує носій інформації.

Термін «комунікабельність» (від пізньолатинського – communicabilis – той, що з’єднується) означає сумісність (здатність до спільної роботи) рі- знотипних систем передачі інформації (наприклад, у телебаченні – з різним числом рядків розкладання телевізійного кадру тощо). Тому *комунікабельні носії інформації – це носії інформації, здатні до взаємодії*.

Приклад некомунікабельності носіїв: через такий сенсор, як органи зору (очі) людина не здатна сприйняти голосову (акустичну) інформацію. Приклад комунікабельності носіїв: через сенсор – органи зору (очі) людина здатна сприйняти інформацію, зафіксовану на паперовому носії зрозумілою для неї мовою.

Загрози доступності (відмова в обслуговуванні) спрямовані на навми- сне або ненавмисне порушення комунікабельності носіїв інформації в про- цесі їх взаємодії. Порушення комунікабельності перериває дозволені режи- мом доступу процеси переміщення інформації. Інформація зберігає досту- пність, якщо зберігається комунікабельність носіїв інформації під час їх взаємодії.

З секретною інформацією пов’язані такі поняття, як:

***Державна таємниця*** – вид таємної інформації, що охоплює відомо- сті у сфері оборони, економіки, науки й техніки, зовнішніх відносин, дер- жавної безпеки та охорони правопорядку, розголошення яких може завдати

шкоди національній безпеці України та які визнані в порядку, встановле- ному Законом України «Про державну таємницю», і підлягають охороні державою.

***Матеріальні носії секретної інформації*** – матеріальні об’єкти, у тому числі фізичні поля, в яких відомості, що становлять державну таєм- ницю, відображені у вигляді текстів, знаків, символів, образів, сигналів, те- хнічних рішень, процесів тощо.

***Система захисту державної таємниці*** – сукупність органів захисту державної таємниці, використовуваних ними засобів і методів захисту ві- домостей, що становлять державну таємницю та їх носіїв, а також заходів, що проводяться з цією метою.

***Допуск до державної таємниці*** – процедура оформлення права гро- мадян на доступ до відомостей, що становлять державну таємницю, а підп- риємств, установ і організацій – на проведення робіт з використанням таких відомостей.

***Доступ до відомостей, що становлять державну таємницю*** – на- дання уповноваженою посадовою особою дозволу громадянину на ознайо- млення з конкретною секретною інформацією та провадження діяльності, пов’язаної з державною таємницею, або ознайомлення з конкретною секре- тною інформацією та провадження діяльності, пов’язаної з державною та- ємницею, цією посадовою особою відповідно до її службових повноважень. ***Гриф секретності*** – реквізит матеріального носія секретної інформа-

ції, що засвідчує ступінь секретності даної інформації. Засекречування ві- домостей та їх носіїв – введення в передбаченому порядку для відомостей, що становлять державну таємницю, обмежень на їх поширення.

***Засекречування відомостей та їх носіїв*** – введення в передбаченому порядку для відомостей, що становлять державну таємницю, обмежень на їх поширення.

***Комерційна таємниця*** – відомості, що не є державними секретами, пов’язані з виробництвом, технологіями, фінансами, процесами управління та іншою діяльністю організацій або фірм, розголошування яких може за- вдати шкоди їхнім інтересам.

***Ступінь секретності*** – категорія, що характеризує важливість такої інформації, можливі збитки внаслідок її розголошування, ступінь обме- ження доступу до неї та рівень її охорони державою. Критерій визначення ступеня секретності інформації встановлює відповідний державний орган. До загроз безпеки інформації та інформаційних ресурсів відносяться:

*джерело загроз; фактор (вразливість); загроза ( дія); наслідки (атака).*

**Джерело загрози** – це потенційні антропогенні, техногенні або сти- хійні носії загрози безпеці.

**Фактор (вразливість)** – це властиві об’єкту інформатизації причини, які призводять до порушення безпеки інформації на конкретному об’єкті та

зумовлені вадами процесу функціонування об’єкта інформатизації, власти- востями архітектури інформаційно-телекомунікаційної системи, протоко- лами обміну та інтерфейсами, що застосовуються, програмним забезпечен- ням і апаратними засобами.

**Загроза (дія)** – це можлива небезпека (потенційна або така, що існує реально) вчинення будь-якого діяння (дії або бездіяльності), спрямованого проти об’єкта захисту (інформаційних ресурсів), яке наносить збиток влас- нику або користувачу, що проявляється як небезпека спотворення або втрати інформації.

**Наслідки (атака)** – це можливі наслідки реалізації загрози (можливі дії) під час взаємодії джерела загрози через наявні фактори (вразливості).

Порушення інформації можуть привести до суттєвих збитків. Збитки – це невигідні для власника майнові наслідки, що виникли внаслідок пра- вопорушення. Прояви збитків можуть бути різноманітні:

* + - моральні й матеріальні збитки ділової репутації організації;
    - моральні, фізичні або матеріальні збитки, пов’язані з розголошенням персональних даних окремих осіб;
    - матеріальні (фінансові) збитки від розголошення конфіденційної інфо- рмації;
    - матеріальні (фінансові) збитки від необхідності відновлення поруше- них інформаційних ресурсів;
    - матеріальні збитки (втрати) від неможливості виконання взятих на себе зобов’язань перед третьою стороною;
    - моральні та матеріальні збитки від дезорганізації діяльності організації;
    - матеріальні та моральні збитки від порушення міжнародних відносин.

Збитки можуть бути спричинені:

* + - *будь-яким суб’єктом* (у цьому випадку відбувається правопорушення). В даному випадку наявна вина суб’єкта, яка визначає спричинену шкоду як склад злочину, що здійснюється зі злими намірами (навмисно) або з необе- режності, і спричинені збитки необхідно класифікувати як склад злочину, відповідно до кримінального права;
    - *незалежно від суб’єкта прояву* (наприклад, стихійних випадків, або інших впливів, таких як прояви техногенних властивостей цивілізації). У даному випадку збитки носять імовірнісний характер і повинні бути зіста- влені як мінімум із тим ризиком, який обговорюється цивільним, адмініст- ративним або арбітражним правом, як предмет розгляду.

Визначення того, хто саме є причиною збитків, є другим за важливі- стю (після спроби цього не допустити) питанням для потерпілого.

Порушення інформації та інформаційних ресурсів можуть бути різ- ними, до них, як правило, відносять наступні:

**Крадіжка** – здійснення з корисливою метою протиправного безопла- тного вилучення і (або) обіг чужого майна на користь винного або інших осіб, що спричинили збитки власникові майна.

**Копіювання комп’ютерної інформації** – це повторювання та стійке збереження інформації на машинному або іншому носієві.

**Знищення** – це зовнішній вплив на майно, у результаті якого воно припиняє своє існування або стає повністю непридатним для використання за цільовим призначенням. Знищене майно не може бути відновлене шля- хом ремонту або реставрації та повністю виводиться з господарського обігу.

**Знищення комп’ютерної інформації** – стирання її у пам’яті комп’ютера.

**Пошкодження** – зміна властивостей майна, унаслідок якого суттєво погіршується його стан, втрачається значна частина його корисних власти- востей і воно стає повністю або частково непридатним для цільового вико- ристання.

**Модифікація комп’ютерної інформації** – внесення будь-яких змін, крім пов’язаних з адаптацією програми для комп’ютера або баз даних.

**Блокування комп’ютерної інформації** – штучне ускладнення дос- тупу користувачів до інформації, не пов’язане з її знищенням.

**Несанкціоноване знищення, блокування, модифікація, копію- вання інформації** – будь-які дії з інформацією, що не дозволені законом, власником або компетентним користувачем.

**Обман (заперечення автентичності, нав’язування хибної інфор- мації)** – навмисне спотворення або приховування істини з метою введення в оману особи, у веденні якої перебуває майно, і таким чином домогтися від неї добровільної передачі майна, а також повідомлення з цією метою сві- домо неправдивих відомостей.

# Джерела загроз безпеці інформації

Носіями загроз безпеці інформації є **джерела загроз**. Джерелами за- гроз можуть бути:

* суб’єкти (особистість) – суб’єктивні;
* об’єктивні прояви;
* внутрішні джерела – усередині організації;
* зовнішні джерела.

Усі джерела загроз безпеці інформації можна поділити на три групи:

* зумовлені діями суб’єкта (антропогенні джерела загроз);
* зумовлені технічними засобами (техногенні джерела загроз);
* зумовлені стихійними джерелами.

***Антропогенними джерелами загроз*** виступають суб’єкти, дії яких можуть бути кваліфіковані як *навмисні або випадкові злочини*. Тільки в

цьому випадку можна говорити про заподіяння збитку. Ця група джерел за- гроз найбільш численна та становить найбільший інтерес з погляду органі- зації захисту, оскільки дії суб’єкта завжди можна оцінити, спрогнозувати та прийняти адекватні заходи. Методи протидії у цьому випадку керовані й залежать від волі організаторів захисту інформації.

Антропогенним джерелом загроз можна вважати суб’єкта, що має до- ступ (санкціонований або несанкціонований) до роботи зі штатними засо- бами об’єкта, що потребує захисту.

*Суб’єкти (джерела*), дії яких можуть призвести до порушення без- пеки інформації, можуть бути як *зовнішніми, так і внутрішніми*.

Зовнішні джерела можуть бути випадковими або навмисними та мати різний рівень кваліфікації.

Внутрішні суб’єкти (джерела) здебільшого являють собою висококва- ліфікованих спеціалістів у галузі розробки та експлуатації програмного за- безпечення та технічних засобів, знайомих зі специфікою завдань, що вирі- шуються, структурою та основними функціями та принципами роботи про- грамно-апаратних засобів захисту інформації, які мають можливість вико- ристання штатного обладнання та технічних засобів мережі.

Необхідно враховувати також, що особливу групу внутрішніх антро- погенних джерел складають особи з порушеною психікою та спеціально впроваджені та завербовані агенти, які можуть бути з числа основного, до- поміжного та технічного персоналу, а також представників служби захисту інформації.

Друга група містить джерела загроз, що визначаються технократич- ною діяльністю людини та розвитком цивілізації. Проте наслідки, викли- кані такою діяльністю, вийшли з-під контролю людини та діють самі по собі. Людство дійсно стає все більше залежним від техніки, і джерела за- гроз, які залежать від властивостей техніки, менше прогнозовані й тому по- требують особливої уваги. Цей клас джерел загроз безпеці інформації є осо- бливо актуальним у сучасних умовах, оскільки очікується різке зростання кількості техногенних катастроф, викликаних фізичним та моральним ста- рінням наявного обладнання, а також відсутністю коштів на його онов- лення. Технічні засоби, що є джерелами потенційних загроз безпеці інфор- мації, також можуть бути зовнішніми та внутрішніми.

Третя група джерел загроз об’єднує обставини, що становлять *непе- реборну силу, тобто такі обставини, які носять об’єктивний і абсолют- ний характер*, що поширюється на всіх. До непереборної сили в законодав-

стві та договірній практиці відносять стихійні лиха або інші обставини, які неможливо передбачити або їм запобігти або можливо передбачити, але не можливо запобігти їм при сучасному рівні знань і можливостей людини. Такі джерела загроз абсолютно не піддаються прогнозуванню, і тому за- ходи захисту від них повинні застосовуватися завжди. Стихійні джерела

потенційних загроз інформаційній безпеці переважно є зовнішніми щодо об’єкта захисту. Під ними розуміють насамперед природні катаклізми.

# Класифікація вразливостей безпеки

Загрози, як можливі небезпечності здійснення будь-якої дії, спрямо- ваної проти об’єкта захисту, проявляються не самі по собі, а через вразли- вості (фактори), що призводять до порушення безпеки інформації на конк- ретному об’єкті інформатизації.

Вразливості безпеці інформації можуть бути:

1. *Об’єктивні* вразливості залежать від особливостей побудови та техніч- них характеристик обладнання, що застосовується на об’єкті захисту. По- вне усунення цих вразливостей неможливе, але вони можуть суттєво пос- лаблятися технічними та інженерно-технічними методами відбиття загроз безпеці інформації.
2. *Суб’єктивні* вразливості залежать від дій співробітників і, в основному, вилучаються організаційними та програмно-апаратними методами.
3. *Випадкові* вразливості залежать від особливостей середовища, яке оточує об’єкт захисту, та непередбачених обставин. Ці фактори зазвичай малопе- редбачувані і їх усунення можливе тільки при проведенні комплексу орга- нізаційних та інженерно-технічних заходів із протидії загрозам інформацій- ній безпеці.

# Моделі порушень інформаційних ресурсів

Особа – користувач ресурсами ІС, яка здійснює спробу несанкціоно- ваного (не авторизованого) доступу до інформаційних ресурсів системи (з метою: ознайомлення, модифікації, знищення, зміни режимів використання або загального функціонування системи тощо), є порушником.

Порушення з боку цих осіб можуть бути як ненавмисними, так і зло- вмисними.

Особливу небезпеку варто очікувати від зловмисних порушників, які в силу тих або інших причин перебувають під впливом:

* кримінальних осіб та їх угруповань;
* бізнесменів, комерсантів та їх об’єднань;
* політичних діячів і партій;
* агентів спецслужб інших держав, або самі входять до їх складу.

**Порушники** можуть бути внутрішніми (із числа співробітників, ко- ристувачів ІС) або зовнішніми (сторонні особи чи особи, які перебувають за межами контрольованої зони, або проникли в її межі несанкціонованим шляхом).

