МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДНІПРОВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ
ОЛЕСЯ ГОНЧАРА

ІНФОРМАЦІЙНА БЕЗПЕКА

КОНСПЕКТ ЛЕКЦІЙ

Дніпро 2022

ІНФОРМАЦІЙНА БЕЗПЕКА: Конспект лекцій / Укладач В.І.Стаценко. Друге навчальне видання. Дніпро [Електронний ресурс]: Репозиторій ФТФ ДНУ, 2022. – 95с..

Кафедра Кібербезпеки та комп’ютерно-інтегрованих технологій

ВСТУП

Інформаційна сфера, як системоутворюючий фактор життя сучасного суспільства, активно впливає на стан політичної, економічної, оборонної та інших складових національної безпеки України.

В сучасному конкурентному світі є дуже актуальним захист головного ресурсу XXI сторіччя – інформації у всіх сферах діяльності: в науці, бізнесі, на державній службі, в особистому житті.

Виграє той, хто вміє регулювати інформаційні потоки у своїх власних інтересах та здатний забезпечити конфедиційність, цілісність та доступ до необхідної інформації для прийняття важливих рішень

Зараз, як ніколи для людині дуже важливе розуміння особливостей інформаційних відносин у сучасному суспільстві, в соціальних, технічнокібернетичних систем та держави у цілому, базові навички критичного та системного мислення, розуміння методів обробки та інтелектуального аналізу інформації з метою протидії інформаційним атакам, маніпуляційному впливу.

Навичка протидії проявам інформаційної зброї; маніпуляціям та деструктивному використанню «соціальної інженерії» є основою ефективного мислення та прийняття рішень в умовах невизначеності, здатності забезпечити цілістність та захищеність власних інформаційних ресурсів.

Конспект лекцій призначений для студентів, які цікавляться інформаційною безпекою, її ролью в підвищенні власної ефективності, розвитку кар'єри та бізнесу.

ТЕМА 1. КОРОТКА ІСТОРІЯ РОЗВИТКУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ. ЇЇ РОЛЬ В СУЧАСНОМУ СВІТІ

«Хто володіє інформацією – той володіє Світом!» цей крилатий вислів належить Натану Ротшильду - міжнародному банкіру, бізнесмену і фінансисту. Він народився в 1777 році в Священній Римській імперії на території сучасної Німеччині, молодою людиною переїхав до Англії, де почав свою бізнес-діяльність. Існує багато версій як Ротшильди за один день заробили 100 мільонів фунтів стерлінгів, що і зараз є величезною сумою, а у червні 1815 року масштаб тих грошей був захмарним. Історики зараз сперечаються – чи дійсно Ротшильд знав першим про фінал битви при Ватерлоо, чи ні, но так чи інакше, Натан блискуче провів свого роду ІПСО того часу і скупив с значним дисконтом цінні папери на біржі.

Якщо переказати ту давню історію сучасними термінами Інформаційної безпеки, то Ротшильд забезпечів собі ДОСТУПНІСТЬ до важливої та актуальної інформації, в власних інтересах порушив її ЦІЛІСНІСТЬ для конкурентів, та на певний час забезпечив її КОНФІДЕНЦІЙНІСТЬ, що і дало йому суттеву конкурентну перевагу. Принципово нічого не змінилося і до нашого часу. Забезпечення КОНФІДЕНЦІЙНІСТі, ЦІЛІСНОСТІ та ДОСТУПНОСТІ і є основна «триєдина задача» інформаційної безпеки. Саме вона і є передумовою прийняття вірних, зважених рішень на підгрунті ретельного аналізу інформації, яка має відношення до питання, що розглядається.

Існує ще один крилатий вираз – «Наш мозок приймає вірне рішення на базі тієї інформації, яка була доступна та проаналізована в момент прийняття рішення. Цей парадоксальний вираз найкраще описує важливість забезпечення виконання триєдиної задачі.

