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 національному 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 навчального курсу «Нормативно-правове забезпечення інформаційної безпеки у національному та міжнародному співробітництві». В ньому розглядаються основні законодавчі акти, міжнародні правові документи, які регулюють діяльність органів державної влади у сфері забезпечення інформаційної безпеки. Особлива 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, надають характеристику стратегії забезпечення інформаційної безпеки, основним реальним та потенційним загрозам інформаційної безпеки нашої держави

Посібник буде корисним як для студентів, які навчаються за спеціальністю «Філологія (прикладна та комп'ютерна лінгвістика)», так і для викладачів.

Бібліогр. 30 назв.

УДК 004.056+340

ISBN 978-617-8113-60-5

ВСТУП

На сучасному етапі розвитку людської цивілізації для кожної країни світу інформація стає стратегічно важливим ресурсом, від ефективного використання 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 діяльності.

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

Забезпечення інформаційної безпеки сприяє забезпеченню досягнення 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 інформаційної 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, загальні поняття безпеки інформаційних ресурсів, особливості та основні форми інформаційного протиборства, надається класифікація загроз для інформаційної безпеки держави, суспільства та особи. Розглянуті способи побудови інформаційно-комунікаційних систем і мереж на основі сучасних способів передачі й обробки інформації та способи захисту інформації в інформаційних системах і мережах. Аналізується політика та система забезпечення інформаційної безпеки України. Особлива увага приділяється характеристики нормативно-правових актів України та міжнародно-правових документів, які сприяють забезпеченню інформаційної безпеки України.

Таким чином, метою вивчення дисципліни «Нормативно-правове забезпечення інформаційної безпеки у національному та міжнародному співробітництві» є:

• сприяти засвоєнню правових знань, формування вмінь і навичок застосовувати здобуті знання у професійної діяльності;

• формування у майбутніх фахівців розуміння сутності явища інформаційна безпека;

• ознайомити їх з основними загрозами інформаційній безпеці та виробити уявлення про ефективність інструментів забезпечення інформаційної 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 інформаційної безпеки;

• чинне законодавство України в сфері інформаційної безпеки.

Уміти:

• орієнтуватись у системі джерел законодавства України та міжнародно-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 виступів, знаходити правову інформацію;

• керуватись у практичній діяльності та поведінці правовими знаннями і переконаннями.

Структура навчальної дисципліни «Нормативно-правове забезпечення інформаційної безпеки у національному та міжнародному співробітництві» визначається відповідно до робочого навчального плану.

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

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. Інформаційні 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 інформаційної та кібербезпеки. Стратегії забезпечення національної безпеки держави. Закон України «Про національну безпеку». Кіберпростір та його співвідношення з інформаційною безпекою. Кібербезпека склад та сутність. Стратегія забезпечення національної безпеки. Фундаментальні національні інтереси України.

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

Інформаційна безпека держави та життєво важливі інтереси особистості, 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 інформаційній безпеці. Класифікація видів загроз інформаційній безпеці України. Внутрішні та зовнішні джерела загроз інформаційній безпеці. України. Принципи забезпечення інформаційної безпеки. Система забезпечення інформаційної безпеки держави. Основні форми і способи забезпечення інформаційної 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, інформаційне протиборство. Методи забезпечення інформаційної безпеки.

Тема 5. Інформаційне протиборство між країнами. Інформаційна війна

Інформаційне протиборство та його види. Об'єкти впливу інформаційного протиборства. Концепція інформаційного протиборства. Ступені інформаційного протиборства. Основні форми інформаційного протиборства. Інформаційна війна та її завдання. Особливості інформаційної війни. Концепція інформаційної війни. Органи інформаційної війни. Основні форми та рівні інформаційної війни. Засоби інформаційної війни. Інформаційні переваги у сфері інформаційного протиборства.

Тема 6. Інформаційна зброя в інформаційні війні

Інформаційна зброя та сфера її застосування. Основні об'єкти застосування інформаційної зброї. Види інформаційної зброї. Інформаційна зброя воєнного та невоєнного застосування. Особливості застосування інформаційної 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 інформаційної боротьби. Загальні основи теорії інформаційної боротьби та її структура. Теорія сил та засобів ураження інформації. Теорія захисту інформації. Фактори впливу: економічний, воєнний та інформаційний. Закони та закономірності інформаційної боротьби. Принципи інформаційної боротьби. Заходи інформаційної боротьби: інформаційне забезпечення, інформаційний захист, інформаційна протидія. Способи та форми інформаційної 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 законодавство, загальні та спеціальні закони, підзаконні акти. Спеціальне законодавство та його значення для забезпечення інформаційної безпеки. Страхове забезпечення та його мета. Ліцензія як засіб забезпечення безпеки інформації. Комерційна таємниця. Забезпечення захисту та безпеки інформації на підприємстві. Особливості захисту комп'ютерних систем. Служба

захисту інформації. Організаційний захист та його заходи. Інженерно-технічний захист та його засоби.

Тема 10. Захист інформаційних систем

Джерела інформації. Люди як джерела інформації. Конфіденційна інформація: 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. Корпоративні інформаційні системи (КІС).

Тема 11. Інформаційна безпека України

Національна безпека та її структура. Принципи забезпечення національної безпеки. Інформаційна безпека та її місце в національній безпеки України. Сутність інформаційної безпеки. Мета та завдання забезпечення інформаційної безпеки України. Основні реальні та потенційні загрози інформаційній 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

1.1. Інформаційна безпека (поняття і визначення).
1.2. Інформаційна безпека, її сутність.
1.3. Інтереси особи, суспільства та держави в інформаційній сфері.

1.1. 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 інформаційною безпекою. Процеси глобалізації дуже гостро дали про себе знати й, крім позитивних елементів, виникли серйозні негативні явища, до яких світова спільнота виявилася неготовою. Тому інформаційна безпека у сучасному 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 маніпуляції суспільством, думкою громадян, створенню конфліктів. Отже, як людина потребує захисту від інформації, так і інформація потребує захисту від людини. Особливо зростає роль інформаційної безпеки у сфері високих технологій, бо саме цифрова інформація стає одночасно і сировиною, і продуктом, 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, багатозначністю, можливістю «інформаційних диверсій», анонімністю доступу. Захист інформації, що розміщена в середовищі комп'ютера – це набагато складніше, ніж збереження таємниці звичайного поштового листування. Враховуючи це, можна зробити висновок, що проблеми інформаційної безпеки надзвичайно актуальні й потребують поглибленого вивчення.

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

Базові засади інформаційної безпеки нашої держави закладено у статтях 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 юридичного визначення у законодавстві. В Законі України «Про Концепцію Національної програми інформатизації» від 4 лютого 1998 р. офіційно визнано інформаційну безпеку як невід'ємну частину політичної, економічної, оборонної 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 безпека як стан захищеності життєво важливих інтересів людини, суспільства і держави. Також інформаційна безпека розкривається у Доктрині інформаційної безпеки України від 25 лютого 2017 р. [12] як невід'ємна складова кожної зі сфер національної безпеки і як важлива самостійна сфера забезпечення національної безпеки. Саме ж поняття інформаційної безпеки застосовується 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 розкриваються 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 середовищі;

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. проблемної сфери, якими обмінюються користувачі системи оброблення даних.

Основним Законом, регулюючим питання інформації в Україні є Закон «Про інформацію», який регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації.

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 інформації, закріплює право особи на інформацію в усіх сферах суспільного і державного життя України, а також систему інформації, її джерела, визначає статус учасників інформаційних відносин, регулює доступ до інформації 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, свобод і законних інтересів.

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

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 інформації.

2. Ніхто не може обмежувати права особи у виборі форм і джерел одержання інформації, за винятком випадків, передбачених законом.

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

3. Забороняється вилучення і знищення друкованих видань, експонатів, інформаційних банків, документів з архівних, бібліотечних, музейних фондів, крім встановлених законом випадків або на підставі рішення суду.

4. Право на інформацію, створену в процесі діяльності фізичної чи юридичної особи, суб'єкта владних повноважень або за рахунок фізичної чи юридичної особи, Державного бюджету України, місцевого бюджету, охороняється в порядку, визначеному законом.

Розділ ІІ Закону присвячено **інформаційній діяльності**, під якою розуміється сукупність дій, спрямованих на задоволення інформаційних потреб громадян, юридичних осіб і держави.

Визначено основні напрями та види інформаційної діяльності – одержання, використання, поширення та зберігання інформації.

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

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

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

За режимом доступу інформація поділяється на **відкриту інформацію та інформацію з обмеженим доступом**. Держава здійснює контроль за режимом доступу до інформації. Державний контроль за додержанням встановленого 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 (бюлетенях, збірниках);

поширення її засобами масової комунікації;

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

Обмеження права на одержання відкритої інформації забороняється законом.

Інформація з обмеженим доступом за своїм правовим режимом поділяється на ***конфіденційну і таємну***.

Конфіденційна інформація – це відомості, які знаходяться у володінні, 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, ділового, виробничого, банківського, комерційного та іншого характеру, одержаною на власні кошти, або такою, яка є предметом їх професійного, ділового, виробничого, банківського, комерційного та іншого інтересу і не порушує передбаченої законом таємниці, самостійно визначають режим доступу до неї, включаючи належність її до категорії конфіденційної, та встановлюють для неї систему (способи) захисту. Виняток становить інформація 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 інформації, 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 військових формувань, їхніх окремих підрозділів, якщо ці відомості не належать до державної таємниці згідно з законодавством України.

Інформація, що становить комерційну таємницю – це відомості науково-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 відношенні якої власником такої інформації введений режим комерційної таємниці.

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

Інформація з обмеженим доступом 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 охоплює 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, встановленому законом, державною таємницею та підлягає охороні з боку держави. Віднесення інформації до категорії відомостей, що становлять державну таємницю, порядок її захисту та обігу, доступ до неї визначається Законом України «Про державну таємницю», яким закладено правову основу створення 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, споживачі, поширювачі, зберігачі (охоронці) інформації. Кожний учасник

інформаційних відносин для забезпечення його прав, свобод і законних інтересів має право на одержання інформації про: діяльність органів державної влади; діяльність народних депутатів; діяльність органів місцевого і регіонального самоврядування та місцевої адміністрації; те, що стосується його особисто.

Розділ V Закону присвячений охороні інформації, відповідальності за порушення законодавства про інформацію. Держава гарантує всім учасникам інформаційних відносин рівні права і можливості доступу до інформації. Стаття 45-[1] забороняє цензуру та втручання в професійну діяльність журналістів 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, порушення територіальної цілісності України, пропаганди війни, насильства, жорстокості, розпалювання расової, національної, релігійної ворожнечі, посягання на права і свободи людини. Не підлягають розголошенню відомості, що стосуються лікарської таємниці, грошових вкладів, прибутків від підприємницької діяльності, усиновлення (удочеріння), листування, телефонних розмов і телеграфних повідомлень, крім випадків, передбачених законом. Порушення законодавства України про інформацію тягне за собою дисциплінарну, цивільно-правову, адміністративну або кримінальну відповідальність згідно з законодавством України.

Розділ VI Закону присвячено міжнародній інформаційній діяльності, співробітництві з іншими державами, зарубіжними і міжнародними організаціями в галузі інформації. Міжнародне співробітництво в галузі інформації з питань, що становлять взаємний інтерес, здійснюється на основі міжнародних договорів, укладених Україною та юридичними особами, які займаються інформаційною діяльністю.

Відносини, які виникають у всіх сферах життя й діяльності держави, суспільства і людини при одержанні, використанні, поширенні та зберіганні 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 інформаційної безпеки можуть бути: інформаційні системи різного масштабу й різного 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 національної безпеки держави.

Важливим поняттям для усвідомлення інформаційної безпеки є визначення інформаційного простору.

Інформаційний простір (національний):

1) інформаційне середовище, в якому здійснюються інформаційні процеси та інформаційні відносини щодо створення, збирання, відображення, реєстрації, накопичення, збереження, захисту та поширення інформації, інформаційних продуктів і ресурсів, на яке поширюється юрисдикція держави;

2) сукупність національних інформаційних ресурсів та інформаційної інфраструктури, які дозволяють на основі єдиних принципів і загальних правил забезпечувати інформаційну взаємодію громадян, суспільства і держави з їх рівним правом доступу до відкритих інформаційних ресурсів та максимально повним задоволенням інформаційних потреб суб'єктів держави на всій її території з додержанням балансу інтересів на входження у світовий інформаційний простір і забезпечення інформаційної безпеки відповідно до Конституції України та міжнародних правових норм.

1.2. Інформаційна безпека, її сутність

Інформаційна безпека – захищеність (стан захищеності) основних інтересів особи, суспільства і держави у сфері інформації, включаючи інформаційну й телекомунікаційну інфраструктуру і власне інформацію та її параметри, такі як повнота, об'єктивність, доступність і конфіденційність. Інформаційна безпека є складовою національної безпеки. Але особливістю інформаційної безпеки є те, що вона, як невід'ємна частина, входить до інших складових національної безпеки: економічної, воєнної, політичної безпеки тощо.

Поняття інформаційної безпеки держави, суспільства та особи, залежно від його використання, розглядається в декількох ракурсах. У найзагальнішому випадку інформаційна безпека – це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави.

Більш розгорнуте формулювання інформаційної безпеки – це стан захищеності потреб в інформації особи, суспільства й держави, за якого забезпечується їхнє існування та прогресивний розвиток незалежно від наявності 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 інформованості 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 стійкій єдності всіх різноманітних і суперечливих формах буття.

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

Критерієм ефективності забезпечення інформаційної безпеки є високий 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 наднаціональних 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. Сукупність внутрішніх і зовнішніх інформаційних загроз створюють передумови для порушення безпечного функціонування системи державного управління.

Вагомість інформаційно-комунікаційних процесів у сучасному світі дає підстави розглядати забезпечення інформаційної безпеки як одне з глобальних 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 розгляду 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 виокремити декілька підходів окреслення сутності цього феномену, а саме розуміння інформаційної безпеки як:

1. Стану захищеності інформаційного простору.

2. Процесу управління загрозами та небезпеками, що забезпечує інформаційний суверенітет держави.

3. Стану захищеності національних інтересів держави в інформаційному 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 потенційних 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 здоров'я людини від деструктивного інформаційного впливу, який призводить до неадекватного сприйняття нею дійсності та (або) погіршення її фізичного стану.

Інформаційна безпека суспільства – можливість безперешкодної реалізації суспільством та окремими його членами своїх конституційних прав, пов'язаних із можливістю вільного одержання, створення й поширення інформації, а також ступінь їхнього захисту від деструктивного інформаційного впливу. Необхідний рівень інформаційної безпеки забезпечується сукупністю політичних, економічних, організаційних заходів, спрямованих на попередження, виявлення й нейтралізацію тих обставин, факторів і дій, які можуть завдати збитків чи зашкодити реалізації інформаційних прав, потреб та інтересів країни 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 держави – це стан її захищеності, при якій спеціальні інформаційні операції, акти зовнішньої інформаційної агресії, інформаційний тероризм, незаконне зняття інформації за допомогою спеціальних технічних засобів, комп'ютерні злочини та інший деструктивний інформаційний вплив не завдає суттєвої шкоди національним інтересам.

1.3. 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 частини:*

- 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 технологій і

– засобів їхнього забезпечення; створення й застосування засобів і механізмів інформаційної безпеки.

В чому ж знаходять свій прояв інтереси учасників інформаційних відносин?