**Кваліфікація порушника.** Порушники мають певний рівень кваліфі- кації, достатній для успішної реалізації загроз ресурсам ІС, тобто:

* + володіють інформацією щодо функціональних особливостей ІС, уміють користуватися штатними засобами;
  + володіють високим рівнем знань в обслуговуванні ідентичних засобів ІС;
  + володіють високим рівнем знань у галузі обчислювальної техніки й про- грамування на мовах розробки програмних засобів ІС, проектуванню й екс- плуатації подібних до ІС систем;
  + володіють інформацією щодо функцій і механізмів захисту, які реалізо- вані як у системі захисту інформації ІС, так і у функціях і механізмах захи- сту, що вбудовані в базове та прикладне програмне забезпечення.

За рівнем можливостей, які надаються штатною інфраструктурою ін- формаційної мережі, виділяють чотири рівні порушників:

* + *перший рівень* відповідає найбільш низькому рівню можливостей поруш- ника у системі – можливістю запуску фіксованого набору програм, які реа- лізують певні функції з обробки інформації;
  + *другий рівень* визначається можливістю створення й запуску власних про- грам із новими функціями обробки й подальшого одержання потрібної по- рушнику інформації;
  + *третій рівень* визначається можливістю управління функціонуванням ІС, тобто впливом на базове програмне забезпечення системи, а також на склад і конфігурацію технічного забезпечення інформаційної системи;
  + *четвертий рівень* визначається інтегрованим обсягом можливостей спів- робітників, які здійснюють розробку, впровадження й експлуатацію техні- чних засобів інформаційної системи, а також можливістю введення до складу інформаційної системи власних технічних засобів із новими функ- ціями, щодо обробки й отримання інформації.

Приблизний перелік персоналу ІС і відповідний ступінь ризику щодо можливої реалізації загроз та нанесення шкоди залежно від зазначених ро- бочих функцій працівників:

# Найбільший ризик:

* + - системний адміністратор;
    - адміністратор бази даних;
    - адміністратор безпеки.

# Високий ризик:

* + - оператор системи;
    - оператор введення й підготовки даних;
    - менеджер обробки даних;
    - системний програміст;

# Середній ризик:

* + - інженер системи;
    - менеджер програмного забезпечення;

# Обмежений ризик:

* + - прикладний програміст;
    - інженер і оператор зв’язку;
    - інженер з устаткування;
    - оператор периферійного устаткування;
    - бібліотекар системних магнітних носіїв;
    - користувач-програміст;
    - користувач-операціоніст;

**Низький ризик**: інженер по периферійному устаткуванню; бібліотекар ма- гнітних носіїв користувачів.

Цілі та методи порушника:

* + особиста авторизація, тобто одержати особисті легальні атрибути доступу, з бажано найширшими правами щодо доступу до ресурсів ІС, з метою їх- нього використання, одержання необхідної інформації в потрібному обсязі, ознайомлення з конфіденційною інформацією, одержання можливості її модифікації або знищення згідно зі своїми намірами;
  + авторизувати інших осіб, які б мали можливість одержати легальні атри- бути доступу, з бажано найширшими правами щодо доступу до ресурсів ІС з метою їхнього використання, одержання необхідної інформації в потріб- ному обсязі, ознайомлення з конфіденційною інформацією, одержання мо- жливості її модифікації або знищення згідно зі своїми намірами;
  + знайти прихильників або довірених осіб серед персоналу або користувачів ІС, які мають можливість одержувати легальні атрибути доступу до ресур- сів ІС з метою їхнього використання, одержання необхідної інформації в потрібному обсязі, ознайомлення з конфіденційною інформацією, одер- жання можливості її модифікації або знищення згідно зі своїми намірами.

Порушники переслідують певні наміри:

1. Одержання атрибутів доступу користувачів шляхом використання техні- чних засобів, крадіжок, купівлі, або одержання іншим шляхом.
2. Проникнення на місця розміщення тих або інших компонентів, елементів або ресурсів ІС (обчислювальних ресурсів, інформаційних ресурсів, базо- вого й прикладного програмного забезпечення тощо) шляхом подолання охорони або охоронної сигналізації та ін.
3. Зміни режимів функціонування ІС, її ресурсів та послуг системи.
4. Установки фізичних засобів у місцях розміщення елементів ІС (техніч- них закладок) чи інших засобів технічної розвідки (у тому числі віддалених, наприклад, в елементах комунікаційної мережі зв’язку) для перехвату ін- формації.
5. Установки фізичних засобів у місцях розміщення елементів ІС (техніч- них закладок) або інших засобів (у тому числі віддалених, наприклад, в еле- ментах комунікаційної мережі зв’язку) для генерації хибних сигналів, інфо- рмаційних символів або спотворених повідомлень.
6. Установки програмних засобів (програмних закладок або вірусів), копі- ювання інформації з метою її використання.
7. Установки програмних засобів (програмних закладок або вірусів) для мо- дифікації системного програмного забезпечення, так і інформації ІС, шля- хом введення програмних вірусів, спотворених сигналів, інформаційних символів або хибних повідомлень з метою перевантаження систем і пору- шення, таким чином, доступності компонентів ІС.
8. Здійснення спроб несанкціонованого доступу до обчислювальних та ін- формаційних ресурсів, базового та прикладного програмного забезпечення.
9. Здійснення спроб несанкціонованого доступу до системи захисту інфор- мації як частини ІС, так і до її телекомунікаційної підсистеми, шляхом по- долання системи управління доступом.

# Порушник може знати:

* склад, розміщення, функціональні особливості, умови й режими функціо- нування елементів ІС, включаючи траси прокладених або можливих ліній зв’язку, комунікаційних мереж зв’язку й трафіки відповідних каналів пере- дачі даних;
* порядок, засоби й режими здійснення охорони елементів ІС, місця їх роз- міщення і навколишню територію;
* порядок, засоби й режими здійснення організаційно-правових і технічних заходів захисту ресурсів ІС;
* основні закономірності формування в ІС баз даних і потоків запитів до них;

# За характером дій зловмисник може здійснювати:

* + *активні дії -* спроба навмисної несанкціонованої зміни стану функці- онування ІС
  + *пасивні дії*, – спроба несанкціонованого проникнення в систему без зміни її стану.

# За характером дій порушників можна класифікувати на:

* + *випадкових порушників* – авторизованих користувачів, які порушили політику безпеки тієї або іншої послуги ненавмисно, а помилково, шляхом виконання непередбачених дій з об’єктом захисту, шляхом випадкового подолання засобів управління доступом тощо;
  + *терплячих зловмисників* – авторизованих користувачів, які порушили політику безпеки тієї або іншої послуги навмисно, але без рішучих дій, маскуючись, шляхом підбору атрибутів доступу інших користу- вачів з метою схованого подолання засобів управління доступом тощо;
  + *рішучих зловмисників*, які мають на меті порушити ту або іншу влас- тивість інформації. Зловмисники прагнуть перебороти: засоби органі- заційного обмеження доступу, охоронної сигналізації, тощо й одер- жати можливість фізичного доступу до засобів обробки, зберігання або передачі інформаційних ресурсів з метою виводу їх з ладу, зміни режимів функціонування, крадіжки носіїв інформації та ін.;
  + *зловмисників*, які використовують засоби віддаленого доступу до ін- формаційних об’єктів з умов: витоку інформації технічними кана- лами, реалізації спеціальних впливів на інформацію з технічних кана- лів, впливу на мережеве устаткування локальних або розподілених мереж, у тому числі й засоби телекомунікаційних мереж, які викори- стовуються елементами ІС.

Дії порушників можуть бути спрямованими на порушення функціона- льних властивостей захищеності інформаційних об’єктів, зокрема на пору- шення:

* + конфіденційності, цілісності й доступності інформаційних об’єктів;
  + функцій спостереження за діяльністю користувачів і процесів, однозна- чної ідентифікації користувачів, ресурсів і процесів.

## Порушники можуть використовувати такі методи та засоби:

* *агентурні методи* одержання відомостей через підкуплених користувачів і персонал, а також через прихильників чи довірених осіб із числа штатних працівників або таких, які мають доступ до ресурсів ІС;
* *пасивні технічні засоби* перехоплення інформаційних сигналів;
* *штатні засоби ІС* або недоліки проектування системи захисту інформації від несанкціонованого доступу (НСД);
* *методи й засоби активного впливу* на елементи ІС, які змінюють конфігу- рацію ІС (підключення додаткових або модифікація штатних технічних за- собів, підключення або «врізання» у канали передачі даних, впровадження й використання спеціального ПЗ і т. ін.).

За місцем здійснення порушень дії зловмисника можна класифіку-

вати:

* без одержання доступу на контрольовану територію із використанням те- хнічних засобів віддаленого доступу через засоби: Internet, електронної по- шти, модемного зв’язку чи дистанційної розвідки (наприклад: по оптичних, акустичних каналах і т. ін.), або з використанням засобів одержання інфор- мації з мережі передачі даних (наприклад: шляхом підключення або «врі- зання» в лінії зв’язку);
* з одержанням доступу на контрольовану територію ІС або до робочих місць кінцевих користувачів, але без доступу до технічних засобів ІС, також із використанням технічних засобів дистанційної розвідки з подальшим не- санкціонованим доступом до будинків, або приміщень, у яких розміщені елементи ІС;
* з одержанням доступу до робочих місць кінцевих користувачів ІС із пода- льшим несанкціонованим доступом до пристроїв введення/виводу інфор- мації, копіювання, до канального або устаткування, яке утворює канал і до інших елементів ІС;
* з одержанням доступу до засобів управління ІС і засобів управління ком- плексною системою захисту інформації з подальшими розширеними мож- ливостями доступу до ресурсів ІС та послуг системи.

## Порушник (user violator) – це користувач, який здійснює несанкці- онований доступ до інформації. До порушників відносяться:

Хакер (hacker) ставить дослідницькі задачі з оцінки та знаходження слабких місць з метою подальшого підвищення надійності комп’ютерної системи.

Кракер (cracker) виконує вторгнення в систему з метою руйнування, крадіжки, псування, модифікації інформації та роблять правопорушення з корисливими намірами швидкого збагачення.

Модель порушника відображає його практичні та потенційні можли- вості, апріорні знання, час та місце дії тощо.

При розробці моделі порушника визначаються:

* припущення щодо категорії осіб, до яких може належати порушник;
* припущення щодо мотивів дій порушника (цілей, які він має);
* припущення щодо рівня кваліфікації та обізнаності порушника і його технічної оснащеності;
* обмеження та припущення щодо характеру можливих дій порушників (за часом та місцем дії та інші).

Припускається, що за своїм рівнем порушник – це фахівець вищої ква- ліфікації, який має повну інформацію про систему.

Виділяють наступні типи порушників:

## Зовнішні порушники:

* добре озброєна й оснащена силова група, що діє ззовні швидко й на- пролом;
* поодинокий порушник, що не має допуску на об’єкт і намагається діяти потайки й обережно, оскільки він усвідомлює, що сили реагування мають переваги.

## Внутрішні порушники:

* допоміжний персонал об’єкта, що допущений на об’єкт, але не допу- щений до життєво важливого центру ІС;
* основний персонал, що допущений до життєво важливого центру (най- більш небезпечний тип порушників);
* співробітників служби безпеки, які часто формально і не допущені до життєво важливого центру, але реально мають достатньо широкі можливо- сті для збору необхідної інформації і вчинення акції.

## Сторонні особи, що можуть бути порушниками:

* *клієнти* (представники організацій, громадяни);
* *відвідувачі* (запрошені з якого-небудь приводу);
* *представники організацій*, що займаються забезпеченням життєдіяль- ності організації (енерго, водо, теплопостачання і т. ін.);
* *представники конкуруючих організацій* (іноземних служб) або особи, що діють за їхнім завданням;
* *особи, які випадково* або навмисно порушили пропускний режим (не маючи на меті порушити безпеку);
* будь-які особи за межами контрольованої зони.

# Питання для самоконтролю

* 1. Що є джерелом та фактором загрози інформації?
  2. Які існують види загроз комп’ютерної інформації?
  3. Які групи джерел загроз безпеці інформації виділяють?
  4. Наведіть класифікацію вразливостей безпеці інформації.
  5. Які класи (види) загроз розрізняються в інформаційній сфері?
  6. Які загрози відносяться до рівня порушення конфіденційності ?
  7. Які загрози відносяться до рівня порушення цілісності ?
  8. Які існують категорії джерел конфіденційної інформації?
  9. Які є моделі порушень інформаційних ресурсів?
  10. В чому полягає мета та цілі порушника об’єктів інформаційної ді- яльності?
  11. Наведіть класифікацію порушника за характером дій.

# Розділ 9. ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ ТА ІНФОРМАЦІЙНИХ РЕСУРСІВ

* 1. Напрями захисту інформації.
  2. Правовий захист.
  3. Організаційний захист.
  4. Інженерно-технічний захист.

# Напрями захисту інформації

***Напрями забезпечення безпеки інформації*** – це нормативно-правові категорії, орієнтовані на забезпечення комплексного захисту інформації від внутрішніх та зовнішніх загроз на державному рівні, на рівні підприємства або організації, на рівні окремої особи.