Триєдина задача ІБ

Формування інформаційного суспільства є закономірним етапом еволюції сучасного соціуму, що характеризується, в першу чергу, масштабним впровадженням інформаційних технологій і розвитком глобального інформаційного простору. Процес становлення нового суспільства, обумовлений впровадженням інформаційних технологій, потребує правильного усвідомлення його інформаційної специфіки і конструктивного розвитку закладеного в ньому потенціалу.

Проблема захисту, що виникла в третьому тисячолітті, завдяки новим видам небезпек і загроз, породжених інформатизацією, турбує дослідників сучасного суспільства.

Складність висвітлення проблеми інформаційної безпеки до теперішнього часу, як зазначають фахівці, пов'язана з відсутністю загальноприйнятого тлумачення термінів, що описують розглянуту предметну область. Поряд з терміном «інформаційна безпека» активно використовується термін «безпека інформації». Не викликає сумнівів той факт, що дані поняття взаємопов'язані.

Інформаційне середовище визначає якість функціонування життєдіяльності суспільства, його рівень розвитку та безпеку. Інформаційна взаємодія, його своєчасність, повнота та інтенсивність

регулюють всі процеси життєзабезпечення суспільства. Тому інформаційна інфраструктура - основна мета інформаційної зброї.

Інформаційна революція починається зі створення електронно-обчислювальних машин в кінці 40-х років XX століття, з того часу обчислюється ера розвитку інформаційних технологій, матеріальне ядро яких утворює мікроелектроніка. Процес розвитку сучасних технологій відображає якісну перебудову інформаційного середовища людини і все зростаюче на цьому тлі значення інформації - головної суспільної цінності, специфічно людської і сутнісно-центральній для інформаційної технології.

Інформаційні технології вплинули на свідомість людини і можливості, змінили його образ життя. Сучасні інформаційні технології поміняли пріоритети і цінності. Сьогодні використовуються в суспільстві інформаційні технології розглядаються як фактор, який надає величезний вплив на глобальний розвиток соціуму і формування інформаційної реальності. В даний час інформаційна сфера опинилася серцевиною економічних, соціальних, політичних та інших конфліктів в суспільстві. Проявилися згодом використання сучасних технологій основні небезпеки і загрози систематизовані в залежності від сфер життєдіяльності суспільства.

Так, в соціальній сфері виникла небезпека нової нерівності в суспільстві: реальна загроза «інформаційного розшарування», яка веде до потенційної загрози формування інформаційної еліти суспільства. Крім того, зростаючу тривогу для суспільства і держави викликає поява нового виду злочинності - комп'ютерної, або кіберзлочинності.

У духовно-культурній сфері суспільства небезпека застосування в протиправних цілях інформаційних технологій призвела до загрози маніпулювання людською свідомістю, психічної і соціальної дезадаптації людини. Небезпека заподіяння шкоди здоров'ю людини в результаті використання інформаційних технологій породила загрозу розвитку різних видів захворювань.

Необхідною умовою нормального існування і розвитку кожного суспільства є його захищеность від широкого спектру загроз – зовнішних та внутрішніх, стійкість до спроб зовнішного тиску, здатність ефективно протистояти спробам атак, нейтралізувати нові загрози, забезпечувати такі умови існування країни та державного апарату, які гарантують стабільний та всебічний прогрес суспільства та його громадян. Для характеристики цього стану використовують поняття національної безпеки. НБ – захищеность життево важливих фнтересфів людини й громадянина, суспільства та держави, за якої забезпечують сталий розвиток суспільства, своєчасне виявлення, запобігання та нейтралізацію реальних та потенційних загроз національним інтересам.

Економічний стан держави сьогодні прямим чином залежить від ситуації, що складається в області створення і застосування інформаційних технологій, внаслідок чого як позитивні рішення в даній області, так і економічні кризи набувають глобального характеру. Крім того, широке впровадження технологій в процеси виробництва викликають небезпеку зміни характеру праці, сверхраціоналізацію і відчуження робочої сили, що несе в собі руйнівну реакцію на людину, потенційну загрозу дегуманізації праці і реальну загрозу техностресса.