Інтереси особи в інформаційній сфері полягають:

- у реалізації конституційних прав людини та громадянина на доступ до інформації, на використання інформації в інтересах здійснення не забороненої законом діяльності, фізичного, духовного та інтелектуального розвитку;

- 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 інфраструктури;

– 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 цілісності держави, політичної, економічної та соціальної стабільності, у безумовному забезпеченні законності та правопорядку, розвитку рівноправного та взаємовигідного міжнародного співробітництва.

Питання для самоконтролю

1. Які основні підходи до визначення поняття «інформаційна безпека» Ви знаєте?

2. Визначить основні ознаки інформаційної безпеки.

3. У чому полягають інтереси особи, суспільства та держави в інформаційній сфері?

4. Надайте характеристику об’єктам та суб’єктам інформаційної безпеки.

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

2.1. Кіберпростір: поняття та склад.
2.2. Проблеми забезпечення інформаційної та кібербезпеки.
2.3.Стратегії забезпечення національної безпеки держави. Закон України «Про національну безпеку».

2.1.Кіберпростір: поняття та склад

Поступове й доволі умовне поєднання віртуального і реального просторів за допомогою ІТ-систем і мережних технологій різного функціонального призначення, які в процесах обробки, передавання та зберігання інформації використовують електромагнітний спектр і діють як єдине ціле, а також відповідного програмного забезпечення призвело, зрештою, до формування 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– призначеного для зберігання, обробки й передавання інформації;
- перебувають у постійному русі по сукупності ІТ- систем і мереж.

Уперше термін «кіберпростір» було використано в *Конвенції про злочинність у сфері комп'ютерної інформації від 23 листопада 2001 року*. Сфера його дії на той час перебувала під впливом загальних механізмів правового 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 правовідносинах.

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 мережами, програмним забезпеченням та інформаційними ресурсами, використовуване 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 користувачам доступ до обчислювальних та інформаційних ресурсів систем, вироблення електронних інформаційних продуктів, а також обмін електронними повідомленнями, даючи змогу із застосуванням електронних інформаційних образів у режимі реального часу вступати у відносини (взаємодіяти) щодо спільного використання обчислювальних та інформаційних ресурсів системи (надання інформаційних послуг, ведення електронної комерції тощо);

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

об'єкти інформаційної інфраструктури, що керуються інформаційними (автоматизованими) системами управління та інформації, що в них циркулює;

середовище, утворене організованою сукупністю інформаційних процесів на основі взаємопоєднаних за єдиними принципами та правилами інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем.

Найбільш відмітними ознаками кіберпростору як субстанції, створенню якої сприяли передусім такі чинники: зміна характеру діяльності людини з ухвалення рішень; упровадження електронно-цифрових форм створення, обробки, зберігання та переміщення інформації, перехід від паперового діловодства до електронного тощо; абсолютна більшість фахівців вважає 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 проникнення в ІТС один одного, блокування або виведення з ладу найбільш уразливих елементів цих систем, дезорганізації оборонних автоматизованих систем управління протилежної сторони, систем управління її транспортом і енергетикою, економікою й фінансовою системою тощо (поряд із наземною, 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 особливостями– існування та передавання інформації;

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

2.2. Проблеми забезпечення інформаційної та кібербезпеки

Сучасний стан справ зумовлює небачені досі глибинні зміни у ставленні більшості держав світу до безпеки власного інформаційного та кіберпростору, 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 безпека** – це інформаційні потоки; бази даних; персонал.

При цьому інформаційну безпеку в найзагальнішому розумінні можна визначити як такий стан захищеності інформаційного простору держави, 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 інтересах оборони.

Спектр інтересів ІБ щодо інформації, інформаційних систем та інформаційних технологій як об'єктів безпеки можна поділити на такі основні категорії: доступність – можливість за прийнятний час отримати певну інформаційну послугу; цілісність – актуальність і несуперечливість інформації, її захищеність від руйнування та несанкціонованого змінювання; конфіденційність – захищеність від несанкціонованого ознайомлення.

Кібербезпеку можна визначити як стан захищеності кіберпростору держави загалом або окремих об'єктів її інфраструктури від ризику стороннього 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 інформаційно-телекомуніційних систем протиборчих сторін, захист власної інформаційної системи.

Головні проблеми забезпечення кібернетичної безпеки постають із таких причин: відсутності чіткого усвідомлення ролі та значення кібербезпекової 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 забезпечення та кадрового наповнення – відповідних структурних підрозділів.

Комплексну сутність кібербезпеки за таких умов складають:

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

2.3. 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 інформаційної й кібербезпеки, а також у боротьбі з кіберзлочинністю. Нормативно-правову базу в цих сферах діяльності становлять такі документи:

- Конвенція Ради Європи про кіберзлочинність, ратифікована Законом України від 7.09.2005 року № 2824-IV;
- Закони України: «Про інформацію», «Про національну безпеку України», «Про Державну службу спеціального зв'язку та захисту інформації України», «Про телекомунікації», «Про захист інформації в інформаційно-телекомунікаційних 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 національної безпеки та оборони України.

В Законі України «Про національну безпеку України» надається визначення 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 планування й реалізації державної політики у сфері національної безпеки;

2. Стратегія воєнної безпеки України – документ, у якому викладається система поглядів на причини виникнення, сутність і характер

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

3. Стратегія кібербезпеки України – документ довгострокового планування, що визначає загрози кібербезпеці України, пріоритети та напрями забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави;

4. Стратегія громадської безпеки та цивільного захисту України – документ довгострокового планування, що розробляється на основі Стратегії національної безпеки України за результатами огляду громадської безпеки та цивільного захисту і визначає напрями державної політики щодо гарантування 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 державної 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 України та забезпечення національної безпеки, цілі та основні напрями державної політики у сфері національної безпеки; поточні та прогнозовані загрози національній безпеці та національним інтересам України з урахуванням зовнішньополітичних та внутрішніх умов; основні напрями зовнішньополітичної та внутрішньополітичної діяльності держави для забезпечення її національних інтересів і безпеки; напрями та завдання реформування й розвитку сектору безпеки і оборони; ресурси, необхідні для реалізації Стратегії.

Стратегія національної безпеки України ґрунтується на таких основних 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, зокрема 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 інтересів України та забезпечення національної безпеки – це відстоювання незалежності і державного суверенітету; відновлення територіальної цілісності у межах міжнародно визнаного державного кордону України; суспільний розвиток, насамперед розвиток людського капіталу; захист прав, свобод 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 цілісності та недоторканності; території, навколишнього природного середовища - від надзвичайних ситуацій.

Основними принципами, що визначають порядок формування державної 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 міжнародних 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 конституційний 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, безпековий, правовий простір, набуття членства в Європейському Союзі та в Організації Північноатлантичного договору, розвиток рівноправних взаємовигідних відносин з іншими державами.

Слід відзначити, що сектор безпеки і оборони підлягає демократичному цивільному контролю, який здійснюється Президентом України, Верховною Радою України, Радою національної безпеки і оборони, Кабінетом

Міністрів України, органами виконавчої влади та органами місцевого самоврядування, встановлюється також судовий контроль та громадський нагляд.

Державна політика у сферах національної безпеки і оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, 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 безпеку України»?
7. В чому полягає значення Стратегії національної безпеки України?
8. На яких засадах ґрунтується Стратегія національної безпеки України?
9. В чому полягає головна мета державної політики в сфері національної безпеки?
10. На яких принципах базується державна політики в сфері національної безпеки та оборони?

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

3.1.Поняття загроз інформаційній безпеці.
3.2. Види загроз інформаційній безпеці.
3.3. Фактори загроз інформаційній безпеці.
3.4. Джерела загроз інформаційній безпеці.
3.5. Етапи розвитку засобів інформаційних комунікацій.

3.1.Поняття загроз інформаційній безпеці

Загрози інформаційній безпеці – сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам особи, суспільства й держави 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, інформаційні ресурси, на системи їхнього формування і використання);

3) загрози інформаційним правам і свободам особи (праву на виробництво, поширення, пошук, одержання, передавання і використання інформації; 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 функцією забезпечення інформаційної безпеки. Багато в чому вигляд розроблюваної системи захисту і склад механізмів її реалізації визначається потенційними загрозами, виявленими на цьому етапі. Наприклад, якщо користувачі мають доступ в Інтернет, то кількість загроз інформаційній безпеці різко зростає, відповідно, це відбивається на методах і засобах захисту і т. д.

Загроза інформаційній безпеці – це потенційна можливість порушення режиму інформаційної безпеки. Навмисна реалізація загрози називається атакою на інформаційну систему. Особи, які навмисно реалізують загрози, є зловмисниками. Найчастіше загроза є наслідком наявності вразливих місць у захисті інформаційних систем, наприклад, неконтрольований доступ до персональних комп'ютерів або неліцензійне програмне забезпечення (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, постійно з'являються виправлення до програмного забезпечення фірми Microsoft, що усувають чергові його вразливі місця. Такий підхід до забезпечення безпеки малоефективний, оскільки завжди існує проміжок часу між моментом виявлення загрози та її усуненням. Саме в цей період зловмисник 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 потенційних загроз. Але деякі загрози не можна вважати наслідком цілеспрямованих дій шкідливого характеру. Існують загрози, викликані випадковими помилками або техногенними явищами.

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

3.2. Види загроз інформаційній безпеці

Відповідно виділяють такі види загроз.

За ступенем гіпотетичної шкоди:

загроза – явні чи потенційні дії, які ускладнюють або унеможливлюють реалізацію національних інтересів в інформаційній сфері та створюють небезпеку для системи державного управління, життєзабезпечення її системоутворюючих елементів;

небезпека – безпосередня дестабілізація функціонування системи державного 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 системі.

За ймовірністю реалізації:

імовірні – такі загрози, які за виконання певного комплексу умов обов'язково відбудуться. Прикладом може слугувати оголошення атаки інформаційних ресурсів суб'єкта забезпечення національної безпеки, яке передує 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 характер;

випадкові – такі загрози, які за виконання певного комплексу умов кожного разу протікають по-різному. Загрози цього рівня доцільно аналізувати за допомогою методів дослідження операцій, зокрема теорії ймовірностей 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 ґрунтів чи надр, природні пожежі, масове ураження сільськогосподарських рослин і тварин хворобами чи шкідниками, зміна стану водних ресурсів і біосфери 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 головних 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 людини (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 системи. 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 окремих органів державної влади або їхніх компонентів;

елементні – загрози, що впливають на окремі елементи структури системи. 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 обмежена 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 дестабілізації, 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 вважається 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 навмисними. Отже, на будь-якому об'єкті повинні здійснюватися деякі дії чи фактори, що будуть перешкоджати реалізації конкретних захисних механізмів і заходів, створюючи тим самим відзначені вище загрози. При цьому вони будуть безпосередньо пов'язані з цими загрозами і будуть, власне кажучи, 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 захисту;

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 здійснення цих факторів, тобто є їх результатом. Надалі ці фактори будемо називати 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, економічні та організаційно-технічні.

Під політичними факторами загроз інформаційній безпеці розуміють:

зміни геополітичної ситуації внаслідок фундаментальних змін у різноманітних регіонах світу, зведення до мінімуму ймовірності світової ядерної війни;

інформаційна експансія розвинених країн, які здійснюють глобальний моніторинг світових політичних, економічних, воєнних, екологічних та інших 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 максимальної 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 кількості вітчизняних та зарубіжних комерційних структур – виробників та споживачів інформації, засобів інформатизації та захисту інформації, включення 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 інформаційної інфраструктури.

Основними організаційно-технічними факторами загроз інформаційній безпеці є:

- недостатня нормативно-правова база у сфері інформаційних відносин, 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 передавання інформації;
- зростання обсягів інформації, яка передається відкритими каналами зв'язку;
- загострення криміногенної ситуації, зростання числа комп'ютерних 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 суспільстві, 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 діяльності, а також у захисті інформації, що забезпечує особисту безпеку, духовний та інтелектуальний розвиток.

Найбільш небезпечним джерелом загроз цим інтересам вважається суттєве розширення можливості маніпулювання свідомістю людини за рахунок формування навколо неї індивідуального «віртуального інформаційного простору», а також можливість використання технологій впливу на її психічну діяльність. Важливою особливістю способу життя людини в інформаційному суспільстві є суттєве скорочення «інформаційних» відстаней (часу доступу до необхідної інформації), що веде до появи нових можливостей як із формування особистості, так і з реалізації її потенціалу.

Людство впритул підходить до рубежів, за якими інформаційна інфраструктура 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 індустріального 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 безпеці, потреба в продовженні роду, довголітті, а також потребами у спілкуванні 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. Спрямованість використання одержаної інформації і результати, що одержуються, визначаються передусім особою людини та її духовним потенціалом. Складність процедур, що реалізуються в сучасних технологіях доступу до необхідних інформаційних ресурсів, критично збільшують залежність окремої людини від інших людей, які розробляють інформаційні технології, визначення 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, визначають умови, в яких він живе і діє, вирішує свої життєві проблеми. Саме тому вважається виключно важливим забезпечити безпеку взаємодії людини з інформаційною структурою.

Іншим небезпечним джерелом загроз інтересам особи є використання на шкоду її інтересам персональних даних, що нагромаджуються різноманітними структурами, у тому числі органами державної влади, а також розширення можливості прихованого збирання інформації, що становить його особисту й сімейну таємницю, відомості про її приватне життя. Це зумовлено насамперед труднощами реалізації механізмів охорони цих відомостей, подальшими досягненнями в мікромініатюризації засобів прихованого збирання і передавання інформації.

Інформаційна безпека людини (в широкому розумінні) передбачає:

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

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

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

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

Джерела загроз інформаційній безпеці суспільства.

Інтереси суспільства, що вступило у стадію постіндустріального розвитку, полягають у захисті життєво важливих інтересів у цій сфері, забезпечення реалізації конституційних прав і свобод людини та громадянина в інтересах зміцнення демократії, досягнення і підтримування суспільної злагоди, 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 можуть 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, трубопровідної і деяких інших інфраструктур.

Небезпечним джерелом загроз виступає можливість концентрації засобів масової інформації в руках невеликої групи власників. Ці загрози можуть проявлятися у вигляді маніпуляції суспільною думкою щодо тих чи інших суспільно значущих подій, а також руйнування моральних устоїв суспільства шляхом нав'язування чужорідних цінностей.

Нарешті, небезпечним джерелом загроз є розширення масштабів вітчизняної і міжнародної комп'ютерної злочинності. Ці загрози можуть проявлятися у вигляді спроб здійснення шахрайських операції з використанням глобальних або вітчизняних інформаційно-телекомунікаційних систем, відмивання 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 розвитку інформаційної інфраструктури держави, реалізації конституційних

прав і свобод людини і громадянина в інтересах зміцнення конституційного ладу, суверенітету і територіальної цілісності країни, встановлення політичної 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 інтересам держави в інформаційному суспільстві може стати неконтрольоване поширення інформаційної зброї та розгортання гонки озброєнь у цій галузі, спроби реалізації концепції ведення інформаційних війн.

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

створення атмосфери бездуховності та аморальності, негативного відношення до культурної спадщини противника;

маніпулювання суспільною свідомістю та політичною орієнтацією соціальних 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, загострення політичної боротьби, провокування репресій проти опозиції, провокація взаємного знищення;

зниження інформаційного забезпечення влади та управління, інспірація помилкових управлінських рішень;

дезінформація населення про роботу державних органів, підрив їхнього авторитету, дискредитація органів управління;

провокування соціальних, політичних, національних і релігійних сутичок;

ініціювання страйків, масових заворушень та інших акцій економічного– протесту;

ускладнення прийняття органами важливих рішень;

підрив міжнародного авторитету держави, її співробітництва з іншими 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 компаній невеликої кількості країн на ринку інформаційних продуктів, оскільки це здатне спровокувати бажання використати наявну перевагу для досягнення 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 етапів:

І етап – до 1816 року – характеризується використанням природно–виникаючих засобів інформаційних комунікацій. У цей період основне завдання інформаційної безпеки полягало в захисті відомостей про події, факти, майно, місцезнаходження й інші дані, що мають для людини особисто або співтовариства, до якого вона належала, життєве значення.