З урахуванням практики, що склалася на теперішній час, виділяють такі напрями захисту інформації:

*правовий захист* – це спеціальні закони, інші нормативні акти, правила, процедури та заходи, що забезпечують захист інформації на правовій ос- нові;

*організаційний захист* – це регламентація виробничої діяльності та від- носин виконавців на нормативно-правовій основі, яка виключає або посла- блює нанесення будь-яких збитків виконавцям;

*інженерно-технічний захист* – це використання різноманітних техніч- них засобів, що перешкоджають нанесенню збитків.

Крім того, заходи захисту, орієнтовані на забезпечення безпеки інфо- рмації, можуть бути охарактеризовані багатьма параметрами, що відобра- жають, крім напрямів, орієнтацію на об’єкти захисту, характер загроз, спо- соби дій, їх поширення, охоплення та масштабність.

Так, за характером загроз заходи захисту орієнтовані на захист інфо- рмації від розголошення, витоку та несанкціонованого доступу.

За способом дії їх можна поділити на попередження, виявлення, при- пинення та відновлення збитків або інших утрат.

За охопленням заходи захисту можуть поширюватись на територію, будівлю, приміщення, апаратуру або окремі елементи апаратури.

Масштабність заходів захисту характеризується як об’єктовий, групо- вий або індивідуальний захист.

# Правовий захист інформації

***Правовий захист інформації*** як ресурсу признаний на міждержав- ному, державному рівні та визначається міждержавними договорами, кон- венціями, деклараціями та реалізується патентами, авторським правом та ліцензіями на їхній захист.

На державному рівні правовий захист регулюється державними та ві- домчими актами. У нашій державі такими правилами (актами, нормами) є Конституція України, закони України, цивільне, адміністративне, криміна- льне право, викладене у відповідних кодексах. Що стосується відомчих но- рмативних актів, то вони визначаються наказами, керівництвами та інстру- кціями, які видаються відомствами, організаціями та підприємствами, що діють у межах певних структур.

Сучасні умови вимагають і визначають необхідність комплексного підходу до формування законодавства із захисту інформації, його складу та змісту, співвіднесення його зі всією системою законів та правових актів Ук- раїни.

Вимоги інформаційної безпеки повинні органічно входити до всіх рі- внів законодавства, у тому числі в конституційне законодавство, основні загальні закони, закони з організації державної системи управління, спеці- альні закони, відомчі правові акти і т. ін.

Зазвичай використовується наступна структура правових актів, які орієнтовані на правовий захист інформації.

***Конституційне законодавство*** – норми, що стосуються питань ін- форматизації та захисту інформації, входять до нього як складові елементи. Загальні закони, кодекси (про власність, про надра, про права громадян, про громадянство, про податки, про антимонопольну діяльність і т. ін.), які включають норми з питань інформатизації та інформаційної безпеки.

***Закони про організацію управління*** стосовно окремих структур гос- подарства, економіки, системи державних органів та визначення їхнього статусу. Такі закони включають окремі норми з питань захисту інформації. Поряд із загальними питаннями інформаційного забезпечення та захисту інформації конкретного органу ці норми повинні встановлювати його обов’язки з формування, актуалізації та безпеки інформації, що представ- ляє загальнодержавний інтерес.

***Спеціальні закони***, які відносяться до конкретних сфер відносин, га- лузей господарства, процесів. До їхнього числа входять Закони України

«Про інформацію», «Про захист інформації в автоматизованих системах» і т. ін. Власне склад і зміст цього блоку законів і створює спеціальне законо- давство як основу правового забезпечення інформаційної безпеки.

***Підзаконні нормативні акти із захисту інформації***. Правоохоронне законодавство України, яке містить норми про відповідальність за право- порушення у сфері інформатизації.

***Спеціальне законодавство в галузі безпеки інформації*** може бути представлене сукупністю законів. В їхньому складі особливе місце посіда- ють Закони України «Про інформацію» та «Про захист інформації в авто- матизованих системах», які закладають основи правового визначення всіх найважливіших компонентів інформаційної діяльності: інформації та інфо- рмаційних систем; суб’єктів – учасників інформаційних процесів; право- відносин виробників та споживачів інформаційної продукції; власників (джерел) інформації - обробників та споживачів на основі відносин власно- сті при забезпеченні гарантій інтересів громадян та держави.

Ці закони також визначають основи захисту інформації в системах об- робки і при її використанні з урахуванням категорій доступу до відкритої інформації і до інформації з обмеженим доступом. Ці закони містять, крім того, загальні норми з організації та ведення інформаційних систем, вклю- чаючи банки даних державного призначення, порядок державної реєстра- ції, ліцензування, сертифікації, експертизи, а також загальні принципи за- хисту та гарантій прав учасників інформаційного процесу. Питання право- вого режиму інформації з обмеженим доступом реалізуються у двох само- стійних законах про державну та комерційну (проект) таємниці.

Таким чином, правовий захист інформації забезпечується нормати- вно-законодавчими актами, сукупність яких за рівнем являє собою ієрархі- чну систему від Конституції України до функціональних обов’язків і конт- рактів конкретного виконавця, які визначають перелік відомостей, що під- лягають охороні, і заходи відповідальності за їх розголошення.

Одним із нових напрямків правового захисту є ***страхове забезпе- чення***. Воно призначене для захисту власної інформації та засобів її обро- бки як від традиційних загроз (крадіжки, стихійні лиха), так і від загроз, що

виникають у ході роботи з інформацією. До них належать розголошення, витік та несанкціонований доступ до конфіденційної інформації.

Метою страхування є забезпечення страхового захисту фізичних та юридичних осіб від страхових ризиків у вигляді повного або часткового ві- дшкодування збитків і втрат, які спричинені стихійними лихами, надзви- чайними подіями в різних галузях діяльності, протиправними діями з боку конкурентів та зловмисників шляхом виплати грошової компенсації або на- дання сервісних послуг (ремонт, відновлення) при настанні страхової події.

Спираючись на державні правові акти та враховуючи відомчі інтереси на рівні конкретного підприємства (фірми, організації), розробляються вла- сні нормативно-правові документи, орієнтовані на забезпечення інформа- ційної безпеки. До таких документів відносяться: положення про збере- ження конфіденційної інформації; перелік відомостей, які складають кон- фіденційну інформацію; інструкція про порядок допуску співробітників до відомостей, які становлять конфіденційну інформацію; положення про спе- ціальне діловодство та документообіг; перелік відомостей, які дозволені до опублікування у відкритому друці; положення про роботу з іноземними фі- рмами та їхніми представниками; зобов’язання співробітника про збере- ження конфіденційної інформації; пам’ятка співробітнику про збереження комерційної таємниці.

Нормативні акти спрямовані на попередження випадків неправомір-

ного оголошення (розголошення) секретів на правовій основі – у випадку їх порушення повинні вживатися відповідні заходи впливу. Залежно від ха- рактеру інформації, її доступності для зацікавлених споживачів, а також економічної доцільності конкретних захисних заходів, можуть бути обрані такі форми захисту інформації: патентування; авторське право; признання відомостей конфіденційними; застосування норм зобов’язального права.

Крім вищевикладених форм правового захисту та права належності інформації, знаходить велике поширення офіційна передача права на кори- стування нею у вигляді ліцензії.

***Ліцензія*** (від лат. licentia – «свобода, право») – це дозвіл, виданий дер- жавою на проведення деяких видів господарської діяльності, включаючи зовнішньоторговельні операції (ввезення та вивезення) та надання права використовувати захищені патентами винаходи, технології, методики. Лі- цензійні дозволи надаються на певний час і на певні види товарів.

***Комерційна таємниця*** – це відомості, які не є державними секре- тами, пов’язані з виробництвом, технологією, управлінням, фінансами та іншою діяльністю, розголошення, витік та несанкціонований доступ до якої може призвести до збитків їхнім власникам.

До комерційної таємниці не відносяться: відомості, що охороняються державою; відомості, які є загальновідомими на законній підставі;

відомості про негативні сторони діяльності; установчі документи та відо- мості про господарську діяльність.

Створюючи систему інформаційної безпеки, необхідно чітко розу- міти, що без правового забезпечення захисту інформації будь-які наступні претензії до несумлінного співробітника, клієнта, конкурента та посадової особи будуть просто безпідставними. Якщо перелік відомостей конфіден- ційного характеру не доведений своєчасно до кожного співробітника (при- родно, якщо він допущений до виконання посадових обов’язків) у письмо- вому вигляді, то співробітник, який викрав важливу інформацію при пору- шенні встановленого порядку роботи з нею скоріше всього не буде покара- ний.

Правові норми забезпечення безпеки та захисту інформації на конк-

ретному підприємстві (фірмі, організації) відображаються в сукупності установчих, організаційних та функціональних документів. Вимоги забез- печення безпеки та захисту інформації відображаються у Статуті (установ- чому договорі) у вигляді таких положень: підприємство має право визна- чати склад, обсяги та порядок захисту конфіденційних відомостей, вима- гати від своїх співробітників забезпечення їх збереження та захисту від вну- трішніх та зовнішніх загроз; підприємство зобов’язане забезпечувати збе- реження конфіденційної інформації. Ці вимоги дають адміністрації підпри- ємства такі права: створювати організаційні структури із захисту конфіде- нційної інформації; видавати нормативні та розпорядчі документи, які ви- значають порядок виділення відомостей конфіденційного характеру та ме- ханізми їхнього захисту; включати вимоги із захисту інформації в угоди з усіх видів діяльності; вимагати захисту інтересів підприємства з боку дер- жавних інстанцій; розробляти «Перелік відомостей конфіденційної інфор- мації».

# Організаційний захист

***Організаційний захист*** – це регламентація виробничої діяльності та відносин виконавців на нормативній основі, що виключає або суттєво ускладнює неправомірне оволодіння конфіденційною інформацією та про- яву внутрішніх та зовнішніх загроз.

*Організаційний захист забезпечує:*

* організацію режиму, охорони, роботу з кадрами, з документами;
* використання технічних засобів безпеки та інформаційно-аналітичну діяльність із виявлення внутрішніх і зовнішніх загроз діяльності підприєм- ства (організації).

Організаційні заходи відіграють суттєву роль у створенні надійного механізму захисту інформації, оскільки можливості несанкціонованого ви- користання конфіденційних відомостей значною мірою обумовлюються не технічними аспектами, а зловмисними діями та недбалістю користувачів

або персоналу. Впливу цих аспектів практично неможливо запобігти за до- помогою технічних заходів. Для цього необхідна сукупність організаційно- правових і організаційно-технічних заходів, які вилучали б (або зводили до мінімуму) можливість виникнення небезпеки конфіденційності інформації.

*До основних організаційних заходів зазвичай відносять такі:*

* організація режиму та охорони – їх мета:
* виключення можливості таємного проникнення на територію та в при- міщення сторонніх осіб;
* забезпечення зручності проходу та переміщення співробітників та ві- двідувачів;
* створення окремих виробничих зон за типом конфіденційних робіт із самостійними системами доступу;
* контроль та дотримання часового режиму праці та перебування на те- риторії персоналу підприємства;
* організація та підтримка надійного пропускного режиму та контролю

співробітників і відвідувачів і т. ін.;

* організація роботи зі співробітниками, яка передбачає підбір і розста- новку персоналу, включаючи ознайомлення зі співробітниками, їх ви- вчення, навчання правилам роботи з конфіденційною інформацією, ознайо- млення з мірою відповідальності за порушення правил захисту інформації;
* організація роботи з документами та документованою інформацією, включаючи організацію розробки та використання документів і носіїв кон-

фіденційної інформації, їх облік, використання, повернення, зберігання та знищення;

* організація використання технічних засобів збирання, обробки, нагро- мадження та зберігання конфіденційної інформації;
* організація роботи з аналізу внутрішніх та зовнішніх загроз конфіден-

ційній інформації та розробка заходів із забезпечення її захисту;

* організація роботи з проведення систематичного контролю за роботою персоналу з конфіденційною інформацією, порядком обліку, зберігання та знищення документів та технічних носіїв.

У кожному конкретному випадку організаційні заходи носять специ- фічну для цієї організації форму та зміст, які спрямовані на забезпечення безпеки інформації в конкретних умовах.

*Особливості організаційного захисту комп’ютерних інформаційних систем.*

Організація захисту комп’ютерних інформаційних систем та мереж визначає порядок і схему функціонування основних їхніх підсистем, вико- ристання пристроїв та ресурсів, відносини користувачів між собою відпо- відно до нормативно-правових вимог та правил.

Захист інформації на основі організаційних заходів відіграє значну роль у забезпеченні надійності та ефективності, оскільки несанкціонований

доступ та витік інформації найчастіше зумовлені зловмисними діями, не- дбалістю користувачів або персоналу. Ці фактори практично неможливо виключити або локалізувати за допомогою апаратних і програмних засобів, криптографії та фізичних засобів захисту, тому сукупність організаційних, організаційно-правових та організаційно-технічних заходів, які застосову- ються разом із технічними методами, мають за мету виключити, зменшити або повністю усунути збитки при дії різноманітних деструктивних факто- рів.