Військово-політична сфера життєдіяльності сучасного суспільства відрізняється низьким ступенем захисту інформації про особу людини,

що міститься в державних системах і комп'ютерних мережах. Небезпека контролю над людиною, маніпулювання, поширення конфіденційної інформації ведуть до потенційної загрози інформаційного тоталітаризму. Небезпека інформаційно-технологічної залежності країн послужила грунтом для зародження потенційної загрози інформаційного колоніалізму. Негативним ефектом застосування сучасних технологій у військово-політичній сфері служать відкрилися можливості виробництва нових видів інформаційної зброї.

Коріння інформаційного протиборства лежать глибоко в історії, воно найбільш яскраво проявляється в моменти політичного і військового протистояння. У VI-V століттях до нашої ери давньокитайський полководець Сунь-Цзи виклав ряд інформаційно-інтелектуальних прийомів ведення військових дій, які зберегли свою актуальність сьогодні і стали певним методичним базисом, закладеним в основу сучасної політики і дипломатії. В основі концепції Сунь-Цзи лежить теорія управління ворогом: «його заманюють в пастки вигодою, позбавляють хоробрості, послаблюючи і виснажуючи перед атакою». У XVI столітті італійський мислитель Ніколо Макіавеллі сформулював інформаційно-психологічну концепцію державної влади, де виклав основні принципи впровадження інформаційного протиборства в політичній сфері. Крім того, історія багата прикладами проведення великих інформаційно-пропагандистських акцій, класичних варіантів дезінформації народу глобального масштабу, які відіграли свою фатальну роль.

Найбільш активний розвиток інформаційні експансії і інформаційна зброя отримали на протязі прошлого сторіччя, а особливо в другій половині XX сторіччя, коли особливе місце в прийомах атакуючого впливу набуває інформаційна пропаганда с застосуванням нових

телекомунакаційних технологій та екраних видів мистецтва. Першими в світі лідерами зі створення і застосування інформаційних засобів ураження на той час стають лідери конфліктуючих сторон як часів Другої світової війни, так і «Холодної війни» після закінчення Другої світової війни. СРСР та США - колишні союзники, після перемоги над нацизмом розпочали протистояння двох систем без прямого зіткнення. Локальні конфлікти (вторгнення) в країнах Східної Европи, в Афганістан, підтримка та «опосередована участь» в військових переворотах та конфліктах в інших регіонах, вторгнення в Гренаду, в Панаму, війна в Югославії, бойові дії в районі Перської затоки. Всіці події супроводжувалися відповідним освітленням як в ЗМІ так і в творах масової культури. Після розпаду СРСР масштабні збройні конфлікти з масовим інформаційним впливом розпочалися і на колишній території наддержави – Молдавія, Абхазія, Грузія, Арменія та Азербайджан, Україна. Вже очевидно, що зараз, в XXI сторіччі, пріоритет в озброєнні країн більш спрямований на придбання інформаційної переваги в інфопросторі, ніж на збільшення кількості традиційної авіа- і бронетанкової техніки – головними рушіями війни в XX сторіччі. Хоча події останіх років показали і важливість розвитку звичайних військових технологій. Інформаційно-комп'ютерні системи, комунікаційні технології, соціальні мережі, штучний інтелект разом з традиційними методами пропаганди та контрпропаганди тепер теж основні вражаючі методи і засоби в сучасній війні.

Світовий інформаційний простір майже не має географічних і державних кордонів, в результаті чого його захист і зміцнення залежать одночасно від всього світового співтовариства, рівнозначно як вразливість і шкоди його розвитку відбивається на різних країнах. У

зв'язку з цим, необхідно розглянути питання узгодження стандартів і національних законів, а також завдання співпраці в їх реалізації, прийняття міжнародних договорів щодо функціонування міжнародного інформаційного простору в соціальних, політичних, культурних, юридичних і інших аспектах, розробити адекватні заходи протидії інформаційному протиборства.