ІІ етап – починаючи з 1816 року – пов'язаний із початком використання штучно створюваних технічних засобів електро- і радіозв'язку. Для забезпечення скритності й перешкодостійкості радіозв'язку необхідно було використовувати досвід першого періоду інформаційної безпеки на вищому технологічному рівні, а саме застосування перешкодостійкого кодування повідомлення (сигналу) з подальшим декодуванням прийнятого повідомлення (сигналу).

ІІІ етап – починаючи з 1935 року – пов'язаний із появою засобів радіолокації й гідроакустики. Основним способом забезпечення інформаційної 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 радіоелектронними перешкодами.

IV етап – починаючи з 1946 року – пов'язаний із винаходом і впровадженням у практичну діяльність електронно-обчислювальних машин (комп'ютерів). Завдання інформаційної безпеки вирішувалися переважно методами і способами обмеження фізичного доступу до устаткування засобів добування, переробки і передачі інформації.

V етап – починаючи з 1965 року – зумовлений створенням і розвитком– локальних інформаційно-комунікаційних мереж. Завдання інформаційної безпеки також вирішувалися, в основному, методами і способами фізичного захисту засобів добування, переробки і передачі інформації, об'єднаних у локальну мережу шляхом адміністрування і управління доступом до мережевих ресурсів.

VI етап – починаючи з 1973 року – пов'язаний із використанням надмобільних комунікаційних пристроїв із широким спектром завдань. Загрози інформаційній безпеці стали набагато серйознішими. Для забезпечення 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 нанесення збитку інформаційній безпеці окремих користувачів, організацій і цілих країн. Інформаційний ресурс став найважливішим ресурсом держави, а забезпечення його безпеки – найважливішою й обов'язковою складовою

національної безпеки. Формується інформаційне право – нова галузь міжнародної правової системи.

VII етап – починаючи з 1985 року – пов'язаний зі створенням і розвитком глобальних інформаційно-комунікаційних мереж із використанням космічних засобів забезпечення. Можна припустити що черговий етап розвитку інформаційної безпеки, очевидно, буде пов'язаний із широким використанням надмобільних комунікаційних пристроїв із широким спектром завдань і глобальним охопленням у просторі та часі, забезпечуваним космічними інформаційно-комунікаційними системами. Для вирішення завдань інформаційної безпеки на цьому етапі необхідним є створення макросистеми інформаційної безпеки людства під егідою ведучих міжнародних форумів.

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 походження, 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 комунікацій.

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

4.1. Основні принципи забезпечення інформаційної безпеки держави.
4.2. Основні форми забезпечення інформаційної безпеки держави.
4.3. Методи забезпечення інформаційної безпеки.

4.1. 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 загроз та небезпек.

Метою забезпечення інформаційної безпеки є створення нормальних умов функціонування конкретного органу державного управління, а також проведення моніторингу стану інформаційної безпеки для розроблення оптимальної 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 держави;

– взаємна відповідальність суб'єктів забезпечення інформаційної безпеки;

– 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 – «попереджую») зумовлена властивою людині послідовністю виконання операцій, що складає будь-яку елементарну дію. Усе починається з приймання (добування) інформації, а закінчується активною дією: реакцією на одержану інформацію. 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.

2) адекватна інформованість об'єктів безпеки, у тому числі й міжнародних. 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 інформації повинні регулюватися законодавчими актами, які видаються щодо специфіки діяльності суспільних об'єднань та організацій або змісту інформації. Наприклад, адекватна інформованість суспільства про його матеріальні цінності досягається у сфері нормотворчості та правозастосування законодавства 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 інформаційної сфери можна говорити про його трансформацію в принцип адекватної інформованості держав світового співтовариства, який передбачає право кожної держави на інформаційну безпеку, забезпечення інформаційної безпеки всіх членів співтовариства рівною мірою, врахування інтересів усіх сторін без будь-якої дискримінації, виключення односторонніх переваг, відмова від дій, що наносять шкоду іншій державі. Законодавча база, яка визначає перелік відомостей, що віднесені до державної таємниці, механізм та порядок її захисту повинні розроблятися, виходячи із наведеного принципу, а також багатосторонніх угод держав, які входять до міжнародної системи інформаційної безпеки. Формування останньої буде, очевидно, справою далекої перспективи, яка ознаменує собою вищий рівень прояву довіри та зацікавленості держав світового співтовариства в забезпеченні виконання на практиці принципу адекватної інформованості. Така система повинна стати підсистемою в системі колективної безпеки.

4.2. Основні форми забезпечення інформаційної безпеки держави

Форми та способи забезпечення інформаційної безпеки утворюють власне інструмент, з допомогою якого сили інформаційної безпеки вирішують 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 інформаційної безпеки. Найважливіша вимога до обґрунтування способів, форм і механізмів 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 інтересів. Це є принциповим, оскільки застосування тих чи інших форм і способів 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 інформаційного 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 інформаційної безпеки держави відомостями про дестабілізуючі фактори і загрози стану інформованості фізичних і юридичних осіб (інформаційне

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

Інформаційний захист досягається шляхом внесення в порядку законодавчої ініціативи законопроектів, здійснення судового захисту, проведення оперативних заходів силами і засобами інформаційної безпеки.

Інформаційна кооперація – форма забезпечення інформаційної безпеки між рівноправними суб'єктами інформаційного процесу (фізичними, юридичними, міжнародними), який включає сукупність їхніх взаємоузгоджених дій, спрямованих на одержання відомостей про дестабілізуючі фактори, 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 інформаційного процесу. 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 стратегічних 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 інформованості з боку територіальних або відомчих органів інформаційної безпеки;

-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 (підприємств). Разом із тим за наявності у них власних органів інформаційної безпеки, їхні можливості у сфері автономного захисту суттєво розширюються.

4.3. 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 допомогою 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 залежно 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 системи державного управління необхідно, по-перше, описати, а лише потім класифікувати різні види загроз та небезпек, ризиків та викликів і відповідно 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 спричинили актуалізацію тих чи інших чинників небезпеки, а також розробляються заходи з їх нейтралізації. У числі таких методів причинних зв'язків можна назвати такі: **метод схожості, метод відмінності, метод сполучення схожості і відмінності, метод змін, що супроводжують, метод залишків.**

Вибір методів аналізу стану забезпечення інформаційної безпеки залежить 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, виділяють:

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 ідентифікації та перевірка дійсності користувачів, управління доступом, протоколювання й аудит, криптографія, екранування, забезпечення високої доступності.

управлінський, На рівні управління здійснюється управління, координація і контроль організаційних, технологічних і технічних заходів на всіх рівнях управління з боку єдиної системи забезпечення інформаційної безпеки органів державного управління.

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

рівень користувача, На рівні користувача реалізація політики інформаційної 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 координації дій органів державного управління, які пов’язані між собою однією метою.

Процедурний. На процедурному рівні вживаються заходи, що реалізуються людьми. Серед них можна виділити такі групи процедурних заходів: управління персоналом, фізичний захист, підтримання працездатності, реагування на порушення режиму безпеки, планування реанімаційних робіт.

Можна виокремити декілька типів методів забезпечення інформаційної безпеки:

однорівневі методи будуються на підставі одного принципу управління інформаційною безпекою;

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

комплексні методи – багаторівневі технології, які об’єднані в єдину систему координуючими функціями на організаційному рівні з метою забезпечення інформаційної безпеки з огляду на аналіз сукупності чинників небезпеки, які мають семантичний зв’язок або генеруються з єдиного інформаційного центру інформаційного впливу;

інтегровані високоінтелектуальні методи - багаторівневі, багатокомпонентні технології, які побудовані на підставі могутніх автоматизованих інтелектуальних засобів із організаційним управлінням.

Загальні методи забезпечення інформаційної безпеки активно використовуються на будь-якій стадії управління загрозами. До таких стадій належать:

прийняття рішення з визначення області та контексту інформаційної загрози 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 низьких організаційних ланках системи державного управління;

виділення необхідних політичних, економічних, соціальних, адміністративних і організаційних ресурсів, достатніх для реалізації програми відбиття інформаційної загрози та збереження сталого розвитку інформаційних 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 забезпечення інформаційної безпеки здебільшого зводяться до джерела загрози, апелювання до суспільної думки, а також до держави, яка має вживати рішучих заходів із нейтралізації інформаційних загроз. Саме суспільство почасти використовує у своїй діяльності методи соціального регулювання, надання допомоги окремим індивідам і суспільним організаціям, яким спричинена шкода внаслідок виявлення загрози.

Причому, на жаль, слід констатувати, що в нашій країні не на достатньому рівні усвідомлюють небезпеку саме в інформаційній сфері, немає штатних одиниць в органах державного управління із забезпечення інформаційної безпеки, не проводиться підготовка відповідних фахівців для органів державного управління.

Дуже важливим є застосування аналітичних методів пізнання і дослідження стану суспільної свідомості у сфері інформаційної безпеки. Наприклад, усвідомлення важливості забезпечення інформаційної безпеки на рівні індивіда, суспільства й організації заважає поширений міф про те, що захист інформації і криптографія те ж саме. Водночас таке розуміння є наслідком використання застарілих підходів до інформаційної безпеки, коли інформаційна безпека лише ототожнюються із захистом інформації шляхом її шифрування. Нині важливою умовою забезпечення інформаційної безпеки є не стільки секретність, конфіденційність інформації, скільки її доступність, цілісність, захист від загроз.

Отже, система має відповідно реагувати та гарантувати ефективну діяльність 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 допомогою криптографічних методів, не є головною вимогою при проектуванні систем захисту інформації органів державного управління. Виконання процедур криптокодування і декодування може уповільнити передачу даних та зменшити доступ до них через те, що працівник органу державного управління буде позбавлений можливості своєчасного та швидкого доступу до цих даних та інформації, через функціонування механізму захисту. Саме тому забезпечення конфіденційності інформації має відповідати можливості доступу до неї.

Отже, управління у сфері інформаційної безпеки має здійснюватися на підставі принципу доступності та безпеки. Система забезпечення інформаційної безпеки насамперед має гарантувати доступність і цілісність інформації, а її конфіденційність – у випадку необхідності. Також зазначимо, що вплив хакерів та їхня можливість суттєво вплинути на інформаційні системи 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 підсистеми забезпечення інформаційної безпеки. Переважно забезпечення інформаційної 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 спеціальні програми-фільтри, що відсіюють можливість доступу до внутрішньої мережі ззовні. Можна перераховувати й інші методи захисту інформації, водночас, нині ототожнення забезпечення інформаційної безпеки із забезпеченням безпеки комп'ютерних систем є просто концептуальною помилкою. 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, відкривають паралельні вікна в Інтернеті, та самі, не усвідомлюючи того, відкривають доступ не лише до інформації, що в цей час обробляється, а загалом до комп'ютерної мережі всієї системи органів державного управління, починаючи від Кабінету Міністрів України, закінчуючи місцевими органами виконавчої влади. Таким чином, один із найкращих засобів захисту інформації від нападу – не допускати його. Втім не треба плекати надію на створення 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 реалізація, а також негативні наслідки є природним компонентом системи інформаційної безпеки. Саме вони дають змогу побачити недоліки в системі управління інформаційною безпекою, і водночас слугують імпульсом до вдосконалення, 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 забезпечення 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 вирахування коефіцієнта ймовірності настання та розміру негативних наслідків. 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, система 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, відповідно, знижує здатність підтримувати державне управління в межах оптимальних параметрів. Причому аналіз подій у світі дає всі підстави стверджувати, що інформаційні війни стають органічною частиною політики національної 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 інформаційних атак у ході інформаційної війни.

Серед методів забезпечення інформаційної безпеки важливе значення має метод дихотомії. Для протидії загрозам інформаційній безпеці вживаються 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 недоцільності 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 небезпечних дій щодо об’єкта безпеки стає невигідним унаслідок виникнення небажаних наслідків або неможливим. Основним предметом за такого випадку є інформація, яка є у супротивника у вигляді відомостей, знань, оцінок. 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 властивостей. Вплив на інформаційну інфраструктуру важливий у тому випадку, коли загрозу може становити середовище поширення небезпечної інформації.

Методи впливу на інформацію у формі повідомлень можна поділити також на електронні та неелектронні.

Електронні методи впливу застосовуються в тих випадках, коли повідомлення закріплюються на електромагнітних носіях, що призначені для оброблення за допомогою засобів обчислювальної техніки. Вони полягають 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 реалізуються без використання засобів обчислювальної техніки для впливу на повідомлення, закріплення на інших, передусім паперових, носіях інформації.

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 конкретної 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

5.1. Основні форми інформаційного протиборства.
5.2. Інформаційна війна та її завдання.
5.3. Концепція інформаційної війни.
5.4. Органи інформаційної війни.
5.5. Основні форми інформаційної війни.

5.1. 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 стратегічних 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 боротьби, що становить сукупність спеціальних (політичних, економічних,

дипломатичних, технологічних, військових та інших) методів, способів і засобів вигідного впливу на інформаційну сферу об'єкта зацікавленості та захисту власної інформаційної сфери в інтересах досягнення поставлених цілей.

Інформаційне протиборство (у вузькому розумінні – у військовій, оборонній сферах) – це комплекс заходів інформаційного характеру, здійснюваних з метою захоплення й утримання стратегічної ініціативи, досягнення інформаційної переваги над противником і створення сприятливого пропагандистського підґрунтя при підготовці й веденні бойової й іншої діяльності збройних сил.

Види інформаційного протиборства: інформаційно-технічне й інформаційно-психологічне. Головними об'єктами впливу інформаційно-технічного протиборства є системи телекомунікації і зв'язку, радіоелектронні засоби тощо. Об'єктом інформаційно-психологічного протиборства залишаються свідомість і психіка населення й особового складу збройних сил, спецслужб противника та системи формування суспільної думки і прийняття стратегічних рішень.

Концепція інформаційного протиборства передбачає його ведення на воєнному та державному рівнях. На державному рівні метою інформаційного протиборства є послаблення позицій конкуруючих держав, підрив їхніх національно-державних основ, порушення системи національного управління за рахунок інформаційного впливу на політичну, дипломатичну, економічну та соціальну сфери життєдіяльності країни, проведення психологічних 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 протиборства країн.

За інтенсивністю, масштабами та засобами, які використовуються, виділяють такі ступені інформаційного протиборства: інформаційна експансія, інформаційна агресія та інформаційна війна.

Інформаційна експансія – діяльність із досягнення національних інтересів методом безконфліктного проникнення в інформаційну сферу з метою: поступової, плавної, непомітної для суспільства зміни системи соціальних 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 інформаційними ресурсами, інформаційно-телекомунікаційною структурою і національними ЗМІ; нарощування присутності власних ЗМІ в інформаційній 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 розміри, завданого збитку; обмеження розмірів простору, об'єктів інформаційної інфраструктури та соціальних груп, що піддаються ураженню інформаційною 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 агресором усієї поставленої конкретної мети й рідко набуває затяжного характеру), а також по силах і засобах, що залучаються.