Організаційні засоби захисту комп’ютерних інформаційних систем та мереж найчастіше застосовуються в таких випадках:

* при проектуванні, будівництві та обладнанні приміщень, вузлів мереж та інших об’єктів інформаційної системи для запобігання впливу стихій- ного лиха, можливості недозволеного проникнення в приміщення і т. ін.;
* при доборі та підготовці персоналу – у цьому випадку передбачається перевірка осіб, які приймаються на роботу, створення умов, за яких персо- нал був би зацікавлений у збереженні інформації, навчання правилам ро- боти із закритою інформацією, ознайомлення з мірою відповідальності за порушення правил захисту;
* при зберіганні та використанні документів та інших носіїв (маркування, реєстрація, визначення правил видачі та повернення, ведення документації тощо);
* при дотриманні надійного пропускного режиму до технічних засобів комп’ютерних мереж та систем при роботі змінами (призначення відпові- дальних за захист інформації у змінах, контроль за роботою персоналу, ве- дення автоматизованих журналів роботи, знищення встановленим поряд- ком закритих виробничих документів);
* при внесенні змін у програмне забезпечення (суворе санкціонування, розгляд та затвердження проектів змін, перевірка їх на задоволення вимог захисту, документальне оформлення змін і т. ін.);
* при підготовці та контролі роботи користувачів.

Одним із найважливіших організаційних заходів є *створення спеціа- льних штатних служб захисту інформації* в закритих інформаційних сис- темах у вигляді адміністратора безпеки мережі та адміністратора безпеки розподілених баз та банків даних, які містять відомості конфіденційного характеру.

Цілком очевидно, що організаційні заходи повинні чітко плануватися, спрямовуватися та здійснюватися певною організаційною структурою, пе- вним спеціально створеним для цих цілей структурним підрозділом, уком- плектованим відповідними фахівцями з безпеки діяльності та захисту інфо- рмації.

Найчастіше таким структурним підрозділом є *служба безпеки підпри- ємства* (фірми, організації), на яку покладаються такі функції: організація

та забезпечення охорони персоналу, матеріальних та фінансових цінностей та захисту конфіденційної інформації; забезпечення пропускного та внут- рішньо-об’єктного режиму на території, у будівлях та приміщеннях, конт- роль дотримання вимог режиму співробітниками, суміжниками, партне- рами та відвідувачами; керівництво роботами з правового та організацій- ного регулювання відносин із захисту інформації; участь у розробці осно- воположних документів з метою закріплення в них вимог забезпечення без- пеки та захисту інформації, а також положень про підрозділи, трудові до- говори, угоди, підряди, посадові інструкції та обов’язки керівництва, спе- ціалістів, робітників та службовців; розробка та здійснення разом з іншими підрозділами заходів із забезпечення роботи з документами, що містять конфіденційні відомості; при всіх видах робіт організація та контроль ви- конання вимог «Інструкції із захисту конфіденційної інформації»; ви- вчення всіх сторін виробничої, комерційної, фінансової та іншої діяльності для виявлення та наступної протидії будь-яким спробам нанесення збитків, ведення обліку та аналіз порушень режиму безпеки, накопичення та аналіз даних про зловмисні прагнення конкурентної та інших організацій, про ді- яльність підприємства та його клієнтів, партнерів, суміжників; розробка, ведення, оновлення та поповнення «Переліку відомостей, що носять конфі- денційний характер» та інших нормативних актів, які регламентують поря- док забезпечення та захисту інформації; забезпечення суворого виконання вимог нормативних актів із забезпечення виробничих секретів підприємс- тва; здійснення керівництва службами та підрозділами безпеки підвідом- чих підприємств, організацій, закладів та іншими структурами; організація та регулярне проведення обліку співробітників підприємства та служби безпеки з усіх напрямів захисту інформації та забезпечення безпеки вироб- ничої діяльності; ведення обліку та суворого контролю виділених для кон- фіденційної роботи приміщень, технічних засобів у них, що мають потен- ційні канали витоку інформації та канали проникнення до джерел інформа- ції, які перебувають під охороною; забезпечення проведення всіх необхід- них заходів із припинення спроб нанесення моральних та матеріальних зби- тків з боку внутрішніх та зовнішніх загроз; підтримка контактів із право- охоронними органами та службами безпеки сусідніх підприємств для ви- вчення криміногенної ситуації в районі (зоні) та надання взаємної допомоги в кризових ситуаціях.

Служба безпеки є самостійною організаційною одиницею підприємс-

тва, що підпорядковується безпосередньо керівникові підприємства. Очо- лює службу безпеки начальник служби безпеки в посаді заступника керів- ника підприємства з безпеки.

Організаційно служба безпеки може складатися з таких структурних одиниць:

підрозділу режиму та охорони;

спеціального підрозділу з обробки документів конфіденційного харак- теру;

інженерно-технічних підрозділів;

інформаційно-аналітичних підрозділів.

У такому складі служба безпеки здатна забезпечити захист конфіденцій- ної інформації від будь-яких загроз.

Організаційні заходи є вирішальною ланкою формування та реалізації комплексного захисту інформації та створення системи безпеки підприєм- ства.

# Інженерно-технічний захист

***Інженерно-технічний захист*** – це сукупність спеціальних органів, технічних засобів та заходів для їхнього використання в інтересах захисту конфіденційної інформації.

Основне завдання інженерно-технічного захисту – це попередження розголошення, витоку, несанкціонованого доступу та інших форм незакон- ного втручання в інформаційні ресурси.

Різноманітність цілей, завдань, об’єктів захисту та заходів, що прово- дяться, передбачають розгляд деякої системи класифікації засобів інжене- рно-технічного захисту за видом, орієнтацією та іншими характеристи- ками.

Наприклад, засоби інженерно-технічного захисту можна класифіку-

вати за об’єктами впливу, характером заходів, способами реалізації, масш- табом охоплення, класом засобів зловмисників, яким здійснюється проти- дія з боку служби безпеки.

За функціональним призначенням засоби інженерно-технічного захи- сту поділяються на такі групи:

1. фізичні засоби захисту,
2. апаратні засоби захисту,
3. програмні засоби захисту,
4. криптографічні засоби захисту.

***Фізичні засоби*** включають різноманітні пристрої та споруди, які пе- решкоджають фізичному проникненню (або доступу) зловмисників на об’єкти захисту та матеріальних носіїв конфіденційної інформації та здійс- нюють захист персоналу, матеріальних носіїв, фінансів та інформації від протиправних дій.

***До апаратних засобів*** відносяться прилади, пристрої, та інші технічні рішення, які використовуються в інтересах захисту інформації. Основне за- вдання апаратних засобів – забезпечення стійкого захисту від розголо- шення, витоку і несанкціонованого доступу через технічні засоби забезпе- чення діяльності організації (підприємства).

***Програмні засоби*** охоплюють спеціальні програми, програмні ком- плекси та системи захисту інформації в інформаційних системах різнома- нітного призначення та засобах обробки (збирання, нагромадження, збері- гання, обробки та передачі) даних.

***Криптографічні засоби*** – це спеціальні математичні та алгоритмічні засоби захисту інформації, що передається системами та мережами зв’язку, зберігається та обробляється на ЕОМ із використанням різноманітних ме- тодів шифрування.

Апаратні методи та засоби захисту знайшли достатньо широке розпо- всюдження. Проте із-за того, що вони не мають достатньої гнучкості, часто втрачають свої захисні властивості при розкритті принципу їхньої дії й у подальшому не можуть бути використані.

Програмні методи та засоби більш надійні, період їхнього гарантова- ного використання значно більший, ніж апаратних методів та засобів.

Криптографічні методи та засоби посідають важливе місце і є надій- ним засобом забезпечення захисту інформації на тривалі періоди.

Очевидно, що такий поділ засобів захисту інформації достатньо умо- вний, оскільки на практиці дуже часто вони взаємодіють і реалізуються у вигляді програмно-апаратних засобів із широким використанням алгорит- мів закриття інформації. Фізичні засоби захисту – це різноманітні пристрої, конструкції, апарати, вироби, призначені для створення перепон на шляху руху зловмисників.

***Фізичні засоби захисту*** – це різноманітні пристрої, конструкції, апа- рати, вироби, призначені для створення перепон на шляху руху зловмисни- ків. До фізичних засобів відносяться механічні, електромеханічні, елект- ронні, електронно-оптичні, радіо- і радіотехнічні та інші пристрої для забо- рони несанкціонованого доступу (входу, виходу), пронесення (винесення) засобів і матеріалів та інших можливих видів злочинних дій.

Ці засоби застосовуються для вирішення таких завдань:

* охорона території підприємства та спостереження за нею;
* охорона будівель, внутрішніх приміщень та контроль за ними;
* охорона обладнання, продукції, фінансів та інформації;
* здійснення контрольованого доступу до будівель та приміщень.

Усі фізичні засоби захисту об’єктів можна поділити на три категорії: засоби попередження, засоби виявлення та системи ліквідації загроз.

Охоронна сигналізація та охоронне телебачення, наприклад, відно- сяться до засобів виявлення загроз; загорожі навколо об’єктів – це засоби попередження несанкціонованого проникнення на територію, а підсилені двері, стіни, стелі, грати на вікнах та інші заходи служать захистом також і від проникнення, і від інших злочинних дій (підслуховування, обстрілу, ки- дання гранат і т. ін.).

Засоби пожежогасіння належать до систем ліквідації загроз. У загаль- ному випадку за фізичною природою та функціональним призначенням усі засоби цієї категорії можна поділити на такі групи: охоронні та охоронно- пожежні системи; охоронне телебачення; охоронне освітлення; засоби фі- зичного захисту.

До засобів фізичного захисту належать:

* природні та штучні перепони (бар’єри);
* особливі конструкції периметрів, проходів, віконних та дверних прорізів, приміщень, сейфів, сховищ і т. ін.;

- зони безпеки.

Природні та штучні бар’єри призначені для протидії незаконному проникненню на територію об’єкта. Проте основне захисне навантаження лягає все ж таки на штучні бар’єри, такі як паркани та інші види огорож. Практика показує, що огорожі складної конфігурації здатні затримати зло- вмисника на достатньо тривалий час. На сьогодні нараховується значний арсенал таких засобів: від простих сітчастих до складних комбінованих ого- рож, які здійснюють певний вплив відлякування на порушника.

***Зони безпеки*** повинні розташовуватися на об’єкті послідовно, від ого- рожі навкруг території об’єкта до сховищ цінностей, створюючи ланцюг перешкод (рубежів), які доведеться долати зловмисникові. Від складності та надійності перепони на його шляху залежить проміжок часу, необхід- ного на подолання кожної зони, та ймовірність того, що розташовані в ко- жній зоні засоби виявлення (охоронні пости, охоронна сигналізація та охо- ронне телебачення) виявлять наявність порушника та подадуть сигнал три- воги.

Основу планування та обладнання зон безпеки об’єкта становлять

принцип рівноміцності меж зон безпеки. Сумарна міцність зон безпеки буде оцінюватися найменшою з них.

Останніми роками велика увага надається створенню систем фізич- ного захисту, сполучених із системами сигналізації.

***До апаратних засобів захисту інформації*** відносяться найрізнома- нітніші за принципом дії, побудовою та можливостями технічні конструк- ції, які забезпечують припинення розголошення, захист від витоку та про- тидію несанкціонованому доступові до джерел конфіденційної інформації. ***Апаратні засоби захисту інформації*** – це різноманітні технічні при- строї, системи та споруди, призначені для захисту інформації від розголо- шення, витоку і несанкціонованого доступу. Для захисту центральних про- цесорів (ЦП) застосовується кодове резервування – створення додаткових бітів у форматах машинних команд (розрядів секретності) і резервних ре- гістрів (у пристроях ЦП). Одночасно передбачаються два можливих ре- жими роботи процесора, які відділяють допоміжні операції від операцій

безпосереднього вирішення задач користувача. Для цього служить спеціа- льна програма переривань, яка реалізується апаратними засобами.

Одним із заходів апаратного захисту ПК та інформаційних мереж є обмеження доступу до оперативної пам’яті за допомогою встановлення меж або полів. Для цього створюються регістри контролю та регістри захи- сту даних. Застосовуються також додаткові біти парності – різновид мето- дів кодового резервування. Для позначення ступеню конфіденційності про- грам і даних, категорій користувачів використовуються біти, які назива- ються бітами конфіденційності (це два-три додаткових розряди, за допомо- гою яких кодуються категорії секретності користувачів, програм, даних).

Програми та дані, які завантажуються в ОЗП, потребують захисту, що гарантує їх від несанкціонованого доступу. Часто використовуються біти парності, ключі, постійна спеціальна пам’ять.

Апаратні засоби захисту застосовуються й у терміналах користувачів. Для попередження витоку інформації при приєднанні незареєстрованого терміналу необхідно перед видачею запитуваних даних здійснити іденти- фікацію (автоматичне визначення коду або номера) терміналу, з якого пос- тупив запит. У багато користувальницькому режимі цього терміналу його ідентифікації недостатньо. Необхідно здійснити аутентифікацію користу- вача, тобто встановити його дійсність та повноваження. Це необхідно й тому, що різні користувачі, зареєстровані в системі, можуть мати доступ тільки до окремих файлів, і суворо обмежені повноваження їхнього вико- ристання. Для ідентифікації термінала найчастіше застосовується генера- тор коду, включений до апаратури терміналу, а для аутентифікації корис- тувача - такі апаратні засоби як ключі, персональні кодові картки, персона- льний ідентифікатор, пристрої розпізнавання голосу користувача або фо- рми його пальців. Проте найбільш поширеними засобами аутентифікації є паролі, перевірені не апаратними, а програмними засобами впізнавання.

***Апаратні засоби захисту інформації*** - це різноманітні технічні при-

строї, системи та споруди, призначені для захисту інформації від розголо- шення, витоку й несанкціонованого доступу.