На рубежі XX і XI століття людство зробило крок на щабель кардинальних технологічних перетворень, пов'язаних з виникненням нового ряду значних небезпек і загроз. Пройти шлях по висхідній сходах до нової інформаційної цивілізації, заснованої на колосальні можливості технологій, не зірватися вниз, здатне суспільство з високими моральними ідеалами і ясним розумінням усієї глибини відповідальності за кожен свій крок. Сьогодні інформаційні технології, що розглядаються як фактор, який надає величезний вплив на глобальний розвиток соціуму і формування інформаційної реальності, вплинули на свідомість людини і його можливості, змінили життя суспільства, трансформували пріоритети і цінності. Як ці високі технології, будучи засобом здійснення життєдіяльності людини, будуть застосовані в майбутньому, залежить від суспільства і його вибору.

Свого часу засновники концепції інформаційного суспільства справедливо зазначали, що інформація і знання стануть ключовим фактором розвитку, що перевершує за значимістю всі види матеріального виробництва, енергії і послуг. У цій теорії інформаційні технології та телекомунікації представлені основним агентом економічних, соціальних і політичних змін в сучасному світі. Разом з тим, прогнози найближчого майбутнього соціального ладу в порівнянні з нинішніми реаліями виявляються кілька утопічними. Концептуальний аналіз дозволив

виявити відносно невисоку ступінь критичності дослідників до феномену інформаційного суспільства, в силу чого виявлялися слабо врахованими виникають в сучасному соціумі нові види небезпек і загроз.

Таким чином - формування інформаційного суспільства є закономірним етапом еволюції сучасного соціуму. Інформаційне середовище визначає якість функціонування життєдіяльності суспільства. Інформаційні технології вплинули на свідомість людини і можливості, змінили його образ життя. Сучасні інформаційні технології поміняли пріоритети і цінності. Сьогодні використовуються в суспільстві інформаційні технології розглядаються як фактор, який надає величезний вплив на глобальний розвиток соціуму і формування інформаційної реальності.

ТЕМА 2. СТРУКТУРА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ. ІНФОРМАЦІЙНІ ІНТЕРЕСИ ДЕРЖАВИ, СУСПІЛЬСТВА, ОСОБИ

Розглянемо основні поняття, категорії, визначення і терміни.

Інформаційна сфера - область діяльності, що відноситься до ство¬рення, передачі і використання інформації, включаючи особисту і суспільну свідомість, інформаційну і телекомунікаційну інфраструктуру та власне, ін¬формацію. Інформаційна сфера - це частина соціальної діяльності суспільст¬ва, тому в ній проявляються загальні закони буття, загальні і специфічні за¬кономірності соціального розвитку.

Єдиний інформаційний простір країни - це сукупність інформа¬ційних ресурсів та інформаційної інфраструктури, що дозволяє на основі єдиних принципів і за загальними правилами забезпечувати безпечну інфор¬маційну взаємодію держави, організацій і громадян при їх рівнодоступності до відкритих інформаційних ресурсів, а також максимально повне задово¬лення їх інформаційних потреб на всій території держави при збереженні ба¬лансу інтересів на входження у світовий інформаційний простір і забезпе¬чення національного інформаційного суверенітету.

Інформаційні ресурси - інформаційна інфраструктура (апаратура і системи створення, обробки, збереження і передачі інформації), включаючи файли і бази даних та інформацію й інформаційні потоки.

Загроза інформаційній безпеці - це такий стан, коли проявляються наміри або дії, які можуть нанести шкоду інтересам особистості, суспільства та держави в галузі інформації.

Незаконне використання інформаційних і телекомунікаційних систем і інформаційних ресурсів - їх використання без відповідного дозво¬лу або порушення встановлених правил, законодавства чи принципів міжна¬родного права.

Інформаційна інфраструктура включає в себе:

організаційні структури, що забезпечують функціонування і розви¬ток єдиного інформаційного простору (зокрема, збирання, обробку, збере¬ження, поширення, пошук і передачу інформації). Забезпечувальну частину складають науково-методичне, інформаційне, лінгвістичне, технічне, кадро¬ве, фінансове забезпечення;

інформаційно-телекомунікаційні структури (системи) - територіально роз¬поділені державні і корпоративні комп'ютерні мережі, телекомунікаційні ме¬режі і системи спеціального призначення та загального користування, мережі і канали передачі даних, засоби комутації і керування інформаційними пото¬ками;

телекомунікаційні технології;

системи засобів масової інформації.