5.2. Інформаційна війна та її завдання

Інформаційна війна – найвищий ступінь інформаційного протиборства, спрямований на розв'язання суспільно-політичних, ідеологічних, а також національних, територіальних та інших конфліктів між державами, націями, класами й соціальними групами шляхом широкомасштабної реалізації 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 застосовувати 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 національні правові норми, які дозволяють у мирний час (за відсутності офіційного оголошення війни з боку агресора) юридично кваліфікувати ворожі дії іноземної держави в інформаційній сфері, що супроводжуються нанесенням збитку інформаційній або іншій безпеці країни, як акції інформаційної агресії або інформаційної війни. Крім того, відсутні чіткі, однозначні, закріплені юридично критерії оцінки отриманого в результаті інформаційної агресії або інформаційної війни матеріального, морального, іншого збитку. Це дозволяє в мирний час активно використовувати самий небезпечний і агресивний арсенал сил і засобів інформаційної війни – як основний засіб досягнення політичної мети.

Інформаційна війна ведеться не тільки у фізичному просторі, де перебувають фізичні інформаційні системи і засоби, але й у деякій віртуальній зоні (віртуальному або кібернетичному просторі). Інформаційна війна розширює простір ведення війн, глибинами у світовому океані.

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

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

Будь-які міжнародні юридичні й моральні норми ведення інформаційної 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, злочинні, терористичні й наркобізнесові угруповання, комерційні фірми і навіть особи, які діють без злочинних намірів.

Завданнями інформаційної війни є:

– створення атмосфери бездуховності, негативного ставлення до культури та історичної спадщини в суспільстві конкурента чи ворога;

– маніпулювання громадською думкою й політичною орієнтацією населення держави з метою створення політичного напруження та стану, близького до хаосу;

– дестабілізація політичних відносин між партіями, об'єднаннями й рухами для розпалення конфліктів, стимулювання недовіри, підозри, загострення ворожнечі, боротьби за владу;

- провокування та застосування репресій із боку влади щодо опозиції;

– зниження рівня інформаційного забезпечення органів влади й управління, інспірація помилкових управлінських рішень;

– уведення населення в оману щодо роботи державних органів влади, підрив їхнього авторитету, дискредитація їхніх дій.

5.3. Концепція інформаційної війни

Концепція інформаційної війни – це система поглядів на інформаційну війну та шляхи її ведення.

За останніми оцінками, концепція інформаційної війни повинна передбачати:

- заглушення (у воєнний час) елементів інфраструктури державного і воєнного управління (ураження центрів командування й управління);

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

- одержання розвідувальної інформації шляхом перехоплення і декодування (дешифрування) інформаційних потоків, що передаються каналами зв'язку, а також побічним випромінюванням і за рахунок спеціально впроваджених у приміщення технічних засобів і електронних пристроїв перехоплення інформації (радіоелектронна розвідка);

- здійснення несанкціонованого доступу до інформаційних ресурсів (шляхом використання програмно-апаратних засобів зламу систем захисту інформаційних і телекомунікаційних мереж противника) із наступним їхнім спотворенням, знищенням або викраденням чи порушенням нормального функціонування цих систем (так звана «хакерна війна»);

- формування й масове поширення інформаційними каналами противника або глобальними мережами інформаційної взаємодії дезінформації або тенденційної інформації для впливу на оцінки, наміри й орієнтацію населення 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 масової інформації.

5.4. 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 планування 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 інформаційні атаки тактичного рівня і займаються ліквідацією наслідків інформаційного нападу; підрозділи розробки конструкцій та архітектури автоматизованих систем управління, що здійснюють розробку єдиної архітектури й технічних стандартів у галузі засобів і систем захисту від інформаційної зброї; групи незалежних експертів, що здійснюють аналіз уразливості АСУ, у тому числі через здійснення експериментальних атак на АСУ та їхні окремі елементи.

5.5. 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 інформації, 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 державному рівні є схилення воєнно-політичного керівництва противника до

прийняття вигідних для протилежної сторони рішень, то у воєнний час – повний параліч інформаційної інфраструктури противника при забезпеченні 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 спеціальна 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 противниками. Визначення мети операції, завдань, часу та місця проведення потребує безпосереднього затвердження воєнно-політичним керівництвом держави.

Для погодження запланованих дій і заходів у галузі інформаційного протиборства при керівництві державою створюють спеціальний міжвідомчий орган із забезпечення інформаційної безпеки та об’єднаний центр інформаційних операцій.

Їхніми завданнями є:

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

На воєнному рівні інформаційна війна планується вестись всебічно забезпеченими силами та засобами, що виділяються для боротьби із силами бойового управління противника. Метою даної боротьби є «обезголовлення» противника, позбавлення його надійної системи управління, захоплення ініціативи та примус противника реагувати на ситуацію, що склалася, бажаним для командування чином при забезпеченні високої стійкості, безперервності та оперативності функціонування своїх систем управління військами (силами).

Інформаційна війна на воєнному рівні ведеться на основі використання інформаційно-насичених засобів розвідки, зв’язку, автоматизації, радіоелектронної та психологічної війни, високоточної зброї та звичайних засобів 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 спеціальні бойові формування та органи управління ними. Цим формуванням приписується виконання таких функцій: підготовка й забезпечення планування інформаційних дій, координація зусиль у ході інформаційної операції; 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; придушення або дезорганізація частини інформаційної інфраструктури– противника з одночасним надійним захистом аналогічної структури своїх збройних 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 інформаційної переваги над противником. У цій операції головні зусилля спрямовуються 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 інформаційної переваги противника і має за мету зниження цієї переваги. У такій 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 бойового 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 послідовно 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 елементів 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 безпеку; 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 електромагнітного спектра, а також на забезпечення ефективного використання електромагнітного спектра своїми військами.

Радіоелектронна війна є основоположним елементом впливу як на системи управління противника в оперативній і тактичній ланках, так і загалом на інформаційну інфраструктуру противника. Вона включає три основних елементи:

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

Радіоелектронне забезпечення передбачає проведення заходів пошуку, перехоплення випромінювання в електромагнітному спектрі та визначення місцеположення джерел випромінювання для оцінки ступеню можливої загрози і прийняття рішення командирами всіх рангів, а також виконання додаткових функцій, таких як ухилення від загрози з боку противника і високоточна цілевказівка системам озброєння.

Радіоелектронна атака передбачає активний вплив на радіоелектронні засоби противника. За видом впливу атаки поділяється на два компоненти: неруйнівні впливи, які включають електронне придушення й електронну– дезінформацію; руйнівні впливи на основі застосування протирадіолокаційних ракет, зброї спрямованої енергії (лазерної, надвисокочастотної) і т. ін.

Радіоелектронна контрпротидія являє собою сукупність заходів, спрямованих на підвищення живучості та зменшення втрат своїх сил і засобів від впливу керованої зброї і засобів радіоелектронної протидії противника. Необхідні умови для досягнення інформаційної переваги Інформаційна перевага є одним із центральних понять у сфері інформаційного протиборства. Воно являє собою здатність складної саморегулюючої системи управління та інформаційного забезпечення держави або воєнного відомства забезпечити стійкий безперервний процес своєчасного одержання достовірної інформації та доведення її до відповідних споживачів при одночасному отриманні можливості використання у своїх інтересах такої ж системи ймовірного противника або пониження ефективності роботи (виведення з ладу) останньої. При цьому під саморегулюючою системою розуміють 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 споживачам 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

6.1. Інформаційна зброя та сфера її застосування.
6.2. Основні об'єкти застосування інформаційної зброї.
6.3. Види інформаційної зброї.
6. 4. Особливості застосування інформаційної зброї.

6.1. 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 оголошення 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 воєнними, 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 використання з метою: дезорганізації діяльності управлінських структур, транспортних потоків та– засобів комунікації; блокування діяльності окремих підприємств та банків, а також цільових галузей промисловості шляхом порушення багатоланкових технологічних зв'язків та системи взаєморозрахунків, проведення валютно-фінансових махінацій і т. ін.; ініціювання великих техногенних катастроф на території противника в результаті порушення 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.

6.2. Основні об'єкти застосування інформаційної зброї

Основними об'єктами застосування інформаційної зброї як к у мирний, 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 управління 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, телебачення і т. ін.).

6.3. Види інформаційної зброї

Існують різні критерії поділу інформаційної зброї.

За галузями застосування інформаційну зброю можна розділити на *інформаційну зброю воєнного та невоєнного (загального) застосування*. Інформаційна зброя, застосування якої можливе у воєнних умовах (радіоелектронна боротьба), включає в себе засоби з такими функціями:

- ураження звичайними боєприпасами за цілевказівками засобів радіо- та радіотехнічної розвідки з частковим самонаведенням на кінцевій ділянці;
- ураження високоточними боєприпасами нового покоління — інтелектуальними боєприпасами із самостійним пошуком цілі та самонаведенням на її вразливі елементи; радіопридушення засобів зв'язку маскувальними завадами;
- створення завад імітації, які ускладнюють входження у зв'язок, синхронізацію в каналах передавання даних, що ініціюють функції перезапиту та дублювання повідомлень;
- придушення за допомогою засобів силової радіоелектронної боротьби (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 інформаційних 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 собою сукупність спеціально організованої інформації та інформаційних технологій, яка дозволяє цілеспрямовано змінювати (знищувати, спотворювати), копіювати, блокувати інформацію, долати системи захисту, обмежувати допуск законних користувачів, здійснювати дезінформацію, порушувати функціонування носіїв інформації, дезорганізовувати роботу технічних засобів комп'ютерних систем та інформаційно-обчислювальних мереж, що застосовується в ході інформаційної війни (боротьби) для досягнення поставлених цілей.

За метою використання така інформаційна зброя поділяється на *інформаційну 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) порушуються інформаційні технології, що застосовуються в ІОМ. У складі інформаційної зброї атаки виділяють чотири основних види засобів інформаційних 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 виконання ІОМ цільових завдань.

Інформаційна зброя забезпечення – це інформаційна зброя, за допомогою 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 забезпечення дозволяє здійснювати деструктивні впливи на інформацію, що зберігається, обробляється й передається в мережах обміну інформацією, з використанням 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 інформаційної зброї до якої, зазвичай, відносять: алгоритми, що використовують сполучення санкціонованих дій для здійснення несанкціонованого доступу до інформаційних ресурсів; алгоритми застосування санкціонованого (легального) 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 програми (набори інструкцій) які мають спроможність виконувати будь-яку непусту множину таких функцій: приховування ознак своєї присутності в програмно-апаратному середовищі – мережі обміну інформацією; здатність 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 оперативній пам'яті; збереження фрагментів інформації з оперативної пам'яті в деякій ділянці – зовнішньої пам'яті прямого доступу (локальної або віддаленої); спотворення довільним чином, блокування і (або) підміна масивів інформації, що виводиться у зовнішню пам'ять або в канал зв'язку, утворених у результаті роботи прикладних програм, або масивів даних, що уже містяться у зовнішній пам'яті; придушення інформаційного обміну в телекомунікаційних мережах, фальсифікування інформації в каналах державного й воєнного управління; нейтралізація роботи тестових програм і систем захисту інформаційних ресурсів.

Програми з потенційно небезпечними наслідками умовно поділяють на такі класи: (бойові) комп'ютерні віруси; засоби несанкціонованого доступу; програмні закладки.

Комп'ютерні віруси (від лат. virus – «отрута»)] – це спеціальні програми, які здатні самочинно розмножуватися, створюючи свої копії, і поширюватися, модифікуючи (заражаючи) інші програми шляхом приєднання до них для наступного одержання управління та відтворення нових копій.

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

Комп'ютерні віруси можуть розмножуватися, впроваджуватися в програми, передаватися лініями зв'язку, мережами обміну інформацією, виводити 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 інформаційних– ресурсів. До засобів несанкціонованого доступу відноситься будь-яке позаштатне програмне забезпечення, яке противник може використати для порушення цілісності операційної системи або обчислювального середовища. Часто цей тип програмного забезпечення використовується для аналізу систем захисту з метою їхнього подолання й реалізації несанкціонованого доступу до інформаційних ресурсів мереж обміну інформацією. Відмінною ознакою (відносно програмних закладок) засобів несанкціонованого доступу є наявність функцій подолання захисту.

Програмні закладки. Відмінною ознакою є відсутність функцій подолання 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 закладки маскуються під звичайні пристрої мікроелектроніки й застосовуються для збирання, обробки та передавання конфіденційної інформації. Інформаційна зброя, що відноситься до різних класів, може застосовуватися спільно, 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 цілей зазвичай відносять: створення інформації, яку одержує політичне керівництво, командування та особовий склад збройних сил противника, та нав'язування їм фальшивої або беззмістовної інформації; психологічна обробка військ та населення; ідеологічні диверсії та дезінформування; організація масових демонстрацій під фальшивими лозунгами; пропаганда та розповсюдження фальшивих чуток; змінювання та керування індивідуальною 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, психоаналітичного впливу, нейролінгвістичного впливу, психотронного впливу та психотропного впливу.

6.4. 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 відомчі мережі;
- відсутність традиційних кордонів – відмінності між суспільним і особистим, воєнною і кримінальною поведінкою, а також географічні кордони, які історично складалися між націями, розмиваються зростаючою взаємопов'язаністю інформаційних інфраструктур;
- нові можливості для керування суспільною думкою – сучасні інформаційні технології надають широкі можливості для маніпулювання свідомістю людей і ускладнюють державі роботу з політичної підтримки ініціатив у галузі забезпечення безпеки;
- нові завдання перед органами розвідки – неправильне розуміння ролі, можливостей і цілей інформаційної зброї знижує ефективність традиційної розвідувальної 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 інформаційному 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 обмежені в географічному плані, то інформаційною зброєю можуть уражатися 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

7.1. Зміст теорії інформаційної боротьби.
7.2. Закони та закономірності інформаційної боротьби.
7.3. Принципи інформаційної боротьби.
7.4. Заходи інформаційної боротьби.
7.5. Способи та форми інформаційної боротьби.

7.1. Зміст теорії інформаційної боротьби

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

Інформаційна боротьба може бути як самостійним видом, так і складовою частиною будь-якого іншого різновиду боротьби (збройної, ідеологічної, економічної і т. ін.). Вона ведеться постійно як у мирний, так і у воєнний час. Масштаби інформаційної боротьби настільки великі, що її підготовка й ведення повинні носити плановий, систематичний характер, заснований на глибоких знаннях законів і закономірностей інформаційної боротьби.

Метою інформаційної боротьби – є забезпечення необхідного ступеня власної інформаційної безпеки й максимальне зменшення рівня інформаційної 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 визначають її зміст, а також і структуру теорії інформаційної боротьби.

На зміст інформаційної боротьби великий вплив справляє багато факторів, серед яких виділяють політичний, *економічний, духовний, власне воєнний 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 інформаційної 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. Положення воєнної доктрини держави, воєнні концепції протилежної сторони, стан та перспективи розвитку засобів інформаційної боротьби, історичний досвід та нагромаджені знання в цій галузі – саме ця база є головною при розробці фундаментальних положень теорії інформаційної боротьби та визначенні напрямків її розвитку.

Інформаційний фактор нерозривно пов'язаний з інформаційною боротьбою, оскільки остання ведеться в інформаційному середовищі та залежить від рівня інформатизації сторін. Цей фактор визначає розмах боротьби, порядок і способи її ведення, вибір напрямку ударів, структуру сил та засобів, можливості їхнього маневру при проведенні впливу на інформаційне середовище противника.