***Програмний захист інформації*** - це система спеціальних програм, які входять до складу програмного забезпечення та реалізують функції за- хисту інформації. Виділяють такі напрями використання програм для забез- печення безпеки конфіденційної інформації: захист інформації від несанк- ціонованого доступу; захист інформації від копіювання; захист програм від вірусів; захист інформації від вірусів; програмний захист каналів зв’язку.

Програмні засоби захисту мають такі різновиди спеціальних програм: ідентифікації технічних засобів, файлів та аутентифікації користувачів; ре- єстрації та контролю роботи технічних засобів та користувачів; обслугову- вання режимів обробки інформації з обмеженим доступом; захисту

операційних систем ПК та прикладних програм користувачів; знищення інформації у запам’ятовуючих пристроях після використання; допоміжні програми захисту різноманітного призначення.

## Криптографічні засоби захисту.

***Криптографія*** (від грец. – «секретний, прихований» і – «пишу, кре- слю, малюю») – спосіб тайнопису, заснований на використанні шифру, де під шифром зазвичай розуміють сукупність обернених перетворень тексту повідомлень, які виконуються з метою схову від зловмисника (противника) інформації, яка міститься в повідомленні.

Криптографія включає декілька розділів сучасної математики, а також спеціальні галузі фізики, теорії інформації та зв’язку і деяких інших суміж- них дисциплін. Як наука про шифри, криптографія довгий час була засек- речена, оскільки застосовувалася переважно для захисту державних і воєн- них секретів. Проте на теперішній час методи та засоби криптографії вико- ристовуються для забезпечення інформаційної безпеки не тільки держави, але і приватних осіб та організацій.

Для криптографічного перетворення інформації використовуються різноманітні шифрувальні засоби, такі як засоби шифрування документів, засоби шифрування мови, засоби шифрування телеграфних повідомлень та передачі даних.

Апаратні, програмні, апаратно-програмні та криптографічні засоби реалізують ті чи інші послуги інформаційної безпеки різноманітними меха- нізмами захисту, які забезпечують дотримання конфіденційності, цілісно- сті, доступності та повноти інформації.

# Питання для самоконтролю

1. Які напрями захисту інформації ви знаєте?
2. Сформулюйте поняття права.
3. Яка структура правових актів, які орієнтовані на правовий захист інформації?
4. Дати визначення ліцензії.
5. Що таке комерційна таємниця?
6. Які завдання вирішує організаційний захист?
7. Назвіть основні організаційні заходи.
8. Які функції виконує служба безпеки підприємства (фірми, організації)?
9. В чому полягають завдання служби безпеки підприємства (фірми, організації)?
10. Що таке інженерно-технічний захист? Які завдання він виконує?
11. Визначте фізичні засоби захисту та їх завдання.
12. Які апаратні засоби захисту інформації Ви знаєте?
13. Що таке криптографія?
14. Назвіть переваги цифрового шифрування.

# Розділ 10. ЗАХИСТ ІНФОРМАЦІЙНИХ СИСТЕМ

* 1. Джерела конфіденційної інформації.
  2. Інформаційна система як об’єкт захисту.
  3. Рівні захисту інформаційних систем.
  4. Основні принципи захисту інформаційних систем.

# Джерела конфіденційної інформації

***Джерело інформації*** – це матеріальний об’єкт, що володіє певними відомостями (інформацією), що становлять конкретний інтерес для сторон- ніх осіб. Взагалі джерелами конфіденційної інформації можна вважати такі категорії:

1. Люди (співробітники, обслуговуючий персонал, продавці, клієнти та ін.).
2. Документи будь-якого призначення.
3. Публікації: доповіді, статті, інтерв’ю, проспекти, книги та ін.
4. Технічні носії інформації й документів.
5. Технічні засоби обробки інформації.
6. Продукція, що випускається.
7. Виробничі й промислові відходи.

***Люди, як джерела конфіденційної інформації***, посідають особливе місце, як активні елементи, здатні виступати не тільки власниками конфі- денційної інформації, але й суб’єктами зловмисних дій. Люди є і власни- ками, і поширювачами інформації в межах своїх функціональних обов’яз- ків. Вони володіють важливою інформацією, вони ще здатні її аналізувати, узагальнювати, робити відповідні висновки, а також, за певних умов, при- ховувати, красти, продавати та виконувати інші кримінальні дії, аж до вступу в злочинні зв’язки зі зловмисниками.

***Документи*** – це найпоширеніша форма обміну інформацією, її нагро- мадження та зберігання. Під документом розуміють матеріальний носій ін- формації (папір, кіно- і фотоплівка, магнітна стрічка тощо) із зафіксованою на ньому інформацією, призначеною для її використання в часі й просторі. Документ має досить різноманітне функціональне призначення. Він може бути представлений не тільки різним змістом, але й різними фізичними фо- рмами.

За спрямованістю розрізняють *організаційно-розпорядницькі, планові, статистичні, бухгалтерські й науково-технічні документи*, що містять, по суті, всю масу відомостей про склад, стан і діяльність будь-якої організа- ційної структури від державного до індивідуального рівня, про будь-який виріб, товар, задум, розробку.

***Публікації*** – це інформаційні носії у вигляді різноманітних видань, вони поділяються на первинні та вторинні.

*До первинних* належать книги, статті, періодичні видання, збірники, нау- ково-технічні звіти, дисертації, рекламні проспекти, доповіді та ін.

*До вторинних* – інформаційні карти, реферативні журнали, експрес-ін- формацію, огляди, бібліографічні покажчики, каталоги та ін.

Інформація може бути фіксованою та нефіксованою.

*Фіксована інформація* – це відомості, закріплені на якому-небудь фізич- ному носії. Фіксована інформація різниться залежно від виду носія, на якому вона перебуває.

*Нефіксована інформація* – це знання, якими володіють учені, фахівці, працівники, які так чи інакше беруть участь у виробництві та здатні пере- давати ці знання іншим.

***До технічних носіїв інформації*** відносяться паперові носії, кіно- і фотоматеріали (мікро- і кінофільми), магнітні носії (дискети, жорсткі ди- ски, стримери), відеозапис, інформація на екранах ПК, на табло колектив- ного користування, на екранах промислових телевізійних установок і інших засобів.

За специфікою призначення й виконання ***технічні засоби обробки ін- формації*** можна поділити на дві великі групи:

1. технічні засоби забезпечення виробничої і трудової діяльності;
2. технічні засоби автоматизованої обробки інформації.

До групи засобів забезпечення виробничої і трудової діяльності вхо- дять різноманітні технічні засоби, такі, наприклад, як телефонні апарати й телефонний зв’язок; телеграфний, фототелеграфний і факсимільний зв’язок; системи радіозв’язку (автономні, територіальні, релейні, супутни- кові й ін.); телевізійні (у тому числі і засоби промислового телебачення); радіоприймачі та радіотрансляційні системи та інші засоби й системи.

Усі ці засоби можуть бути джерелами перетворення акустичних сиг- налів, що містять комерційні секрети, в електричні й електромагнітні поля, здатні утворити електромагнітні канали витоку охоронюваних відомостей.

Особливу групу технічних засобів становлять автоматизовані системи обробки інформації (АСОІ).

Привабливість ПК і інформаційних систем як джерел конфіденційної інформації зумовлена певними об’єктивними особливостями, до числа яких відносяться:

* різке розширення сфери застосування інформаційної й обчислювальної техніки (ПК, локальні й розподілені інформаційні мережі національного й міжнародного масштабу);
* збільшення обсягів оброблюваної й збереженої інформації в локальних і розподілених банках даних;
* збільшення числа користувачів ресурсами ПК та мереж.

Привабливість полягає ще й у тому, що АСОІ містить досить значні асортименти інформації. В її базах даних є вся інформація про конкретне підприємство – від досьє на співробітників до конкретної продукції, її ха- рактеристики, вартості та інші відомості.

***Продукти праці*** виступають джерелами інформації, за якою досить активно полюють конкуренти. Особливу увагу звертають конкуренти на нову продукцію, що перебуває на стадії підготовки до виробництва.

Виробництво будь-якої продукції визначається етапами «життєвого циклу»: ідеєю, макетом, дослідним зразком, випробуваннями, серійним ви- робництвом, експлуатацією, модернізацією та зняттям з виробництва. Ко- жен із цих етапів супроводжується специфічною інформацією, що проявля- ється різними фізичними ефектами, які у вигляді характеристик (демаску- ючих ознак) можуть розкрити охоронювані відомості про вироблений то- вар.

***Відходи виробництва***, так званий непридатний матеріал, можуть ба- гато розповісти про використовувані матеріали, їхній склад, особливості виробництва, технології. До них можливий доступ через смітники, місця збору металобрухту, ящики відходів дослідницьких лабораторій, сміттєві кошики кабінетів. Не менш серйозними джерелами конфіденційної інфор- мації є *промислові відходи*: стружка, обрізки, зіпсовані заготівлі, поламані комплектуючі та ін. Аналіз відходів допоможе довідатися про особливості виробництва, технології.

Як кожне окремо, так і в сукупності джерела конфіденційної інфор- мації містять досить повні відомості про склад, стан і напрямки діяльності підприємства.

# Інформаційна система як об’єкт захисту

Загалом інформація являє собою незамінну сировину для вироблення будь-якого рішення, яку необхідно добути, переробити та поставити до за- кінчення терміну придатності тому, кому вона потрібна, тобто цінні відо- мості, що добуваються на превелику силу, повинні вчасно надійти тому, кому вони необхідні, оскільки інформація корисна тільки тоді, коли її мо- жна використовувати для прийняття серйозних рішень. Усе це визначає не- обхідність впровадження складних систем збору, обробки й аналізу різної інформації.

При вирішенні проблеми задоволення інформаційної потреби необхі- дно враховувати три компоненти:

* + - *людину* (споживача інформації), що формулює свої задачі;
    - *інформаційний фонд* (інформаційний ресурс), у якому зосереджена необхідна людині інформація;
    - *відповідний пристрій*, що є посередником між споживачем і інфор- маційним масивом.

Набір перелічених компонентів являє собою інформаційну систему. Інформаційна система має певну структуру, склад, фахівців, засоби,

обладнання й порядок функціонування.

*Продуктом інформаційної системи* є інформація, властивості якої змінюються відповідно до заданої технології за допомогою комплексу різ- них технічних засобів і людей, що виконують певні технологічні операції.

Технологічні операції – це сукупність дій, спрямованих на зміну стану предмета виробництва.

*В інформаційній системі предметом виробництва є інформація, що на виході системи набуває потрібного користувачу вигляду та змісту.*

У структуру інформаційної системи входять такі складові:

1. Користувачі.
2. Інформаційні ресурси, документи та масиви документів у різних формах та видах (бібліотеки, архіви, фонди, бази даних, бази знань, а також інші форми організації та зберігання інформації), які містять інформацію про всі напрямки життєдіяльності суспільства.
3. Носії інформації: на паперовій основі; звуконосії; відеоносії; магнітні носії; спеціальні технічні носії.
4. Засоби збору, зберігання та обробки інформації - традиційні технічні за- соби (телефон, радіо, звукопідсилювальні системи, поліграфія) та автома- тизовані системи.
5. Засоби передачі інформації (дротові, радіо, волоконно-оптичні).

Вихідною матеріальною основою роботи інформаційної системи висту- пають інформаційні ресурси. Ресурсами, як відомо, називають елементи економічного потенціалу, які перебувають у власності суспільства і які у разі необхідності можуть бути використані для досягнення конкретних ці- лей господарського й соціального розвитку.

Інформаційні ресурси можуть бути фіксованими й нефіксованими. Фік- совані інформаційні ресурси являють собою інформацію, закріплену на якому-небудь фізичному носії, а нефіксовані – знання, якими володіють люди (учені, фахівці, працівники), що беруть участь у суспільному вироб- ництві та здатні передавати ці знання іншим учасникам виробничого про- цесу.

*Об’єктом захисту* виступає *інформаційна система*

*Предмет* захисту інформації в інформаційній системі - *інформація*. Для інформаційних систем як об’єктів безпеки властиві такі характерис-

тики: *конфіденційність, доступність та цілісність інформації (даних) в ін- формаційній системі.*

*Конфіденційність інформації* (даних) в інформаційній системі – це властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і (або) процесом інформаційної системи. Інформація зберігає конфіденційність, якщо дотримуються вста- новлені правила ознайомлення з нею.

*Доступність даних в інформаційній системі* – це властивість даних, що полягає в можливості їхнього отримання користувачем або програмою.

Визначається певними факторів: *можливістю працювати за терміналом, володінням паролем, знанням мови запитів та ін.*

*Цілісність –* це внутрішня єдність, пов’язаність усіх частин інформа- ційних ресурсів при їх обробці, зберіганні та передачі, як одного цілого в інформаційній системі. Тобто це стан даних, або інформаційної системи, коли дані та програми використовуються встановленим чином, що забезпе- чує:

стійку роботу системи;

автоматичне відновлення у випадку виявлення системою потенційної помилки;

автоматичне використання альтернативних компонентів замість тих, що вийшли з ладу.

Для інформаційної системи можна розглядати такі поняття, *як ціліс- ність даних, цілісність інформації, цілісність бази даних, цілісність інфо- рмаційної системи.*

***Цілісність даних в інформаційній системі*** – це стан, за якого дані, що зберігаються в системі, в точності відповідають даним у вихідних доку- ментах; властивість, що має відношення до набору даних і означає, що дані не можуть бути змінені або зруйновані без санкції на доступ. Цілісність да- них вважається збереженою, якщо дані не спотворені й не зруйновані (сте- рті).