Інформаційна безпека - захищеність (стан захищеності) основних інтересів особистості, суспільства і держави в сфері інформації, включаючи інформаційну і телекомунікаційну інфраструктуру і власне інформацію та її параметри, такі, як повнота та об'єктивність, доступність і конфіденцій¬ність.

Інформаційна безпека є складовою національної безпеки. Але особли¬вістю інформаційної безпеки є те, що вона, як невід'ємна частина, входить до інших складових національної безпеки: економічної, воєнної, політичної без¬пеки тощо.

На сучасному етапі основними реальними та потенційними загрозами національній безпеці України в інформаційній сфері є:

прояви обмеження свободи слова та доступу громадян до інформації;

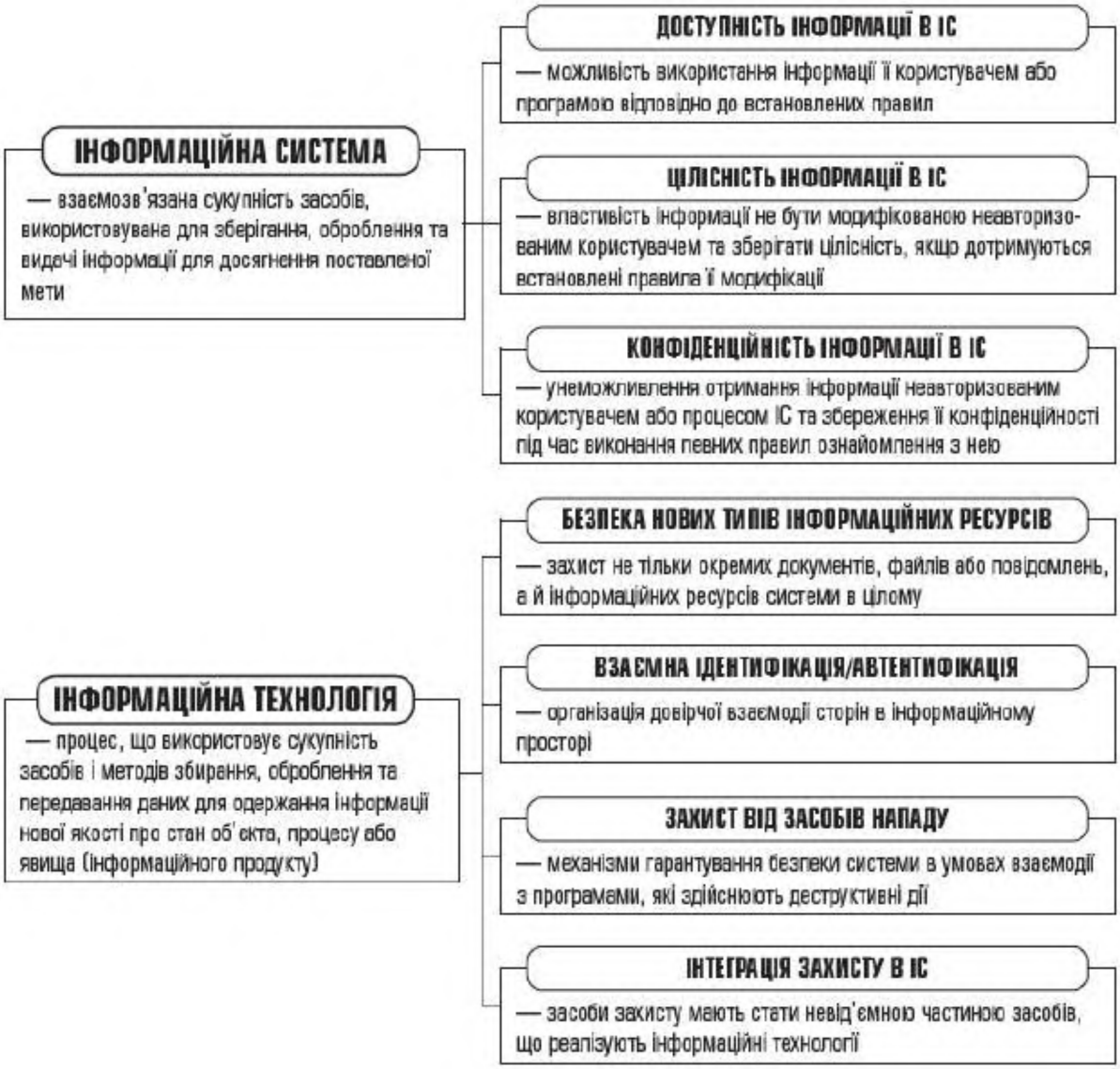
поширення засобами масової інформації культу насильства, жорсто¬кості, порнографії;