Загальні основи теорії інформаційної боротьби – найважливіші спільні вихідні положення теорії інформаційної боротьби. У загальних основах визначаються:

- 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 інформації, 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 інформаційної 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 фактори, що впливають на зміст і ефективність ураження інформації.

Теорія сил і засобів ураження інформації визначає та вивчає показники оцінки ефективності ураження інформації, математичну модель ураження інформації, стан підготовки і вирішення завдань ураження інформації.

Теорія захисту інформації включає загальні положення, що визначають: предмет, завдання і зміст теорії; об'єкти і елементи захисту інформації; основні фактори, що впливають на зміст і ефективність захисту інформації, а також визначає та вивчає загрози інформації й методологічні основи її захисту, систему показників оцінки ефективності захисту інформації, загальну математичну модель захисту інформації, організаційно-технічні і правові основи захисту інформації.

7.2. Закони та закономірності інформаційної боротьби

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

Закони інформаційної боротьби являють собою більш менш точне відображення у свідомості людей тих об'єктивних зв'язків і відносин, які існують і діють в інформаційному просторі. Якщо вони пізнані, відображені, описані, то стають основою для практичної діяльності з підготовки і ведення інформаційної боротьби.

Особливостями законів (закономірностей) війни, а також інформаційної боротьби є наступне:

1) вони проявляються тільки через діяльність людей;

2) мають універсальний характер кількість і якість засобів інформаційної боротьби, а також особового складу зумовлюють форми та способи інформаційної боротьби та її ефективність. Винайдення нових засобів інформаційної боротьби та їхнє впровадження в практику неминуче призводить до виникнення нових форм і способів інформаційної боротьби.

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

7.3. Принципи інформаційної боротьби

Принципи інформаційної боротьби – це науково обґрунтовані положення, правила, рекомендації з підготовки і ведення інформаційної боротьби, керівництва її силами й засобами. Вони створюються на основі законів 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 інформаційної боротьби політичним цілям;
- принцип необхідності зосередження сил та засобів інформаційної боротьби 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 середовище противника;
- принцип високої активності й рішучості дій;
- принцип узгодженого спільного застосування всіх сил і засобів інформаційної боротьби;
- принцип безперервності інформаційної боротьби;
- принцип відповідності (підпорядкованості) цілей і завдань інформаційної боротьби політичним цілям;
- принцип необхідності зосередження сил та засобів інформаційної боротьби 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 середовище противника;
- принцип високої активності й рішучості дій;
- принцип узгодженого спільного застосування всіх сил і засобів інформаційної боротьби;
- принцип безперервності інформаційної боротьби;
- принцип ведення інформаційної боротьби з напруженням, необхідним для вирішення поставлених завдань;
- принцип своєчасного маневру силами й засобами інформаційної боротьби;
- принцип раптовості, застосування несподіваних для противника способів виконання завдань;
- принцип врахування духовного фактора в інтересах виконання поставлених завдань;
- принцип всебічного забезпечення, підтримки боєздатності та своєчасності відновлення сил і засобів інформаційної війни;
- принцип твердості й безперервності управління силами і засобами інформаційної боротьби, непохитності в досягненні поставленої мети, виконанні прийнятих рішень і поставлених завдань.

7.4. Заходи інформаційної боротьби

Інформаційна боротьба включає комплекс заходів інформаційного забезпечення, інформаційного захисту й інформаційної протидії.

Інформаційне забезпечення в умовах інформаційної боротьби – це комплекс заходів добування інформації про противника в умовах протиборства, збирання інформації про свої сили і засоби, обробка інформації й обмін нею між органами керування з метою організації і ведення бойових дій. Результативність інформаційного забезпечення залежить від багатьох факторів 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 класифікувати таким чином:

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

Види інформування мають певні особливості.

Правильне інформування – це передавання органу керування неспотвореної інформації про істинну ситуацію.

Правильне дезінформування – це передавання органу керування неспотвореної інформації про неправдиву ситуацію.

Трансінформування – це передавання органу керування трансінформації (інформація про істинну ситуацію, трансформована в інформацію про неправдиву ситуацію).

Трансдезінформування – це передавання органу керування трансдезінформації (інформація про неправдиву ситуацію, перетворена в інформацію про правдиву ситуацію).

Сприйняття інформації – процес формування в органі керування уявлення про ситуацію, включаючи її кількісні та якісні параметри. Найбільш суттєві характеристики при цьому – розпізнавальні ознаки істинних і неправдивих елементів ситуації. Ступінь відповідності уявлень органу керування про ці характеристики їхнім вихідним величинам створює передумови для виникнення різноманітних ситуацій інформаційної боротьби. Ці передумови реалізуються залежно від того, наскільки інформація, що поступає, співвідноситься з образами істинних і неправдивих елементів ситуації, які зберігаються в інформаційному кадастрі.

Інформаційне рішення – це одиничний акт сприйняття органом керування поточної інформації про ситуацію та її віднесення до будь-якої відомості 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 інформаційного рішення передує всім іншим етапам процесу мислення людини або етапам обробки інформації в сучасних інформаційних системах.

Інформаційна протидія – сукупність заходів інформаційної боротьби, спрямованих на протидію інформаційному забезпеченню протиборчої сторони. Вона включає блокування добування, обробки й обміну інформацією та впровадження дезінформації на всіх етапах інформаційного забезпечення. Завдання інформаційної протидії вирішуються шляхом маскування, контррозвідки, радіоелектронного придушення й руйнування інформаційних систем противника.

Інформаційний захист – це сукупність заходів захисту від інформаційної 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 стійкої роботи засобів управління й розвідки в умовах ведення противником радіоелектронної боротьби, застосування розвідувально-ударних комплексів, самонавідної зброї та усунення взаємного впливу радіоелектронних засобів.

7.5. Способи та форми інформаційної боротьби

Способи інформаційної боротьби визначають порядок і прийоми застосування сил і засобів інформаційної боротьби для захоплення й утримання інформаційної переваги над противником при підготовці і проведенні 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 боротьби, 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 способів:

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 вирішення завдань управління військами (силами).

Інтелектуальні способи інформаційної боротьби реалізують рефлексне управління противником. Застосування таких способів дозволяє досягти інформаційної переваги в якості інформації, яка використовується для управління військами (силами).

Комбіновані способи інформаційної боротьби забезпечують досягнення 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) інформації 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 бойових 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 противника на вирішення другорядних завдань.

Спосіб сковування сил противника є різновидом способу відвернення 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 здійснювати невигідні й марні дії і, як наслідок, вступити в бій із розтраченими ресурсами та зниженою боєздатністю. При цьому можуть проводитися обмежені бойові або відволікаючі дії.

Спосіб інсценування полягає в тому, що на етапі підготовки до бойових 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 пильність 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 завдань у міждержавних конфліктах. Реалізація способу полягає в проведенні комплексу заходів інформаційної протидії, що дозволяє нав'язати противникові уяву про необхідність діяти всупереч коаліційним інтересам. З цією метою може використовуватися дезінформування громадської думки, а також формування фальшивих уявлень про воєнно-політичну ситуацію у голів держав, що беруть участь у конфлікті. Крім того, можуть проводитися заходи, які сприяють загостренню реально наявних або штучно створюваних суперечностей у стані ворога з метою зменшити його воєнну й економічну могутність.

До форм ведення інформаційної боротьби відносяться: *інформаційна операція, інформаційна битва, інформаційна дія (акція), інформаційний удар.*

Інформаційна операція (від лат. Operatio – «дія») – це сукупність узгоджених за метою, завданнями, місцем і часом дій (акцій), ударів і битв, що проводяться за єдиним задумом і планом для вирішення завдань інформаційної 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 угруповання військ (сил).

Інформаційна операція поділяється на наступні види:

1) Наступальна інформаційна операція, метою якої є завоювання інформаційної переваги над противником.
2) Оборонна інформаційна операція, її мета знизити переваги противника.

Інформаційна битва являє собою сукупність узгоджених і взаємопов'язаних за метою, завданнями, місцем і часом інформаційних дій та ударів, об'єднаних загальним задумом, які здійснюються спеціально

виділеними силами і засобами та спрямовані для вирішення одного оперативного 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, завданнями, місцем і часом заходів, що проводяться силами і засобами, залученими для ведення інформаційної боротьби, протягом певного часу в певному районі (напрямку). Під час інформаційних дій можуть здійснюватися інформаційні удари. Для ефективного проведення заходів інформаційної боротьби інформаційні впливи на противника необхідно починати ще у мирний час, нерідко заздалегідь до початку воєнних (бойових) дій. Такі інформаційні впливи зазвичай називають інформаційними акціями, оскільки вони виходять за межі власне інформаційної боротьби у сфері інформаційного протиборства геополітичних суб'єктів.

Інформаційні дії (акції) можна класифікувати за різними критеріями:

I. За видами:

1. наступальні
2. оборонні

II. За масштабом:

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

III. 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 узгоджений інформаційний вплив сил і засобів на найбільш важливий елемент (елементи) системи управління (керування) противника для досягнення рішучих цілей із завоювання інформаційної переваги (зниження інформаційної переваги противника). Інформаційні удари можна класифікувати за **масштабом** (*стратегічні, оперативно-стратегічні, оперативні, оперативно-тактичні, тактичні*), **типами** (*радіоелектронні, радіоелектронно-вогневі, комп'ютерні, спеціальні й комбіновані*) і **ступенем зосередження 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 боротьби.

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 ефективності інформаційної боротьби.

Розділ 8. ОСНОВИ БЕЗПЕКИ ІНФОРМАЦІЙНИХ РЕСУРСІВ

8.1. Поняття та загальні властивості інформації. Поняття загроз.
8.2. Загрози безпеки інформації та інформаційних ресурсів.
8.3. Джерела загроз безпеці інформації.
8.4. Класифікація вразливостей безпеки.
8.5. Моделі порушень інформаційних ресурсів.

8.1. Поняття та загальні властивості інформації. Поняття загроз.

Інформація – це зафіксоване на носії уявлення про предмети, процеси, події, явища та ін. Під фіксацією розуміють закріплення чого-небудь у певному положенні або вигляді. Найпростішим прикладом є письмове закріплення відомостей, думок. Інформація для свого функціонування завжди 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 розуміються передбачені, або встановлені Законом носії інформації: документи або інші носії інформації, які є матеріальними об’єктами, що зберігають інформацію.

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 психічна діяльність, що полягає у створенні уявлень і уявних ситуацій, яка загалом не сприймалася людиною в реальній дійсності (творча уява) або відтворюють 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 властивості для користувача або власника інформації можна розглядати як деякі бажані стани інформації (носіїв інформації). Такими властивостями є:

- конфіденційність – властивість інформації бути захищеною від несанкціонованого ознайомлення;
- цілісність – властивість інформації бути захищеною від несанкціонованого спотворення, руйнування або знищення;
- доступність – властивість інформації бути захищеною від несанкціонованого блокування.

8.2. 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 інформації з обмеженим доступом.

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

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

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

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 функцію проміжних носіїв інформації.

Загрози конфіденційності спрямовані на заборонене режимом доступу переміщення інформації від носія-джерела до носія-одержувача. Інформація зберігає конфіденційність, якщо додержується насамперед режимна адекватність носіїв інформації. Поняття «режимна адекватність» складається з термінів:

- режим – це сукупність норм для досягнення якої-небудь мети. Наприклад, для захисту інформації. Тут обов’язково враховується режим доступу до інформації як передбачений правовими нормами порядок отримання, використання, поширення і зберігання інформації;
- адекватність (від лат. Adaequatus – прирівняний, рівний) – це відповідність, 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 доступу (порядком отримання, використання, поширення та зберігання інформації) 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) різнотипних 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 навмисне або ненавмисне порушення комунікабельності носіїв інформації в процесі їх взаємодії. Порушення комунікабельності перериває дозволені режимом доступу процеси переміщення інформації. Інформація зберігає доступність, якщо зберігається комунікабельність носіїв інформації під час їх взаємодії.

З секретною інформацією пов’язані такі поняття, як:

Державна таємниця – вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки й техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати

шкоди національній безпеці України та які визнані в порядку, встановленому 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 таємницю, відображені у вигляді текстів, знаків, символів, образів, сигналів, технічних рішень, процесів тощо.

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

Допуск до державної таємниці – процедура оформлення права громадян на доступ до відомостей, що становлять державну таємницю, а підприємств, установ і організацій – на проведення робіт з використанням таких відомостей.

Доступ до відомостей, що становлять державну таємницю – надання уповноваженою посадовою особою дозволу громадянину на ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, або ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, цією посадовою особою відповідно до її службових повноважень.

Гриф секретності – реквізит матеріального носія секретної інформації, що засвідчує ступінь секретності даної інформації. Засекречування відомостей 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 завдати шкоди їхнім інтересам.

Ступінь секретності – категорія, що характеризує важливість такої інформації, можливі збитки внаслідок її розголошування, ступінь обмеження 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 стихійні 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, властивостями архітектури інформаційно-телекомунікаційної системи, протоколами обміну та інтерфейсами, що застосовуються, програмним забезпеченням 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 власнику 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 правопорушення. 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 інформації;
- матеріальні (фінансові) збитки від необхідності відновлення порушених 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 необережності, 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 зіставлені як мінімум із тим ризиком, який обговорюється цивільним, адміністративним або арбітражним правом, як предмет розгляду.

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

Порушення інформації та інформаційних ресурсів можуть бути різними, до них, як правило, відносять наступні:

Крадіжка – здійснення з корисливою метою протиправного безоплатного 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 шляхом 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 властивостей і воно стає повністю або частково непридатним для цільового використання.

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 доступу користувачів до інформації, не пов'язане з її знищенням.

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

Обман (заперечення автентичності, нав'язування хибної інформації) – 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 свідомо неправдивих відомостей.

8.3. Джерела загроз безпеці інформації

Носіями загроз безпеці інформації є **джерела загроз**. Джерелами загроз 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 загроз найбільш численна та становить найбільший інтерес з погляду організації 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 доступ (санкціонований або несанкціонований) до роботи зі штатними засобами об'єкта, що потребує захисту.

Суб'єкти (джерела), дії яких можуть призвести до порушення безпеки 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 висококваліфікованих спеціалістів у галузі розробки та експлуатації програмного забезпечення та технічних засобів, знайомих зі специфікою завдань, що вирішуються, структурою та основними функціями та принципами роботи програмно-апаратних засобів захисту інформації, які мають можливість використання штатного обладнання та технічних засобів мережі.

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

Друга група містить джерела загроз, що визначаються технократичною діяльністю людини та розвитком цивілізації. Проте наслідки, викликані такою діяльністю, вийшли з-під контролю людини та діють самі по собі. Людство дійсно стає все більше залежним від техніки, і джерела загроз, які залежать від властивостей техніки, менше прогнозовані й тому потребують особливої уваги. Цей клас джерел загроз безпеці інформації є особливо актуальним у сучасних умовах, оскільки очікується різке зростання кількості техногенних катастроф, викликаних фізичним та моральним старінням наявного обладнання, а також відсутністю коштів на його оновлення. Технічні засоби, що є джерелами потенційних загроз безпеці інформації, також можуть бути зовнішніми та внутрішніми.

Третя група джерел загроз об'єднує обставини, що становлять *непереборну силу, тобто такі обставини, які носять об'єктивний і абсолютний характер*, що поширюється на всіх. До непереборної сили в законодавстві 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 заходи 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.

8.4. Класифікація вразливостей безпеки

Загрози, як можливі небезпечності здійснення будь-якої дії, спрямованої проти об'єкта захисту, проявляються не самі по собі, а через вразливості (фактори), що призводять до порушення безпеки інформації на конкретному об'єкті інформатизації.