***Цілісність інформації*** – це властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим корис- тувачем і (або) процесом.

***Цілісність бази даних*** – це стан бази даних, коли всі значення даних правильні в тому сенсі, що відображають стан реального світу (в межах за- даних обмежень по точності та часовій узгодженості) і підпорядковуються правилам взаємної несуперечності. Підтримка цілісності бази даних міс- тить перевірку цілісності й відновлення з будь-якого неправильного стану, яке може бути виявлено; це входить у функції адміністратора бази даних.

***Цілісність системи*** – це властивість системи, яка полягає в тому, що жоден її компонент не може бути усунений, модифікований або доданий із порушенням політики безпеки.

***Захищена інформаційна система*** – інформаційна система, яка для певних умов експлуатації забезпечує безпеку (конфіденційність, цілісність) інформації, що функціонує в системі, та підтримує свою працездатність в умовах впливу на неї заданої множини загроз.

# Рівні захисту інформаційних систем

Побудова надійного захисту інформаційної системи неможлива без попереднього аналізу можливих загроз безпеки системи.

Цей аналіз повинен складатися з таких етапів:

* виявлення характеру інформації, яка зберігається в системі;
* оцінки цінності інформації, яка зберігається в системі;
* побудови моделі зловмисника;
* визначення та класифікації загроз інформації в системі (несанкціоноване зчитування, несанкціонована модифікація);
* визначення затрат часу і матеріальних ресурсів на злам системи, припус- тимих для зловмисників;
* оцінки припустимих витрат часу, засобів і ресурсів системи на організа- цію її захисту.

Система захисту інформації повинна виконувати такі функції:

* реєстрація й облік користувачів, носіїв інформації, інформаційних маси- вів;
* забезпечення цілісності прикладного програмного забезпечення;
* захист комерційної таємниці, включаючи використання сертифікованих засобів криптографічного захисту;
* створення захищеного електронного документообігу з використанням сертифікованих засобів криптографічні перетворення й електронного під- пису;
* централізоване управління системою захисту інформації;
* управління доступом;
* забезпечення ефективного антивірусного захисту тощо.

# Комплекс вимог, які висуваються до системи безпеки:

1. ***На рівні користувача*** повинно бути забезпечено допуск тільки автори- зованих абонентів до роботи в інформаційний системі, створено захисну оболонку навколо її елементів, а також організовано індивідуальне захи- щене середовище діяльності кожного користувача.
2. ***На мережевому рівні*** організовується захищений інформаційний обмін даними між автоматизованими робочими місцями, а також створюється на- дійна оболонка фізичного захисту периметра розташування ІС загалом. Си- стема захисту на цьому рівні повинна будуватись з урахуванням реалізації захисту на попередніх рівнях.
3. ***На локальному рівні*** організовується розподілення інформаційних ресу- рсів ІС на сегменти за рівнями конфіденційності по територіальному і фу- нкціональному принципах, а також виділяється в окремий сегмент засоби обробки конфіденційної інформації. Підвищенню рівня захищеності сприяє обмеження й мінімізація кількості точок входу/виходу (точок взаємодії) між сегментами, створення надійної оболонки по периметру сегментів і ін- формаційної системи загалом, організація захищеного обміну інформацією між сегментами.
4. ***Захист на технологічному рівні*** (програмний продукт і технічні засоби обробки інформації). Система захисту на цьому рівні повинна бути автоно- мною, але забезпечувати реалізацію єдиної політики безпеки й будуватись

на основі використання сукупності вбудованих систем захисту операційної системи і систем управління базами даних та знань.

1. ***Організація захисту на фізичному рівні*** повинна зменшити можливість несанкціонованих дій сторонніх осіб і персоналу підприємства, а також зменшити вплив техногенних джерел.

# Основні принципи захисту інформаційних систем

До основних принципів захисту інформаційних систем відносяться:

*Принцип виправданості доступу* – користувач повинен мати доста- тню «форму допуску» для отримання інформації того рівня конфіденційно- сті, що він вимагає, і ця інформація дійсно необхідна йому для виконання виробничих функцій.

*Принцип достатньої глибини контролю доступу*. Засоби захисту ін- формації повинні включати механізми контролю доступу до всіх видів ін- формаційних і програмних ресурсів ІС, які у відповідності з принципом ви- правданості доступу слід розмежовувати між користувачами.

*Принцип цілісності засобів захисту.* Цей принцип передбачає, що за- соби захисту інформації в ІС повинні чітко виконувати свої функції згідно з переліченими принципами й бути ізольованими від користувачів, а для свого супроводу повинні включати спеціальний захищений інтерфейс для засобів контролю, сигналізації про спроби порушення захисту інформації і впливу на процеси в системі.

Реалізація перелічених принципів здійснюється з допомогою так зва- ного ***«монітору звернень»,*** який контролює будь-які запити до даних чи програм з боку користувачів (чи їх програм) за установленими для них ви- дами доступу до цих даних і програм.

# Питання для самоконтролю

1. Які існують категорії джерел конфіденційної інформації?
2. Які складові має інформаційна система?
3. Розкрийте поняття «цілісність».
4. Розкрийте поняття «доступність».
5. Розкрийте поняття конфіденційності інформації.
6. Назвіть основні напрями забезпечення безпеки інформації.
7. Розкрийте зміст моделі системи захисту інформації.
8. Якими показниками може бути оцінено якість розподілу доступу?
9. Назвіть основні принципи та рівні захисту інформаційних систем.
10. Розкрийте поняття інформаційно-комунікаційної системи.
11. Назвіть рівні інформаційно-комунікаційних мереж.
12. Визначить сутність випадкового методу доступу до ресурсів системи.
13. В чому полягають основні завдання захисту інформації в мережі?
14. Розкрийте різновиди побудови комп’ютерних мереж.
15. Що повинні включати угоди обміну програмним забезпеченням?
16. Назвіть заходи управління обробкою й зберіганням інформації.

# Розділ 11. ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ

* 1. Інформаційна безпека та її місце в системі національній безпеки Ук- раїни.
  2. Основні реальні та потенційні загрози інформаційній безпеці України.
  3. Стан та перспективи розвитку інформаційної безпеки.

# Інформаційна безпека та її місце в системі національної без- пеки України

Необхідною умовою нормального існування й розвитку кожного сус- пільства є захищеність від зовнішніх і внутрішніх загроз, стійкість до спроб зовнішнього тиску, як здатність протистояти таким спробам і нейтралізу- вати загрози, що виникають, так і забезпечувати такі внутрішні і зовнішні умови існування країни, які гарантують можливість стабільного і всебіч- ного прогресу суспільства і його громадян.

Для характеристики цього стану використовується поняття націона- льної безпеки. Законом України «Про національну безпеку України» ви- значаються та розмежовуються повноваження державних органів у сферах національної безпеки й оборони, створюється основа для інтеграції полі- тики та процедур органів державної влади, інших державних органів, фун- кції яких стосуються національної безпеки й оборони, сил безпеки і сил оборони, визначається система командування, контролю та координації операцій сил безпеки і сил оборони, запроваджується всеосяжний підхід до планування у сферах національної безпеки й оборони, забезпечуючи в та- кий спосіб демократичний цивільний контроль над органами та формуван- нями сектору безпеки й оборони.

Згідно з цим Законом ***під національною безпекою України*** слід розу-

міти захищеність державного суверенітету, територіальної цілісності, де- мократичного конституційного ладу та інших національних інтересів Ук- раїни від реальних та потенційних загроз.

***Національні інтереси України*** – життєво важливі інтереси людини, суспільства й держави, реалізація яких забезпечує державний суверенітет України, її прогресивний демократичний розвиток, а також безпечні умови життєдіяльності й добробут її громадян.

***Воєнна безпека*** – захищеність державного суверенітету, територіаль- ної цілісності і демократичного конституційного ладу та інших життєво ва- жливих національних інтересів від воєнних загроз.

***Громадська безпека і порядок*** – захищеність життєво важливих для суспільства та особи інтересів, прав і свобод людини та громадянина,

забезпечення яких є пріоритетним завданням діяльності сил безпеки, ін- ших державних органів, органів місцевого самоврядування, їх посадових осіб та громадськості, які здійснюють узгоджені заходи щодо реалізації й захисту національних інтересів.

***Державна безпека*** – захищеність державного суверенітету, територі- альної цілісності і демократичного конституційного ладу та інших життєво важливих національних інтересів від реальних і потенційних загроз нево- єнного характеру.

***Загрози національній безпеці України*** – явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України.

Законодавчою основою забезпечення національної безпеки є Консти- туція України, закони України, укази Президента України, ухвали й розпо- рядження Кабінету Міністрів України, інші нормативно-правові акти дер- жавних органів влади й управління, прийняті в межах їх компетенції в цій сфері; міжнародні договори й угоди визнані Україною.

Основним суб’єктом забезпечення безпеки є держава, що здійснює функції в цій сфері через органи законодавчої, виконавчої і судової влади.

До основних об’єктів безпеки відносяться:

*особа* – її права та свободи;

*суспільство* – його матеріальні й духовні цінності;

*держава* – її конституційний лад, суверенітет і територіальна ціліс- ність.

Громадяни, суспільні й інші організації та об’єднання є суб’єктами безпеки, володіють правами й обов’язками з участі в забезпеченні безпеки.

# Основними принципами забезпечення безпеки є:

законність; дотримання балансу життєво важливих інтересів особи, суспільства і держави; взаємна відповідальність особи, суспільства і дер- жави із забезпечення безпеки; інтеграція з міжнародними системами без- пеки.

Систему національної безпеки утворюють: органи законодавчої, ви- конавчої і судової влади; державні, суспільні й інші організації та об’єд- нання; громадяни, що беруть участь у забезпеченні безпеки відповідно до закону; законодавство, що регламентує відносини у сфері безпеки; сили за- безпечення безпеки.

Для безпосереднього виконання функцій забезпечення національної безпеки в системі виконавчої влади створюються і діють сили забезпечення національної безпеки. Сили забезпечення безпеки включають: правоохо- ронні та розвідувальні органи, державні органи спеціального призначення з правоохоронними функціями, сили цивільного захисту та інші органи, на

які Конституцією та законами України покладено функції із забезпечення національної безпеки України.

Національна безпека досягається проведенням єдиної державної полі- тики у сфері забезпечення безпеки, системою заходів економічного, полі- тичного й іншого характеру, адекватних загрозам життєво важливих інте- ресів особи, суспільства і держави. Оскільки в умовах інформатизації кра- їни, розвитку інформаційних технологій, інформаційні ресурси форму- ються в усіх сферах діяльності, і насамперед у політичній, військовій, еко- номічній, науково-технічній, інформаційну безпеку треба розглядати як комплексний показник національної безпеки. Цим визначається її важливе місце й одна з провідних ролей у системі національної безпеки країни в сучасних умовах.

Отже, у сучасних умовах важливою складовою національної безпеки

є інформаційна безпека України, що є станом захищеності національних інтересів у інформаційній сфері.

# Основні реальні та потенційні загрози інформаційній безпеці України

До головних чинників, що впливають на стан морально-ідеологічної стабільності та безпеки в Україні, належать:

* + - * відсутність цілісної системи інформаційно-аналітичного забезпе- чення органів державної влади й управління;
      * руйнування інтелектуального потенціалу, неготовність системи освіти до підтримання процесів випереджувального розвитку держави;
      * повільність процесів усвідомлення прошарком колишньої радянсь- кої партійно-господарчої номенклатури, наукової й творчої інтелігенції, па- ростками нової буржуазії свого місця в суспільстві та формування власне української еліти, що призводить до неможливості сформувати керівними колами зрозумілої й привабливої для суспільства національної ідеї;
      * низький загальний рівень розвитку інформаційної інфраструктури, що не виключає ймовірність експансії іноземних компаній на ринку інфор- маційних послуг;
      * руйнування національного інформаційною простору та виникнення можливості його використання в антидержавних інтересах;
      * недостатній професійний, інтелектуальний і творчий рівень вітчиз- няних виробників інформаційного продукту та послуг, їхня не конкуренто- спроможність на світовому інформаційному ринку;
      * інформаційна експансія провідних іноземних держав, розроблення й використання ними, міжнародними чи вітчизняними злочинними організа- ціями різних сучасних способів безпосереднього підриву;
      * мало контрольована діяльність окремих політичних сил, ЗМІ та осіб, спрямована на руйнування моральних цінностей, підрив морального й фі- зичного здоров’я нації;
      * використання ЗМІ з позицій, протилежних інтересам громадян, по- літичних і громадських організацій, держави: втрата довіри до влади з боку значної частини населення внаслідок поширення компромату, застосу- вання «брудних» політичних технологій, особливо під час виборчих кампа- ній;
      * конкурентна боротьба за володіння ЗМІ, процес їхньої монополізації й концентрації інформаційної та політичної влади;
      * маніпулювання громадською думкою (шляхом дезінформації, пе- рекручування даних, замовчування правдивих відомостей тощо).

Відсутність цілісної системи інформаційно-аналітичного забезпе- чення органів влади та управління значно ускладнює прийняття ними зва- жених. науково обґрунтованих рішень, що породжує конфліктні ситуації у владних структурах. Недостатнє інформаційно-аналітичне забезпечення ді- яльності характерне для всіх державних органів як на центральному, так і на регіональному рівнях. Владні структури не мають достатніх можливос- тей завчасно прогнозувати розвиток подій у державі та навколо неї, належ- ним чином враховувати сприятливі й обмежувати несприятливі фактори, що визначають результативність прийнятих політичних рішень, здійсню- вати планування навіть на середньострокову перспективу. Організація ро- боти інформаційно-аналітичних підрозділів дотепер не має системного ха- рактеру, а в періоди чергових скорочень чисельності державних органів ді- яльність деяких таких підрозділів взагалі припиняється.

*Основними реальними та потенційними загрозами інформаційній*

*безпеці України є:*

1. у зовнішньополітичній сфері: поширення у світовому інформацій- ному просторі викривленої, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України; прояви комп’ютерної зло- чинності, комп’ютерного тероризму, що загрожують стабільному та без- печному функціонуванню національних інформаційно-телекомунікаційних систем; зовнішні негативні інформаційні впливи на суспільну свідомість і засоби масової інформації, а також Інтернет;
2. у сфері державної безпеки: негативні інформаційні впливи, спря- мовані на підрив конституційного ладу, суверенітету, територіальної ціліс- ності й недоторканності кордонів України; використання засобів масової інформації, Інтернету для пропаганди сепаратизму за етнічною, мовною, релігійною й іншими ознаками; несанкціонований доступ до інформацій- них ресурсів органів державної влади; розголошення інформації, яка ста- новить державну та іншу передбачену законодавством таємницю, а також конфіденційної інформації, що є власністю держави;
3. у воєнній сфері: порушення встановленого регламенту збирання, оброблення й передавання інформації з обмеженим доступом в органах вій- ськового управління та на підприємствах оборонно-промислового компле- ксу України; несанкціонований доступ до інформаційних ресурсів, неза- конне збирання та використання інформації з питань оборони; реалізація програмно-математичних заходів із метою порушення функціонування ін- формаційних систем у сфері оборони України; перехоплення інформації в телекомунікаційних мережах, радіоелектронне глушіння засобів зв’язку та управління; інформаційно-психологічний вплив на населення України, у тому числі особовий склад військових формувань, із метою послаблення їх готовності до оборони держави та погіршення іміджу військової служби;
4. у внутрішньополітичній сфері: недостатня розвиненість інститутів

громадянського суспільства, недосконалість партійно-політичної системи, непрозорість політичної та громадської діяльності, що створює передумови для обмеження свободи слова, маніпулювання суспільною свідомістю; не- гативні інформаційні впливи, у тому числі із застосуванням спеціальних засобів, на індивідуальну та суспільну свідомість; поширення суб’єктами інформаційної діяльності викривленої, недостовірної та упередженої інфо- рмації;

1. в економічній сфері: відставання вітчизняних наукоємних і висо- котехнологічних виробництв, особливо у сфері телекомунікаційних засо- бів і технологій; недостатній рівень інформатизації економічної сфери, зо- крема кредитно-фінансової системи, промисловості, сільського господарс- тва, сфери державних закупівель; несанкціонований доступ, порушення встановленого порядку роботи з інформаційними ресурсами в галузях на- ціональної економіки, викривлення інформації в таких ресурсах; викорис- тання неліцензованого програмного забезпечення, засобів і комплексів об- роблення інформації; недостатній рівень розвитку національної інформа- ційної інфраструктури;
2. у соціальній та гуманітарній сферах: відставання України від роз- винутих держав за рівнем інформатизації соціальної та гуманітарної сфер, насамперед освіти, охорони здоров’я, соціального забезпечення, культури; недодержання прав людини і громадянина на отримання інформації, необ- хідної для захисту їхніх соціально-економічних прав; поширення в ЗМІ не властивих українській культурній традиції цінностей і способу життя, культу насильства, жорстокості, порнографії, зневажливого ставлення до людської й національної гідності; тенденція до витіснення з інформацій- ного простору та молодіжної культури українських мистецьких творів, на- родних традицій і форм дозвілля; послаблення суспільно-політичної, міже- тнічної та міжконфесійної єдності суспільства; відставання розвитку укра- їнського кінематографу, книговидання, книгорозповсюдження й бібліотеч- ної справи від рівня розвинутих держав;
3. у науково-технічній сфері: зниження наукового потенціалу в галузі інформатизації та зв’язку; низька конкурентоспроможність вітчизняної ін- формаційної продукції на світовому ринку; відтік за кордон наукових ка- дрів і суб’єктів права інтелектуальної власності; недостатній захист від не- санкціонованого доступу до інформації внаслідок використання іноземних інформаційних технологій і техніки; неконтрольована експансія сучасних інформаційних технологій, що створює передумови технологічної залеж- ності України;
4. в екологічній сфері: приховування, несвоєчасне надання інформа- ції або надання недостовірної інформації населенню про надзвичайні еко- логічні ситуації чи надзвичайні ситуації техногенного та природного хара- ктеру; недостатня надійність інформаційно-телекомунікаційних систем збору, обробки й передачі інформації в умовах надзвичайних ситуацій; ни- зький рівень інформатизації органів державної влади, що унеможливлює здійснення оперативного контролю та аналізу стану потенційно небезпеч- них об’єктів і територій, завчасного реагування на надзвичайні ситуації.

Діяльність органів виконавчої влади у сфері забезпечення інформа- ційної безпеки України має бути зосереджена на конструктивному поєд- нанні діяльності держави, громадянського суспільства та людини за трьома головними напрямами: інформаційно-психологічному, зокрема щодо за- безпечення конституційних прав і свобод людини й громадянина, ство- рення сприятливого психологічного клімату в національному інформацій- ному просторі для затвердження загальнолюдських та національних мора- льних цінностей; технологічного розвитку, зокрема стосовно розбудови та інноваційного оновлення національних інформаційних ресурсів, впрова- дження новітніх технологій створення, оброблення та поширення інформа- ції; захисту інформації, зокрема щодо забезпечення конфіденційності, ці- лісності й доступності інформації, у тому числі технічного захисту інфор- мації в національних інформаційних ресурсах від кібернетичних атак.

# Стан та перспективи розвитку інформаційної безпеки Укра-

**їни**

Відповідно до законодавства України, інформаційна безпека має таке

визначення: «стан захищеності життєво важливих інтересів людини, суспі- льства і держави, при якому запобігається нанесення шкоди через непов- ноту, невчасність та невірогідність інформації, що використовується; нега- тивний інформаційний вплив; негативні наслідки застосування інформацій- них технологій; несанкціоноване поширення, використання, порушення ці- лісності, конфіденційності та доступності інформації».

Інформаційна безпека означає:

* законодавче формування державної інформаційної політики;
* створення відповідно до законів України можливостей досягнення інформаційної достатності для ухвалення рішень органами державної

влади, громадянами та об’єднаннями громадян, іншими суб’єктами права в Україні;

* гарантування свободи інформаційної діяльності та права доступу до інформації в національному інформаційному просторі України;
* всебічний розвиток інформаційної структури;
* підтримка розвитку національних інформаційних ресурсів України з урахуванням досягнень науки і техніки та особливостей духовно-культур- ного життя народу України;
* створення та впровадження безпечних інформаційних технологій;
* захист права власності всіх учасників інформаційної діяльності в на- ціональному просторі України;
* збереження права власності держави нестратегічні об’єкти інформа- ційної інфраструктури України;
* охорону державної таємниці, а також інформації з обмеженим дос- тупом, що є об’єктом права власності або об’єктом лише володіння, кори- стування чи розпорядження державою;
* створення загальної системи охорони інформації, зокрема охорони державної таємниці, а також іншої інформації з обмеженим доступом;
* захист національного інформаційного простору України від розпов- сюдження спотвореної або забороненої для поширення законодавством України інформаційної продукції;
* встановлення законодавством режиму доступу іноземних держав або їх представників до національних інформаційних ресурсів України та порядок використання цих ресурсів на основі договорів з іноземними дер- жавами;
* законодавче визначення порядку поширення інформаційної продук- ції зарубіжного виробництва на території України.

Державна політика інформаційної безпеки визначається пріоритетні- стю національних інтересів, системою небезпек і загроз та здійснюється шляхом реалізації відповідних доктрин, стратегій, концепцій і програм в інформаційній сфері відповідно до чинного законодавства.

## Пріоритетами державної політики в інформаційній сфері мають

бути:

1. щодо забезпечення інформаційної безпеки: створення інтегрованої

системи оцінки інформаційних загроз та оперативного реагування на них; удосконалення повноважень державних регуляторних органів, які здійс- нюють діяльність щодо інформаційного простору держави, з метою досяг- нення адекватного рівня спроможності держави відповідати реальним та потенційним загрозам національним інтересам України в інформаційній сфері; законодавче врегулювання механізму виявлення, фіксації, блоку- вання та видалення з інформаційного простору держави, зокрема з україн- ського сегмента мережі Інтернет, інформації, яка загрожує життю,

здоров’ю громадян України, пропагує війну, національну та релігійну во- рожнечу, зміну конституційного ладу насильницьким шляхом або пору- шення територіальної цілісності України, загрожує державному суверені- тету, пропагує комуністичний та/або націонал-соціалістичний (нацистсь- кий) тоталітарні режими та їхню символіку; визначення механізмів регу- лювання роботи підприємств телекомунікацій, поліграфічних підприємств, видавництв, телерадіоорганізацій, телерадіоцентрів та інших підприємств, установ, організацій, закладів культури та засобів масової інформації, а та- кож використання місцевих радіостанцій, телевізійних центрів та друка- рень для військових потреб і проведення роз’яснювальної роботи серед військ та населення; заборони роботи приймально-передавальних радіоста- нцій особистого та колективного користування і передачі інформації через комп’ютерні мережі в умовах запровадження правового режиму воєнного стану; оптимізація законодавчих механізмів реалізації зобов’язань України в межах Європейської конвенції про транскордонне телебачення щодо дер- жав, які не є підписантами зазначеної Конвенції; створення і розвиток стру- ктур, що відповідають за інформаційно-психологічну безпеку, насамперед у Збройних Силах України, з урахуванням практики держав – членів НАТО; розвиток і захист технологічної інфраструктури забезпечення інформацій- ної безпеки України; забезпечення повного покриття території України цифровим мовленням, насамперед у прикордонних районах, а також тим- часово окупованих територій; розвиток цифрового мовлення, унеможлив- лення впливу на його інфраструктуру суб’єктів, що пов’язані з державою- агресором; побудова дієвої та ефективної системи стратегічних комуніка- цій; розвиток механізмів взаємодії держави та інститутів громадянського суспільства щодо протидії інформаційній агресії проти України; боротьба з дезінформацією та деструктивною пропагандою з боку Російської Феде- рації; посилення спроможностей сектору безпеки і оборони щодо протидії спеціальним інформаційним операціям, спрямованим на зміну конститу- ційного ладу насильницьким шляхом, порушення суверенітету і територіа- льної цілісності, підрив обороноздатності України, деморалізацію особо- вого складу Збройних Сил України та інших військових формувань, загос- трення суспільно-політичної ситуації; виявлення та притягнення до відпо- відальності згідно із законодавством суб’єктів українського інформацій- ного простору, що створені та використовуються державою-агресором для ведення інформаційної війни проти України, та унеможливлення їхньої пі- дривної діяльності; унеможливлення вільного обігу інформаційної проду- кції (друкованої та електронної), насамперед походженням з території дер- жави-агресора, що містить пропаганду війни, національної і релігійної во- рожнечі, зміни конституційного ладу насильницьким шляхом або пору- шення суверенітету і територіальної цілісності України, провокує масові заворушення; проведення розвідувальними органами України акцій

сприяння реалізації та захисту національних інтересів України в інформа- ційній сфері, протидії зовнішнім загрозам інформаційній безпеці держави за межами України; недопущення використання інформаційного простору держави в деструктивних цілях або для дій, що спрямовані на дискредита- цію України на міжнародному рівні;

1. щодо забезпечення захисту і розвитку інформаційного простору України, а також конституційного права громадян на інформацію: стиму- лювання розвитку національного виробництва текстового і аудіовізуаль- ного контенту, зокрема шляхом створення системи квотування та прове- дення цільових конкурсів на надання грантів; забезпечення функціону- вання Суспільного телебачення і радіомовлення України, у тому числі його належного фінансування; створення системи мовлення територіальних громад, яка сприятиме розширенню комунікативних можливостей та зни- женню конфліктності всередині громад; підтримка вітчизняної книговида- вничої справи, зокрема перекладів іноземних творів, забезпечення ними навчальних закладів і бібліотек; розвиток правових інструментів захисту прав людини і громадянина на вільний доступ до інформації, її поширення, оброблення, зберігання та захист; комплексна підтримка розвитку механі- змів саморегуляції засобів масової інформації на засадах соціальної відпо- відальності; підвищення медіа-грамотності суспільства, сприяння підгото- вці професійних кадрів для медіа-сфери з високим рівнем компетентності; удосконалення законодавчого регулювання інформаційної сфери відпо- відно до актуальних загроз національній безпеці; задоволення потреб на- селення тимчасово окупованих територій в об’єктивній, оперативній і до- стовірній інформації; повне покриття території України цифровим та інте- рнет-мовленням замість аналогового і надання рівних можливостей дос- тупу кожному громадянину до інформаційних ресурсів мережі Інтернет; формування системи державної підтримки виробництва вітчизняного ау- діовізуального продукту; пропагування, у тому числі через аудіовізуальні засоби, зокрема соціальну рекламу, основних етапів і досвіду державотво- рення, цінностей свободи, демократії, патріотизму, національної єдності, захисту України від зовнішніх і внутрішніх загроз;
2. щодо відкритості та прозорості держави перед громадянами: роз-