Вразливості безпеці інформації можуть бути:

1. Об'єктивні вразливості залежать від особливостей побудови та технічних характеристик обладнання, що застосовується на об'єкті захисту. Повне усунення цих вразливостей неможливе, але вони можуть суттєво послаблятися 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 малопередбачувані і їх усунення можливе тільки при проведенні комплексу організаційних та інженерно-технічних заходів із протидії загрозам інформаційній безпеці.

8.5. Моделі порушень інформаційних ресурсів

Особа – користувач ресурсами ІС, яка здійснює спробу несанкціонованого (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 зловмисними.

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, користувачів 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 кваліфікації, 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 програмування на мовах розробки програмних засобів ІС, проектуванню й експлуатації подібних до ІС систем;
- володіють інформацією щодо функцій і механізмів захисту, які реалізовані як у системі захисту інформації ІС, так і у функціях і механізмах захисту, що вбудовані в базове та прикладне програмне забезпечення.

За рівнем можливостей, які надаються штатною інфраструктурою інформаційної мережі, виділяють чотири рівні порушників:
- *перший рівень* відповідає найбільш низькому рівню можливостей порушника у системі – можливістю запуску фіксованого набору програм, які реалізують певні функції з обробки інформації;
- *другий рівень* визначається можливістю створення й запуску власних програм із новими функціями обробки й подальшого одержання потрібної порушнику 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 співробітників, які здійснюють розробку, впровадження й експлуатацію технічних засобів інформаційної системи, а також можливістю введення до складу інформаційної системи власних технічних засобів із новими функціями, щодо обробки й отримання інформації.

Приблизний перелік персоналу ІС і відповідний ступінь ризику щодо можливої реалізації загроз та нанесення шкоди залежно від зазначених робочих 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 магнітних 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 їхнього 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 атрибути доступу, з бажано найширшими правами щодо доступу до ресурсів ІС з метою їхнього використання, одержання необхідної інформації в потрібному обсязі, ознайомлення з конфіденційною інформацією, одержання можливості 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 ресурсів ІС з метою їхнього використання, одержання необхідної інформації в потрібному обсязі, ознайомлення з конфіденційною інформацією, одержання можливості її модифікації або знищення згідно зі своїми намірами.

Порушники переслідують певні наміри:

1. Одержання атрибутів доступу користувачів шляхом використання технічних засобів, крадіжок, купівлі, або одержання іншим шляхом.
2. Проникнення на місця розміщення тих або інших компонентів, елементів або ресурсів ІС (обчислювальних ресурсів, інформаційних ресурсів, базового 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 (технічних закладок) чи інших засобів технічної розвідки (у тому числі віддалених, наприклад, в елементах комунікаційної мережі зв’язку) для перехвату інформації.
5. Установки фізичних засобів у місцях розміщення елементів ІС (технічних закладок) або інших засобів (у тому числі віддалених, наприклад, в елементах комунікаційної мережі зв’язку) для генерації хибних сигналів, інформаційних символів або спотворених повідомлень.
6. Установки програмних засобів (програмних закладок або вірусів), копіювання інформації з метою її використання.

7. Установки програмних засобів (програмних закладок або вірусів) для модифікації системного програмного забезпечення, так і інформації ІС, шляхом введення програмних вірусів, спотворених сигналів, інформаційних символів або хибних повідомлень з метою перевантаження систем і порушення, таким чином, доступності компонентів ІС.
8. Здійснення спроб несанкціонованого доступу до обчислювальних та інформаційних ресурсів, базового та прикладного програмного забезпечення.
9. Здійснення спроб несанкціонованого доступу до системи захисту інформації як частини ІС, так і до її телекомунікаційної підсистеми, шляхом подолання системи управління доступом.

Порушник може знати:

- склад, розміщення, функціональні особливості, умови й режими функціонування елементів ІС, включаючи траси прокладених або можливих ліній зв'язку, комунікаційних мереж зв'язку й трафіки відповідних каналів передачі даних;
- порядок, засоби й режими здійснення охорони елементів ІС, місця їх розміщення 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 функціонування 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 користувачів з метою схованого подолання засобів управління доступом тощо;
- *рішучих зловмисників*, які мають на меті порушити ту або іншу властивість інформації. Зловмисники прагнуть перебороти: засоби організаційного обмеження доступу, охоронної сигналізації, тощо й одержати 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 інформаційних об'єктів з умов: витоку інформації технічними каналами, реалізації спеціальних впливів на інформацію з технічних каналів, впливу на мережеве устаткування локальних або розподілених мереж, у тому числі й засоби телекомунікаційних мереж, які використовуються елементами ІС.

Дії порушників можуть бути спрямованими на порушення функціональних властивостей захищеності інформаційних об'єктів, зокрема на порушення:

- конфіденційності, цілісності й доступності інформаційних об'єктів;
- функцій спостереження за діяльністю користувачів і процесів, однозначної 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 конфігурацію ІС (підключення додаткових або модифікація штатних технічних засобів, підключення або «врізання» у канали передачі даних, впровадження й використання спеціального ПЗ і т. ін.).

За місцем здійснення порушень дії зловмисника можна класифікувати:

- без одержання доступу на контрольовану територію із використанням технічних засобів віддаленого доступу через засоби: Internet, електронної пошти, модемного зв'язку чи дистанційної розвідки (наприклад: по оптичних, акустичних каналах і т. ін.), або з використанням засобів одержання інформації з мережі передачі даних (наприклад: шляхом підключення або «врізання» 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 несанкціонованим доступом до будинків, або приміщень, у яких розміщені елементи ІС;
- з одержанням доступу до робочих місць кінцевих користувачів ІС із подальшим несанкціонованим доступом до пристроїв введення/виводу інформації, копіювання, до канального або устаткування, яке утворює канал і до інших елементів ІС;

- з одержанням доступу до засобів управління ІС і засобів управління комплексною системою захисту інформації з подальшими розширеними можливостями доступу до ресурсів ІС та послуг системи.

Порушник (user violator) – це користувач, який здійснює несанкціонований 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 можливості, 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 кваліфікації, який має повну інформацію про систему.

Виділяють наступні типи порушників:

Зовнішні порушники:

- добре озброєна й оснащена силова група, що діє ззовні швидко й напролом;
- 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 допущений до життєво важливого центру ІС;
- основний персонал, що допущений до життєво важливого центру (найбільш небезпечний тип порушників);
- співробітників служби безпеки, які часто формально і не допущені до життєво важливого центру, але реально мають достатньо широкі можливості 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 життєдіяльності 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 діяльності?
11. Наведіть класифікацію порушника за характером дій.

Розділ 9. ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ ТА ІНФОРМАЦІЙНИХ РЕСУРСІВ

9.1. Напрями захисту інформації.
9.2. Правовий захист.
9.3. Організаційний захист.
9.4. Інженерно-технічний захист.

9.1. 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 основі;

організаційний захист – це регламентація виробничої діяльності та відносин виконавців на нормативно-правовій основі, яка виключає або послаблює нанесення будь-яких збитків виконавцям;

інженерно-технічний захист – це використання різноманітних технічних засобів, що перешкоджають нанесенню збитків.

Крім того, заходи захисту, орієнтовані на забезпечення безпеки інформації, можуть бути охарактеризовані багатьма параметрами, що відображають, крім напрямів, орієнтацію на об'єкти захисту, характер загроз, способи дій, їх поширення, охоплення та масштабність.

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

За способом дії їх можна поділити на попередження, виявлення, припинення 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, груповий або індивідуальний захист.

9.2. Правовий захист інформації

Правовий захист інформації як ресурсу признаний на міждержавному, державному рівні та визначається міждержавними договорами, конвенціями, деклараціями та реалізується патентами, авторським правом та ліцензіями на їхній захист.

На державному рівні правовий захист регулюється державними та відомчими актами. У нашій державі такими правилами (актами, нормами) є Конституція України, закони України, цивільне, адміністративне, кримінальне право, викладене у відповідних кодексах. Що стосується відомчих нормативних актів, то вони визначаються наказами, керівництвами та інструкціями, 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 України.

Вимоги інформаційної безпеки повинні органічно входити до всіх рівнів законодавства, у тому числі в конституційне законодавство, основні загальні закони, закони з організації державної системи управління, спеціальні 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 інформатизації 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 господарства, 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 представляє загальнодержавний інтерес.

Спеціальні закони, які відносяться до конкретних сфер відносин, галузей 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 законодавство як основу правового забезпечення інформаційної безпеки.

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

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

Ці закони також визначають основи захисту інформації в системах обробки 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, включаючи банки даних державного призначення, порядок державної реєстрації, ліцензування, сертифікації, експертизи, а також загальні принципи захисту та гарантій прав учасників інформаційного процесу. Питання правового режиму інформації з обмеженим доступом реалізуються у двох самостійних законах про державну та комерційну (проект) таємниці.

Таким чином, правовий захист інформації забезпечується нормативно-законодавчими актами, сукупність яких за рівнем являє собою ієрархічну систему від Конституції України до функціональних обов'язків і контрактів конкретного виконавця, які визначають перелік відомостей, що підлягають охороні, і заходи відповідальності за їх розголошення.

Одним із нових напрямків правового захисту є ***страхове забезпечення***. Воно призначене для захисту власної інформації та засобів її обробки 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 відшкодування збитків і втрат, які спричинені стихійними лихами, надзвичайними подіями в різних галузях діяльності, протиправними діями з боку конкурентів та зловмисників шляхом виплати грошової компенсації або надання сервісних послуг (ремонт, відновлення) при настанні страхової події.

Спираючись на державні правові акти та враховуючи відомчі інтереси на рівні конкретного підприємства (фірми, організації), розробляються власні нормативно-правові документи, орієнтовані на забезпечення інформаційної безпеки. До таких документів відносяться: положення про збереження конфіденційної інформації; перелік відомостей, які складають конфіденційну інформацію; інструкція про порядок допуску співробітників до відомостей, які становлять конфіденційну інформацію; положення про спеціальне діловодство та документообіг; перелік відомостей, які дозволені до опублікування у відкритому друці; положення про роботу з іноземними фірмами та їхніми представниками; зобов'язання співробітника про збереження конфіденційної інформації; пам'ятка співробітнику про збереження комерційної таємниці.

Нормативні акти спрямовані на попередження випадків неправомірного оголошення (розголошення) секретів на правовій основі – у випадку їх порушення повинні вживатися відповідні заходи впливу. Залежно від характеру 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 користування нею у вигляді ліцензії.

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

Комерційна таємниця – це відомості, які не є державними секретами, 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 відомості про господарську діяльність.

Створюючи систему інформаційної безпеки, необхідно чітко розуміти, що без правового забезпечення захисту інформації будь-які наступні претензії до несумлінного співробітника, клієнта, конкурента та посадової особи будуть просто безпідставними. Якщо перелік відомостей конфіденційного характеру не доведений своєчасно до кожного співробітника (природно, якщо він допущений до виконання посадових обов'язків) у письмовому вигляді, то співробітник, який викрав важливу інформацію при порушенні встановленого порядку роботи з нею скоріше всього не буде покараний.

Правові норми забезпечення безпеки та захисту інформації на конкретному підприємстві (фірмі, організації) відображаються в сукупності установчих, організаційних та функціональних документів. Вимоги забезпечення безпеки та захисту інформації відображаються у Статуті (установчому договорі) у вигляді таких положень: підприємство має право визначати склад, обсяги та порядок захисту конфіденційних відомостей, вимагати від своїх співробітників забезпечення їх збереження та захисту від внутрішніх та зовнішніх загроз; підприємство зобов'язане забезпечувати збереження конфіденційної інформації. Ці вимоги дають адміністрації підприємства такі права: створювати організаційні структури із захисту конфіденційної інформації; видавати нормативні та розпорядчі документи, які визначають порядок виділення відомостей конфіденційного характеру та механізми їхнього захисту; включати вимоги із захисту інформації в угоди з усіх видів діяльності; вимагати захисту інтересів підприємства з боку державних інстанцій; розробляти «Перелік відомостей конфіденційної інформації».

9.3. Організаційний захист

Організаційний захист – це регламентація виробничої діяльності та відносин виконавців на нормативній основі, що виключає або суттєво ускладнює неправомірне оволодіння конфіденційною інформацією та прояву 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 підприємства (організації).

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

або персоналу. Впливу цих аспектів практично неможливо запобігти за допомогою 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 приміщення сторонніх осіб;

– забезпечення зручності проходу та переміщення співробітників та відвідувачів;

– створення окремих виробничих зон за типом конфіденційних робіт із самостійними системами доступу;

– контроль та дотримання часового режиму праці та перебування на території персоналу підприємства;

– організація та підтримка надійного пропускного режиму та контролю співробітників і відвідувачів і т. ін.;

– організація роботи зі співробітниками, яка передбачає підбір і розстановку персоналу, включаючи ознайомлення зі співробітниками, їх вивчення, навчання правилам роботи з конфіденційною інформацією, ознайомлення з мірою відповідальності за порушення правил захисту інформації;

– організація роботи з документами та документованою інформацією, включаючи організацію розробки та використання документів і носіїв конфіденційної інформації, їх облік, використання, повернення, зберігання та знищення;

– організація використання технічних засобів збирання, обробки, нагромадження та зберігання конфіденційної інформації;

– організація роботи з аналізу внутрішніх та зовнішніх загроз конфіденційній 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 специфічну 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, використання пристроїв та ресурсів, відносини користувачів між собою відповідно 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, недбалістю 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 застосовуються разом із технічними методами, мають за мету виключити, зменшити або повністю усунути збитки при дії різноманітних деструктивних факторів.

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 стихійного 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 персонал був би зацікавлений у збереженні інформації, навчання правилам роботи 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 відповідальних за захист інформації у змінах, контроль за роботою персоналу, ведення автоматизованих журналів роботи, знищення встановленим порядком 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 спеціальних штатних служб захисту інформації* в закритих інформаційних системах 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, певним спеціально створеним для цих цілей структурним підрозділом, укомплектованим відповідними фахівцями з безпеки діяльності та захисту інформації.

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

та забезпечення охорони персоналу, матеріальних та фінансових цінностей та захисту конфіденційної інформації; забезпечення пропускного та внутрішньо-об'єктного режиму на території, у будівлях та приміщеннях, контроль дотримання вимог режиму співробітниками, суміжниками, партнерами та відвідувачами; керівництво роботами з правового та організаційного регулювання відносин із захисту інформації; участь у розробці основоположних документів з метою закріплення в них вимог забезпечення безпеки та захисту інформації, а також положень про підрозділи, трудові договори, угоди, підряди, посадові інструкції та обов'язки керівництва, спеціалістів, 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 виконання вимог «Інструкції із захисту конфіденційної інформації»; вивчення 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 діяльність підприємства та його клієнтів, партнерів, суміжників; розробка, ведення, оновлення та поповнення «Переліку відомостей, що носять конфіденційний характер» та інших нормативних актів, які регламентують порядок забезпечення та захисту інформації; забезпечення суворого виконання вимог нормативних актів із забезпечення виробничих секретів підприємства; здійснення керівництва службами та підрозділами безпеки підвідомчих підприємств, організацій, закладів та іншими структурами; організація та регулярне проведення обліку співробітників підприємства та служби безпеки з усіх напрямів захисту інформації та забезпечення безпеки виробничої діяльності; ведення обліку та суворого контролю виділених для конфіденційної роботи приміщень, технічних засобів у них, що мають потенційні канали витоку інформації та канали проникнення до джерел інформації, які перебувають під охороною; забезпечення проведення всіх необхідних заходів із припинення спроб нанесення моральних та матеріальних збитків з боку внутрішніх та зовнішніх загроз; підтримка контактів із правоохоронними органами та службами безпеки сусідніх підприємств для вивчення криміногенної ситуації в районі (зоні) та надання взаємної допомоги в кризових ситуаціях.