виток механізмів електронного урядування; сприяння розвитку можливо- стей доступу та використання публічної інформації у формі відкритих да- них; інформування громадян України про діяльність органів державної влади, налагодження ефективної співпраці зазначених органів із засобами масової інформації та журналістами; проведення реформи урядових кому- нікацій; розвиток сервісів, спрямованих на більш масштабне та ефективне залучення громадськості до прийняття рішень органами державної влади та органами місцевого самоврядування; сприяння формуванню культури суспільної дискусії;

1. щодо формування позитивного міжнародного іміджу України: ґру- нтовне реформування системи представлення інформації про Україну на міжнародній арені; розвиток публічної дипломатії, у тому числі культурної та цифрової; активізація скоординованої інформаційної роботи закордон- них дипломатичних установ України; сприяння поширенню та розвитку системи іномовлення України; створення та забезпечення функціонування правового механізму взаємодії державних органів з інститутами громадян- ського суспільства з метою інформаційної підтримки комерційної, гумані- тарної, просвітницької, культурної та іншої діяльності таких інститутів за межами України; постійний моніторинг пропаганди держави-агресора, ро- зроблення та оперативна реалізація адекватних заходів протидії; недопу- щення використання міжнародного інформаційного простору в деструкти- вних цілях або для дій, що спрямовані на дискредитацію України на міжна- родному рівні; реформування системи взаємовідносин з українською діас- порою шляхом забезпечення більш тісної співпраці та проведення ефекти- вних заходів, зокрема в рамках комунікацій «від людини до людини»; уч- асть у міжнародних культурних заходах з метою представлення національ- ної культури та ідентичності; запровадження міжнародних культурних фе- стивалів в Україні з метою популяризації української культури та розвитку комунікацій «від людини до людини».

Для формування збалансованої державної політики та ефективного

проведення комплексу узгоджених заходів щодо захисту національних ін- тересів в інформаційній сфері створення розвиненого й захищеного інфор- маційного середовища слугує організація функціонування системи інфор- маційної безпеки, складовими компонентами якої є національні інтереси в інформаційній сфері, загрози та небезпеки цим інтересам, сама інформа- ційна безпека як інструмент зі створення сприятливих умов для їх реаліза- ції, які в сукупності становлять об’єкт управління органами державного уп- равління, систему забезпечення інформаційної безпеки, тобто суб’єкт уп- равління, більше того, основні напрямки політики національної безпеки в інформаційній сфері, а також внутрішнє та зовнішнє середовище.

Інформаційна безпека забезпечується комплексом заходів системи за- безпечення національної безпеки України, що включає сукупність держав- них органів, громадських організацій, посадових осіб та окремих громадян.

# Питання для самоконтролю

1. Що розуміється під «інформаційною безпекою України»?
2. Яке місце в системі національної безпеки України займає інформаційна безпека?
3. Розкрийте основні напрями політики інформаційної безпеки України?
4. Які найважливіші завдання у сфері інформаційної безпеки постають пе- ред державою?
5. В яких сферах проявляються реальні та потенційні загрози безпеці Укра- їни?
6. Охарактеризуйте загрози інформаційній безпеці України у воєнній сфері.
7. Охарактеризуйте загрози інформаційній безпеці України в економічній сфері.
8. Охарактеризуйте загрози інформаційній безпеці України в екологічній сфері.
9. Які завдання реалізації інформаційної політики з питань євроінтеграції?
10. Які основні підходи до визначення дестабілізуючих факторів ви знаєте?

# РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Конституція України // Відомості ВРУ, 1996, №30, ст..141, [Електронний ресурс]. Режим доступу: [https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-](https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text)

[%D0%B2%D1%80#Text](https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text)

1. Конвенція Ради Європи про кіберзлочинність, ратифікована Законом Ук- раїни від 7.09.2005 року № 2824-ІV. [Електронний ресурс]. Режим доступу: <https://zakon.rada.gov.ua/laws/show/994_575#Text>
2. Про інформацію: Закон України // Відомості Верховної Ради України (ВВР), 1992, № 48, ст.650. [Електронний ресурс]. Режим доступу: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>
3. Про національну безпеку України: Закон України// Відомості Верховної Ради (ВВР), 2018, № 31, ст.241. [Електронний ресурс]. Режим доступу: <https://zakon.rada.gov.ua/laws/show/2469-19#Text>
4. Про захист інформації в інформаційно-телекомунікаційних системах: За- кон України// Відомості Верховної Ради України (ВВР), 1994, № 31, ст.286. [Електронний ресурс]. Режим доступу: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>
5. Про доступ до публічної інформації: Закон України // Відомості Верхов- ної Ради України (ВВР), 2011, № 32, ст. 314. [Електронний ресурс]. Режим доступу: <https://zakon.rada.gov.ua/laws/show/2939-17#Text>
6. Про Державну службу спеціального зв’язку та захисту інформації Укра- їни: Закон України// Відомості Верховної Ради України (ВВР), 2006, № 30, ст.258. [Електронний ресурс]. Режим доступу: <https://zakon.rada.gov.ua/laws/show/3475-15#Text>
7. Резолюция 60/45, принятая Генеральной Ассамблеей ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». [Електронний ресурс]. Режим доступу: <https://zakon.rada.gov.ua/laws/show/995_e45#Text>
8. Директива 97/66/ЄС Європейського Парламенту і Ради «Стосовно обро- бки персональних даних і захисту права на невтручання в особисте життя в телекомунікаційному секторі». [Електронний ресурс]. Режим доступу: <https://zakon.rada.gov.ua/laws/show/994_243#Text>
9. Решение № 1106 «Первоначальный перечень мер укрепления доверия в рамках ОБСЕ с целью сокращения рисков возникновения конфликтов в ре- зультате использования информационных и коммуникационных техноло- гий» от 03.12.2013. [Електронний ресурс]. Режим доступу: <https://www.osce.org/files/f/documents/0/a/109648.pdf>
10. Конвенція про заборону або обмеження застосування конкретних видів звичайної зброї, які можуть вважатися такими, що завдають надмірних ушкоджень або мають невибіркову дію. [Електронний ресурс]. Режим до- ступу: <https://zakon.rada.gov.ua/laws/show/995_266#Text>
11. Верголяс О.О. Міжнародно-правове регулювання інформаційного про- тиборства: реалії та перспективи. Visegrad Journalon Human Rights. 2019.

№3. C. 58-63

1. Дудикевич В. Б., Опірський І. Р., Гаранюк П. І., Зачепило В. С., Партика А. І. Забезпечення інформаційної безпеки держави: навч. посіб. Львів: Ви- давництво Львівської політехніки, 2017. 204 с.
2. Ємельянов В. М. Кібербезпека як складова національної безпеки та кі- берзахист критичної інфраструктури України / В. М. Ємельянов, Г. Л. Бон- дар // Публічне управління та регіональний розвиток. – 2019. – № 5. – С. 493-523.
3. Інформаційна безпека держави: підручник: в 2 т. Т. 1. / В.М. Петрик та ін.; за заг. ред. В.В. Остроухова. Київ: ДНУ «Книжкова палата України», 2016. 264 с.
4. Інформаційна безпека / За ред. Ю. Я. Бобала та І. В. Горбатого. Львів: Вид-во Львівської політехніки. 2019. 580 с.
5. Історія інформаційно-психологічного протиборства: підруч./ [Я.М.Жа- рков, Л.Ф.Компанцева, В.В.Остроухов В.М.Петрик, М.М.Присяжнюк, Є.Д.Скулиш]; за заг. ред. д.ю.н., проф., засл. юриста України Є.Д.Скулиша. Київ: Наук.-вид. відділ НА СБ України, 2012. 212 с.
6. Кіберзлочини в Україні (кримінально-правова характеристика) [Текст]

: навч. посіб. / А. В. Боровик, І. М. Копотун. - Луцьк : Волинь Поліграф, 2019. - 304 с.

1. Корпоративна безпека: практичний посібник. Консалтингова компанія Сідкон. 2018. 276 с.
2. Когут Ю.І. Кібербезпека та ризики цифрової трансформації компаній. Вид-во SIDCON. 2021. 372 с.
3. Лісовська Ю. П. Інформаційна безпека України: навч. посіб. Київ: Кон- дор, 2018. 172 с.

21. Лизанчук В. Інформаційна безпека України: теорія і практика. Львів. Вид-во ЛНУ ім. Івана Франка. 2017. 728 с.

1. Мехед Д., Ткач Ю., Базилевич В., Гур’єв В., Усов Я. Аналіз вразливос- тей корпоративних інформаційних систем. Захист інформації. 2018. № 1. С. 61 – 66.
2. Могильний С.Б. Інформаційна безпека при роботі в Інтернеті: навч.-ме- тод. посібник / за ред. О. В. Лісового та ін. – К., 2018. – 105 с.
3. Нашинець-Наумова А.Ю. Інформаційна безпека суб’єктів господарю- вання: проблеми теорії та практики правозастосування: Монографія. Видав. Дім «Гельветика». 2017. 386 с.
4. Петрик В., Присяжнюк М. Інформаційна безпека держави. Підручник у 2-х томах. Київ. Вид-во «Книжкова палата України». 2016. 264 с.
5. Почепцов Г. Сучасні інформаційні війни / Г. Почепцов. – К. : Вид.дім

«Києво-Могилянська академія», 2015. – 497 с.

1. Почепцов, Г. Виртуальные войны. Фейки [Текст] / Георгий Почепцов. Харьков : Фолио, 2019. 506 с.
2. Почепцов Г. Сучасні інформаційні війни / Г. Почепцов. – К. : Вид.дім

«Києво-Могилянська академія», 2015. – 497 с.

1. Харитонов Є.О., Давидова І.В. Інформаційна безпека: проблеми прива- тного права. Навч.- методичний посібник. Вид-во Фенікс, 2020. 194 с.

# ІНФОРМАЦІЙНІ РЕСУРСИ В ІНТЕРНЕТІ

* 1. Верховна Рада України: офіційний веб-портал парламенту України. Законодавство України. – Режим доступу: <https://zakon.rada.gov.ua/laws>
  2. Кабінет міністрів України. Урядовий портал. Єдиний веб-портал ор- ганів виконавчої влади України. – Режим доступу : <https://www.kmu.gov.ua/>
  3. Офіційний вісник України. – Режим доступу : [www.gdo.kiev.ua](http://www.gdo.kiev.ua/).
  4. Статистика України: науковий журнал [Електронний ресурс]. – Режим доступу : [www.ukrstat.gov.ua](http://www.ukrstat.gov.ua/).

# ЗМІСТ

[Вступ 3](#_TOC_250010)

Зміст та структура навчальної дисципліни 5

[Розділ 1. Поняття інформаційної безпеки держави, суспільства та особи 7](#_TOC_250009)

[Розділ 2. Інформаційна безпека та кібербезпека 17](#_TOC_250008)

[Розділ 3. Загрози для інформаційної безпеки держави, суспільства, людини 23](#_TOC_250007)

Розділ 4. Принципи, форми та методи забезпечення інформаційної

безпеки держави 33

Розділ 5. Інформаційне протиборство між країнами.

Інформаційна війна 42

[Розділ 6. Інформаційна зброя в інформаційній війні 50](#_TOC_250006)

[Розділ 7. Основи теорії інформаційної боротьби 56](#_TOC_250005)

[Розділ 8. Основи безпеки інформаційних ресурсів 65](#_TOC_250004)

[Розділ 9. Забезпечення безпеки інформації та інформаційних ресурсів 78](#_TOC_250003)

[Розділ 10. Захист інформаційних систем 91](#_TOC_250002)

[Розділ 11. Інформаційна безпека України 98](#_TOC_250001)

[Рекомендована література 108](#_TOC_250000)

*Навчальне видання*

ПЕРЕВАЛОВА Людмила Вікторівна ЛИСЕНКО Ірина В’ячеславівна

ЛИСЕНКО Андрій Миколайович ГАРЯЄВА Ганна Михайлівна

**НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У НАЦІОНАЛЬНОМУ ТА МІЖНАРОДНОМУ СПІВРОБІТНИЦТВІ**

Навчально-методичний посібник для студентів напряму підготовки

«Філологія (прикладна та комп’ютерна лінгвістика)»

Відповідальний за випуск *Лисенко І. В.*

Роботу до видання рекомендував *Кіпенський А. В.*

В авторській редакції

План 2023 р., поз.109

Підп. до друку 9.11.2023. Формат 60×84 1/16. Папір офісний.

Друк цифровий. Гарнітура Times New Roman. Ум. друк. арк. 6,51.

Наклад 150 прим. Зам. № 2/11/23. Ціна договірна.

Видавець та виготовлювач ФОП Панов А.М. Свідоцтво про внесення до Державного реєстру видавців,

виробників і розповсюджувачів видавничої продукції серія ДК № 4847 від 06.02.2015 р.

м. Харків, вул. Жон Мироносиць, 10 оф. 6 тел. +38(057)714-06-74, +38(050)976-32-87

[copy@vlavke.com](mailto:copy@vlavke.com)