Служба безпеки є самостійною організаційною одиницею підприємства, що підпорядковується безпосередньо керівникові підприємства. Очолює службу безпеки начальник служби безпеки в посаді заступника керівника підприємства з безпеки.

Організаційно служба безпеки може складатися з таких структурних одиниць:

підрозділу режиму та охорони;

спеціального підрозділу з обробки документів конфіденційного характеру;

інженерно-технічних підрозділів;

інформаційно-аналітичних підрозділів.

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

Організаційні заходи є вирішальною ланкою формування та реалізації комплексного захисту інформації та створення системи безпеки підприємства.

9.4. 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 незаконного втручання в інформаційні ресурси.

Різноманітність цілей, завдань, об'єктів захисту та заходів, що проводяться, передбачають розгляд деякої системи класифікації засобів інженерно-технічного захисту за видом, орієнтацією та іншими характеристиками.

Наприклад, засоби інженерно-технічного захисту можна класифікувати за об'єктами впливу, характером заходів, способами реалізації, масштабом охоплення, класом засобів зловмисників, яким здійснюється протидія з боку служби безпеки.

За функціональним призначенням засоби інженерно-технічного захисту 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 перешкоджають фізичному проникненню (або доступу) зловмисників на об'єкти захисту та матеріальних носіїв конфіденційної інформації та здійснюють 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 завдання апаратних засобів – забезпечення стійкого захисту від розголошення, витоку і несанкціонованого доступу через технічні засоби забезпечення діяльності організації (підприємства).

Програмні засоби охоплюють спеціальні програми, програмні комплекси та системи захисту інформації в інформаційних системах різноманітного призначення та засобах обробки (збирання, нагромадження, зберігання, 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 методів шифрування.

Апаратні методи та засоби захисту знайшли достатньо широке розповсюдження. 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 гарантованого використання значно більший, ніж апаратних методів та засобів.

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

Очевидно, що такий поділ засобів захисту інформації достатньо умовний, оскільки на практиці дуже часто вони взаємодіють і реалізуються у вигляді програмно-апаратних засобів із широким використанням алгоритмів 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, апарати, вироби, призначені для створення перепон на шляху руху зловмисників. До фізичних засобів відносяться механічні, електромеханічні, електронні, електронно-оптичні, радіо- і радіотехнічні та інші пристрої для заборони 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, відносяться 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, кидання гранат і т. ін.).

Засоби пожежогасіння належать до систем ліквідації загроз. У загальному 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 фізичного 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 зловмисника на достатньо тривалий час. На сьогодні нараховується значний арсенал таких засобів: від простих сітчастих до складних комбінованих огорож, які здійснюють певний вплив відлякування на порушника.

Зони безпеки повинні розташовуватися на об'єкті послідовно, від огорожі 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, необхідного на подолання кожної зони, та ймовірність того, що розташовані в кожній зоні засоби виявлення (охоронні пости, охоронна сигналізація та охоронне телебачення) виявлять наявність порушника та подадуть сигнал тривоги.

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 фізичного захисту, сполучених із системами сигналізації.

До апаратних засобів захисту інформації відносяться найрізноманітніші за принципом дії, побудовою та можливостями технічні конструкції, які забезпечують припинення розголошення, захист від витоку та протидію несанкціонованому доступові до джерел конфіденційної інформації.

Апаратні засоби захисту інформації – це різноманітні технічні пристрої, системи та споруди, призначені для захисту інформації від розголошення, витоку і несанкціонованого доступу. Для захисту центральних процесорів (ЦП) застосовується кодове резервування – створення додаткових бітів у форматах машинних команд (розрядів секретності) і резервних регістрів (у пристроях ЦП). Одночасно передбачаються два можливих режими роботи процесора, які відділяють допоміжні операції від операцій

безпосереднього вирішення задач користувача. Для цього служить спеціальна 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 захисту даних. Застосовуються також додаткові біти парності – різновид методів кодового резервування. Для позначення ступеню конфіденційності програм і даних, категорій користувачів використовуються біти, які називаються бітами конфіденційності (це два-три додаткових розряди, за допомогою 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 ідентифікацію (автоматичне визначення коду або номера) терміналу, з якого поступив запит. У багато користувальницькому режимі цього терміналу його ідентифікації недостатньо. Необхідно здійснити аутентифікацію користувача, 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 використання. Для ідентифікації термінала найчастіше застосовується генератор коду, включений до апаратури терміналу, а для аутентифікації користувача - такі апаратні засоби як ключі, персональні кодові картки, персональний ідентифікатор, пристрої розпізнавання голосу користувача або форми його пальців. Проте найбільш поширеними засобами аутентифікації є паролі, перевірені не апаратними, а програмними засобами впізнавання.

Апаратні засоби захисту інформації - це різноманітні технічні пристрої, системи та споруди, призначені для захисту інформації від розголошення, витоку й несанкціонованого доступу.

Програмний захист інформації - це система спеціальних програм, які входять до складу програмного забезпечення та реалізують функції захисту інформації. Виділяють такі напрями використання програм для забезпечення безпеки конфіденційної інформації: захист інформації від несанкціонованого 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; реєстрації та контролю роботи технічних засобів та користувачів; обслуговування 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, креслю, 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 суміжних дисциплін. Як наука про шифри, криптографія довгий час була засекречена, оскільки застосовувалася переважно для захисту державних і воєнних секретів. Проте на теперішній час методи та засоби криптографії використовуються 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 механізмами захисту, які забезпечують дотримання конфіденційності, цілісності, 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

10.1. Джерела конфіденційної інформації.
10.2. Інформаційна система як об'єкт захисту.
10.3. Рівні захисту інформаційних систем.
10.4. Основні принципи захисту інформаційних систем.

10.1. Джерела конфіденційної інформації

Джерело інформації – це матеріальний об'єкт, що володіє певними відомостями (інформацією), що становлять конкретний інтерес для сторонніх 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 конфіденційної інформації, але й суб'єктами зловмисних дій. Люди є і власниками, і поширювачами інформації в межах своїх функціональних обов'язків. Вони володіють важливою інформацією, вони ще здатні її аналізувати, узагальнювати, робити відповідні висновки, а також, за певних умов, приховувати, красти, продавати та виконувати інші кримінальні дії, аж до вступу в злочинні зв'язки зі зловмисниками.

Документи – це найпоширеніша форма обміну інформацією, її нагромадження та зберігання. Під документом розуміють матеріальний носій інформації (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 формами.

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 організаційної 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, науково-технічні звіти, дисертації, рекламні проспекти, доповіді та ін.

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

Інформація може бути фіксованою та нефіксованою.

Фіксована інформація – це відомості, закріплені на якому-небудь фізичному 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 передавати ці знання іншим.

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

За специфікою призначення й виконання ***технічні засоби обробки інформації*** 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 входять різноманітні технічні засоби, такі, наприклад, як телефонні апарати й телефонний зв'язок; телеграфний, фототелеграфний і факсимільний зв'язок; системи радіозв'язку (автономні, територіальні, релейні, супутникові 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 сигналів, 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 характеристики, 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 виробництвом, експлуатацією, модернізацією та зняттям з виробництва. Кожен із цих етапів супроводжується специфічною інформацією, що проявляється різними фізичними ефектами, які у вигляді характеристик (демаскуючих ознак) можуть розкрити охоронювані відомості про вироблений товар.

Відходи виробництва, так званий непридатний матеріал, можуть багато 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 інформації 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 інформації містять досить повні відомості про склад, стан і напрямки діяльності підприємства.

10.2. Інформаційна система як об'єкт захисту

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

При вирішенні проблеми задоволення інформаційної потреби необхідно 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 інформаційним 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 різних 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 засоби (телефон, радіо, звукопідсилювальні системи, поліграфія) та автоматизовані системи.
5. Засоби передачі інформації (дротові, радіо, волоконно-оптичні).

Вихідною матеріальною основою роботи інформаційної системи виступають 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 цілей господарського й соціального розвитку.

Інформаційні ресурси можуть бути фіксованими й нефіксованими. Фіксовані 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 виробництві та здатні передавати ці знання іншим учасникам виробничого процесу.

Об'єктом захисту виступає *інформаційна система*

Предмет захисту інформації в інформаційній системі - *інформація*.

Для інформаційних систем як об'єктів безпеки властиві такі характеристики: *конфіденційність, доступність та цілісність інформації (даних) в інформаційній 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 встановлені 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 інформаційних 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 забезпечує:

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 цілісність даних, цілісність інформації, цілісність бази даних, цілісність інформаційної системи.*

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

Цілісність інформації – це властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем 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 заданих обмежень по точності та часовій узгодженості) і підпорядковуються правилам взаємної несуперечності. Підтримка цілісності бази даних містить 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.

10.3. 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, припустимих для зловмисників;
- оцінки припустимих витрат часу, засобів і ресурсів системи на організацію її захисту.

Система захисту інформації повинна виконувати такі функції:
- реєстрація й облік користувачів, носіїв інформації, інформаційних масивів;
- 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 підпису;
- 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 авторизованих абонентів до роботи в інформаційний системі, створено захисну оболонку навколо її елементів, а також організовано індивідуальне захищене середовище діяльності кожного користувача.
2. ***На мережевому рівні*** організовується захищений інформаційний обмін даними між автоматизованими робочими місцями, а також створюється надійна оболонка фізичного захисту периметра розташування ІС загалом. Система захисту на цьому рівні повинна будуватись з урахуванням реалізації захисту на попередніх рівнях.
3. ***На локальному рівні*** організовується розподілення інформаційних ресурсів ІС на сегменти за рівнями конфіденційності по територіальному і функціональному 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 інформаційної 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 автономною, але забезпечувати реалізацію єдиної політики безпеки й будуватись

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

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

10.4. Основні принципи захисту інформаційних систем

До основних принципів захисту інформаційних систем відносяться:

Принцип виправданості доступу – користувач повинен мати достатню «форму допуску» для отримання інформації того рівня конфіденційності, що він вимагає, і ця інформація дійсно необхідна йому для виконання виробничих функцій.

Принцип достатньої глибини контролю доступу. Засоби захисту інформації повинні включати механізми контролю доступу до всіх видів інформаційних і програмних ресурсів ІС, які у відповідності з принципом виправданості доступу слід розмежовувати між користувачами.

Принцип цілісності засобів захисту. Цей принцип передбачає, що засоби 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 званого ***«монітору звернень»,*** який контролює будь-які запити до даних чи програм з боку користувачів (чи їх програм) за установленими для них видами 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

11.1. Інформаційна безпека та її місце в системі національній безпеки України.
11.2. Основні реальні та потенційні загрози інформаційній безпеці України.
11.3. Стан та перспективи розвитку інформаційної безпеки.

11.1. Інформаційна безпека та її місце в системі національної безпеки України

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

Для характеристики цього стану використовується поняття національної безпеки. Законом України «Про національну безпеку України» визначаються та розмежовуються повноваження державних органів у сферах національної безпеки й оборони, створюється основа для інтеграції політики та процедур органів державної влади, інших державних органів, функції 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 такий спосіб демократичний цивільний контроль над органами та формуваннями сектору безпеки й оборони.

Згідно з цим Законом ***під національною безпекою України*** слід розуміти захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України 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, територіальної цілісності і демократичного конституційного ладу та інших життєво важливих 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, інших 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, територіальної цілісності і демократичного конституційного ладу та інших життєво важливих національних інтересів від реальних і потенційних загроз невоєнного 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 Конституція України, закони України, укази Президента України, ухвали й розпорядження Кабінету Міністрів України, інші нормативно-правові акти державних 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 цілісність.

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 держави із забезпечення безпеки; інтеграція з міжнародними системами безпеки.

Систему національної безпеки утворюють: органи законодавчої, виконавчої і судової влади; державні, суспільні й інші організації та об'єднання; громадяни, що беруть участь у забезпеченні безпеки відповідно до закону; законодавство, що регламентує відносини у сфері безпеки; сили забезпечення безпеки.

Для безпосереднього виконання функцій забезпечення національної безпеки в системі виконавчої влади створюються і діють сили забезпечення національної безпеки. Сили забезпечення безпеки включають: правоохоронні 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 політики у сфері забезпечення безпеки, системою заходів економічного, політичного й іншого характеру, адекватних загрозам життєво важливих інтересів особи, суспільства і держави. Оскільки в умовах інформатизації країни, розвитку інформаційних технологій, інформаційні ресурси формуються в усіх сферах діяльності, і насамперед у політичній, військовій, економічній, 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.

11.2. 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 забезпечення органів державної влади й управління;
- руйнування інтелектуального потенціалу, неготовність системи освіти до підтримання процесів випереджувального розвитку держави;
- повільність процесів усвідомлення прошарком колишньої радянської партійно-господарчої номенклатури, наукової й творчої інтелігенції, паростками 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 інформаційних послуг;
- руйнування національного інформаційною простору та виникнення можливості його використання в антидержавних інтересах;
- недостатній професійний, інтелектуальний і творчий рівень вітчизняних виробників інформаційного продукту та послуг, їхня не конкурентоспроможність на світовому інформаційному ринку;
- інформаційна експансія провідних іноземних держав, розроблення й використання ними, міжнародними чи вітчизняними злочинними організаціями різних сучасних способів безпосереднього підриву;

- мало контрольована діяльність окремих політичних сил, ЗМІ та осіб, спрямована на руйнування моральних цінностей, підрив морального й фізичного здоров'я нації;

- використання ЗМІ з позицій, протилежних інтересам громадян, політичних і громадських організацій, держави: втрата довіри до влади з боку значної частини населення внаслідок поширення компромату, застосування «брудних» політичних технологій, особливо під час виборчих кампаній;

- конкурентна боротьба за володіння ЗМІ, процес їхньої монополізації й концентрації інформаційної та політичної влади;

- маніпулювання громадською думкою (шляхом дезінформації,– перекручування даних, замовчування правдивих відомостей тощо).

Відсутність цілісної системи інформаційно-аналітичного забезпечення органів влади та управління значно ускладнює прийняття ними зважених. науково обґрунтованих рішень, що породжує конфліктні ситуації у владних структурах. Недостатнє інформаційно-аналітичне забезпечення діяльності характерне для всіх державних органів як на центральному, так і на регіональному рівнях. Владні структури не мають достатніх можливостей завчасно прогнозувати розвиток подій у державі та навколо неї, належним чином враховувати сприятливі й обмежувати несприятливі фактори, що визначають результативність прийнятих політичних рішень, здійснювати планування навіть на середньострокову перспективу. Організація роботи інформаційно-аналітичних підрозділів дотепер не має системного характеру, а в періоди чергових скорочень чисельності державних органів діяльність деяких таких підрозділів взагалі припиняється.

Основними реальними та потенційними загрозами інформаційній безпеці України є:

1) у зовнішньополітичній сфері: поширення у світовому інформаційному просторі викривленої, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України; прояви комп'ютерної злочинності, комп'ютерного тероризму, що загрожують стабільному та безпечному 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, спрямовані на підрив конституційного ладу, суверенітету, територіальної цілісності й недоторканності кордонів України; використання засобів масової інформації, Інтернету для пропаганди сепаратизму за етнічною, мовною, релігійною й іншими ознаками; несанкціонований доступ до інформаційних ресурсів органів державної влади; розголошення інформації, яка становить 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 військового управління та на підприємствах оборонно-промислового комплексу України; несанкціонований доступ до інформаційних ресурсів, незаконне збирання та використання інформації з питань оборони; реалізація програмно-математичних заходів із метою порушення функціонування інформаційних 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, недосконаліть партійно-політичної системи, непрозорість політичної та громадської діяльності, що створює передумови для обмеження свободи слова, маніпулювання суспільною свідомістю; негативні інформаційні впливи, у тому числі із застосуванням спеціальних засобів, на індивідуальну та суспільну свідомість; поширення суб'єктами інформаційної діяльності викривленої, недостовірної та упередженої інформації;

5) в економічній сфері: відставання вітчизняних наукоємних і високотехнологічних виробництв,– особливо у сфері телекомунікаційних засобів і технологій; недостатній рівень інформатизації економічної сфери, зокрема кредитно-фінансової системи, промисловості, сільського господарства, сфери державних закупівель; несанкціонований доступ, порушення встановленого порядку роботи з інформаційними ресурсами в галузях національної економіки, викривлення інформації в таких ресурсах; використання неліцензованого програмного забезпечення, засобів і комплексів оброблення інформації; недостатній рівень розвитку національної інформаційної інфраструктури;

6) у соціальній та гуманітарній сферах: відставання України від розвинутих держав за рівнем інформатизації соціальної та гуманітарної сфер, насамперед освіти, охорони здоров'я, соціального забезпечення, культури; недодержання прав людини і громадянина на отримання інформації, необхідної 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 інформаційного простору та молодіжної культури українських мистецьких творів, народних традицій і форм дозвілля; послаблення суспільно-політичної, міжетнічної та міжконфесійної єдності суспільства; відставання розвитку українського кінематографу, книговидання, книгорозповсюдження й бібліотечної справи від рівня розвинутих держав;

7) у науково-технічній сфері: зниження наукового потенціалу в галузі інформатизації та зв'язку; низька конкурентоспроможність вітчизняної інформаційної продукції на світовому ринку; відтік за кордон наукових кадрів і суб'єктів права інтелектуальної власності; недостатній захист від несанкціонованого доступу до інформації внаслідок використання іноземних інформаційних технологій і техніки; неконтрольована експансія сучасних інформаційних технологій, що створює передумови технологічної залежності України;

8) в екологічній сфері: приховування, несвоєчасне надання інформації або надання недостовірної інформації населенню про надзвичайні екологічні ситуації чи надзвичайні ситуації техногенного та природного характеру; недостатня надійність інформаційно-телекомунікаційних систем збору, обробки й передачі інформації в умовах надзвичайних ситуацій; низький рівень інформатизації органів державної влади, що унеможливлює здійснення оперативного контролю та аналізу стану потенційно небезпечних об'єктів і територій, завчасного реагування на надзвичайні ситуації.

Діяльність органів виконавчої влади у сфері забезпечення інформаційної безпеки України має бути зосереджена на конструктивному поєднанні діяльності держави, громадянського суспільства та людини за трьома головними напрямами: інформаційно-психологічному, зокрема щодо забезпечення конституційних прав і свобод людини й громадянина, створення сприятливого психологічного клімату в національному інформаційному просторі для затвердження загальнолюдських та національних моральних цінностей; технологічного розвитку, зокрема стосовно розбудови та інноваційного оновлення національних інформаційних ресурсів, впровадження новітніх технологій створення, оброблення та поширення інформації; захисту інформації, зокрема щодо забезпечення конфіденційності, цілісності й доступності інформації, у тому числі технічного захисту інформації в національних інформаційних ресурсах від кібернетичних атак.

11.3. Стан та перспективи розвитку інформаційної безпеки України

Відповідно до законодавства України, інформаційна безпека має таке визначення: «стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, 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-культурного життя народу України;
- створення та впровадження безпечних інформаційних технологій;
- захист права власності всіх учасників інформаційної діяльності в національному просторі України;
- збереження права власності держави нестратегічні об'єкти інформаційної інфраструктури України;
- охорону державної таємниці, а також інформації з обмеженим доступом, що є об'єктом права власності або об'єктом лише володіння, користування 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 розповсюдження 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 державами;
- законодавче визначення порядку поширення інформаційної продукції зарубіжного виробництва на території України.

Державна політика інформаційної безпеки визначається пріоритетністю 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 здійснюють діяльність щодо інформаційного простору держави, з метою досягнення адекватного рівня спроможності держави відповідати реальним та потенційним загрозам національним інтересам України в інформаційній сфері; законодавче врегулювання механізму виявлення, фіксації, блокування та видалення з інформаційного простору держави, зокрема з українського сегмента мережі Інтернет, інформації, яка загрожує життю,

здоров'ю громадян України, пропагує війну, національну та релігійну ворожнечу, зміну конституційного ладу насильницьким шляхом або порушення територіальної цілісності України, загрожує державному суверенітету, пропагує комуністичний та/або націонал-соціалістичний (нацистський) тоталітарні режими та їхню символіку; визначення механізмів регулювання роботи підприємств телекомунікацій, поліграфічних підприємств, видавництв, телерадіоорганізацій, телерадіоцентрів та інших підприємств, установ, організацій, закладів культури та засобів масової інформації, а також використання місцевих радіостанцій, телевізійних центрів та друкарень для військових потреб і проведення роз'яснювальної роботи серед військ та населення; заборони роботи приймально-передавальних радіостанцій 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 держав, які не є підписантами зазначеної Конвенції; створення і розвиток структур, що відповідають за інформаційно-психологічну безпеку, насамперед у Збройних Силах України, з урахуванням практики держав – членів НАТО; розвиток і захист технологічної інфраструктури забезпечення інформаційної безпеки України; забезпечення повного покриття території України цифровим мовленням, насамперед у прикордонних районах, а також тимчасово окупованих територій; розвиток цифрового мовлення, унеможливлення впливу на його інфраструктуру суб'єктів, що пов'язані з державою-агресором; побудова дієвої та ефективної системи стратегічних комунікацій; розвиток механізмів взаємодії держави та інститутів громадянського суспільства щодо протидії інформаційній агресії проти України; боротьба з дезінформацією та деструктивною пропагандою з боку Російської Федерації; посилення спроможностей сектору безпеки і оборони щодо протидії спеціальним інформаційним операціям, спрямованим на зміну конституційного ладу насильницьким шляхом, порушення суверенітету і територіальної цілісності, підрив обороноздатності України, деморалізацію особового складу Збройних Сил України та інших військових формувань, загострення суспільно-політичної ситуації; виявлення та притягнення до відповідальності згідно із законодавством суб'єктів українського інформаційного простору, що створені та використовуються державою-агресором для ведення інформаційної війни проти України, та унеможливлення їхньої підривної діяльності; унеможливлення вільного обігу інформаційної продукції (друкованої та електронної), насамперед походженням з території держави-агресора, що містить пропаганду війни, національної і релігійної ворожнечі, зміни конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України, провокує масові заворушення; проведення розвідувальними органами України акцій

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

2) щодо забезпечення захисту і розвитку інформаційного простору України, а також конституційного права громадян на інформацію: стимулювання розвитку національного виробництва текстового і аудіовізуального контенту, зокрема шляхом створення системи квотування та проведення цільових конкурсів на надання грантів; забезпечення функціонування Суспільного телебачення і радіомовлення України, у тому числі його належного фінансування; створення системи мовлення територіальних громад, яка сприятиме розширенню комунікативних можливостей та зниженню конфліктності всередині громад; підтримка вітчизняної книговидавничої 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 механізмів саморегуляції засобів масової інформації на засадах соціальної відповідальності; підвищення медіа-грамотності суспільства, сприяння підготовці професійних кадрів для медіа-сфери з високим рівнем компетентності; удосконалення законодавчого регулювання інформаційної сфери відповідно до актуальних загроз національній безпеці; задоволення потреб населення тимчасово окупованих територій в об'єктивній, оперативній і достовірній інформації; повне покриття території України цифровим та інтернет-мовленням замість аналогового і надання рівних можливостей доступу кожному громадянину до інформаційних ресурсів мережі Інтернет; формування системи державної підтримки виробництва вітчизняного аудіовізуального продукту; пропагування, у тому числі через аудіовізуальні засоби, зокрема соціальну рекламу, основних етапів і досвіду державотворення, цінностей свободи, демократії, патріотизму, національної єдності, захисту України від зовнішніх і внутрішніх загроз;

3) щодо відкритості та прозорості держави перед громадянами: розвиток механізмів електронного урядування; сприяння розвитку можливостей доступу та використання публічної інформації у формі відкритих даних; інформування громадян України про діяльність органів державної влади, налагодження ефективної співпраці зазначених органів із засобами масової інформації та журналістами; проведення реформи урядових комунікацій; 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;

4) щодо формування позитивного міжнародного іміджу України: ґрунтовне реформування системи представлення інформації про Україну на міжнародній арені; розвиток публічної дипломатії, у тому числі культурної та цифрової; активізація скоординованої інформаційної роботи закордонних дипломатичних установ України; сприяння поширенню та розвитку системи іномовлення України; створення та забезпечення функціонування правового механізму взаємодії державних органів з інститутами громадянського суспільства з метою інформаційної підтримки комерційної, гуманітарної, просвітницької, культурної та іншої діяльності таких інститутів за межами України; постійний моніторинг пропаганди держави-агресора, розроблення та оперативна реалізація адекватних заходів протидії; недопущення використання міжнародного інформаційного простору в деструктивних цілях або для дій, що спрямовані на дискредитацію України на міжнародному рівні; реформування системи взаємовідносин з українською діаспорою шляхом забезпечення більш тісної співпраці та проведення ефективних заходів, зокрема в рамках комунікацій «від людини до людини»; участь у міжнародних культурних заходах з метою представлення національної культури та ідентичності; запровадження міжнародних культурних фестивалів 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 інтересів в інформаційній сфері створення розвиненого й захищеного інформаційного середовища слугує організація функціонування системи інформаційної безпеки, складовими компонентами якої є національні інтереси в інформаційній сфері, загрози та небезпеки цим інтересам, сама інформаційна безпека як інструмент зі створення сприятливих умов для їх реалізації, які в сукупності становлять об’єкт управління органами державного управління, систему забезпечення інформаційної безпеки, тобто суб’єкт управління, більше того, основні напрямки політики національної безпеки в інформаційній сфері, а також внутрішнє та зовнішнє середовище.

Інформаційна безпека забезпечується комплексом заходів системи забезпечення національної безпеки України, що включає сукупність державних 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 перед державою?

5. В яких сферах проявляються реальні та потенційні загрози безпеці України?
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-%D0%B2%D1%80#Text
2. Конвенція Ради Європи про кіберзлочинність, ратифікована Законом України від 7.09.2005 року № 2824-IV. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/994_575#Text
3. 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
4. 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
5. Про захист інформації в інформаційно-телекомунікаційних системах: Закон 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
6. Про доступ до публічної інформації: Закон України // Відомості Верховної Ради України (ВВР), 2011, № 32, ст. 314. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/2939-17#Text
7. Про Державну службу спеціального зв'язку та захисту інформації України: 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
8. 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

9. Директива 97/66/ЄС Європейського Парламенту і Ради «Стосовно обробки 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
10. Решение № 1106 «Первоначальный перечень мер укрепления доверия в рамках ОБСЕ с целью сокращения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий» от 03.12.2013. [Електронний ресурс]. Режим доступу: https://www.osce.org/files/f/documents/0/a/109648.pdf
11. 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 доступу: https://zakon.rada.gov.ua/laws/show/995_266#Text
12. Верголяс О.О. Міжнародно-правове регулювання інформаційного протиборства: реалії та перспективи. Visegrad Journalon Human Rights. 2019. №3. С. 58-63
13. Дудикевич В. Б., Опірський І. Р., Гаранюк П. І., Зачепило В. С., Партика А. І. Забезпечення інформаційної безпеки держави: навч. посіб. Львів: Видавництво Львівської політехніки, 2017. 204 с.
14. Ємельянов В. М. Кібербезпека як складова національної безпеки та кіберзахист критичної інфраструктури України / В. М. Ємельянов, Г. Л. Бондар // Публічне управління та регіональний розвиток. – 2019. – № 5. – С. 493-523.
15. 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.
16. Інформаційна безпека / За ред. Ю. Я. Бобала та І. В. Горбатого. Львів: Вид-во Львівської політехніки. 2019. 580 с.
17. Історія інформаційно-психологічного протиборства: підруч./ [Я.М.Жарков, 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.
18. Кіберзлочини в Україні (кримінально-правова характеристика) [Текст] : навч. посіб. / А. В. Боровик, І. М. Копотун. - Луцьк : Волинь Поліграф, 2019. - 304 с.
19. Корпоративна безпека: практичний посібник. Консалтингова компанія Сідкон. 2018. 276 с.
20. Когут Ю.І. Кібербезпека та ризики цифрової трансформації компаній. Вид-во SIDCON. 2021. 372 с.
21. Лісовська Ю. П. Інформаційна безпека України: навч. посіб. Київ: Кондор, 2018. 172 с.

21. Лизанчук В. Інформаційна безпека України: теорія і практика. Львів. Вид-во ЛНУ ім. Івана Франка. 2017. 728 с.
23. Мехед Д., Ткач Ю., Базилевич В., Гур'єв В., Усов Я. Аналіз вразливостей корпоративних інформаційних систем. Захист інформації. 2018. № 1. С. 61 – 66.
24. Могильний С.Б. Інформаційна безпека при роботі в Інтернеті: навч.-метод. посібник / за ред. О. В. Лісового та ін. – К., 2018. – 105 с.
25. Нашинець-Наумова А.Ю. Інформаційна безпека суб'єктів господарювання: проблеми теорії та практики правозастосування: Монографія. Видав. Дім «Гельветика». 2017. 386 с.
26. Петрик В., Присяжнюк М. Інформаційна безпека держави. Підручник у 2-х томах. Київ. Вид-во «Книжкова палата України». 2016. 264 с.
27. Почепцов Г. Сучасні інформаційні війни / Г. Почепцов. – К. : Вид.дім «Києво-Могилянська академія», 2015. – 497 с.
28. Почепцов, Г. Виртуальные войны. Фейки [Текст] / Георгий Почепцов. Харьков : Фолио, 2019. 506 с.
29. Почепцов Г. Сучасні інформаційні війни / Г. Почепцов. – К. : Вид.дім «Києво-Могилянська академія», 2015. – 497 с.
30. Харитонов Є.О., Давидова І.В. Інформаційна безпека: проблеми приватного 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 органів виконавчої влади України. – Режим доступу : https://www.kmu.gov.ua/
3. Офіційний вісник України. – Режим доступу : www.gdo.kiev.ua.
4. Статистика України: науковий журнал [Електронний ресурс]. – Режим доступу : www.ukrstat.gov.ua.

ЗМІСТ

Вступ 3

Зміст та структура навчальної дисципліни 5

Розділ 1. Поняття інформаційної безпеки держави, суспільства та особи .. 7

Розділ 2. Інформаційна безпека та кібербезпека 17

Розділ 3. Загрози для інформаційної безпеки держави, суспільства, людини 23

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

Розділ 7. Основи теорії інформаційної боротьби 56

Розділ 8. Основи безпеки інформаційних ресурсів 65

Розділ 9. Забезпечення безпеки інформації та інформаційних ресурсів ... 78

Розділ 10. Захист інформаційних систем 91

Розділ 11. Інформаційна безпека України 98

Рекомендована література 108

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