комп'ютерна злочинність та комп'ютерний тероризм;

розголошення інформації, яка становить державну та іншу, передба¬чену законом таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;

намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

Додамо, що інші терміни та їх визначення, які безпосередньо відно¬сяться до технічного захисту інформації, надаватимуться у посібнику в про¬цесі надання матеріалу.



. НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

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

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 пра¬вові 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 учас-ників інформаційних відносин, регулює доступ до інформації та забезпечує її охорону, захищає особу та суспільство від неправдивої інформації.

У ст. 1 закону інформація визначається як документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, дер¬жаві та навколишньому природному середовищі.

Державну інформаційну політику розробляють і здійснюють органи державної влади загальної компетенції, а також відповідні органи спеціальної компетенції.

Всі громадяни України, юридичні особи і державні органи мають право на інформацію, що передбачає можливість вільного одержання, використан¬ня, поширення та зберігання відомостей, необхідних їм для реалізації ними своїх прав, свобод і законних інтересів, здійснення завдань і функцій.

Кожному громадянину забезпечується вільний доступ до інформації, яка стосується його особисто, крім випадків, передбачених законами Украї¬ни.

Розділ II закону присвячено інформаційній діяльності, під якою розумі¬ється сукупність дій, спрямованих на задоволення інформаційних потреб громадян, юридичних осіб і держави. Визначено основні напрями та види ін¬формаційної діяльності - одержання, використання, поширення та зберігання інформації.

У розділі III закону наведені галузі, види, джерела інформації та режим доступу до неї. Основними галузями інформації визначені: політична, еконо¬мічна, духовна, науково-технічна, соціальна, екологічна, міжнародна.

Основними видами інформації є: статистична; адміністративна інфор¬мація (дані); масова інформація; інформація про діяльність державних орга¬нів влади та органів місцевого і регіонального самоврядування; правова ін¬формація; 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 здійсню¬ється спеціальними органами, які визначають Верховна Рада України і Кабі¬нет Міністрів України.

Доступ до відкритої інформації забезпечується шляхом: систематичної публікації її в офіційних друкованих виданнях (бюлетенях,

збірниках); по¬ширення її засобами масової комунікації; безпосереднього її надання заінте¬ресованим громадянам, державним органам та юридичним особам.

Обмеження права на одержання відкритої інформації забороняється за¬коном.

Інформація з обмеженим доступом за своїм правовим режимом по¬діляється на конфіденційну і таємну.

Конфіденційна інформація - це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і по¬ширюються за їх бажанням відповідно до передбачених ними умов.

Громадяни, юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру, оде¬ржаною на власні кошти, або такою, яка є предметом їх професійного, діло¬вого, виробничого, банківського, комерційного та іншого інтересу і не порушує передбаченої законом таємниці, самостійно визначають режим дос¬тупу до неї, включаючи належність її до категорії конфіденційної, та встано¬влюють для неї систему (способи) захисту.

Виняток становить інформація комерційного та банківського характе¬ру, а також інформація, правовий режим якої встановлено Верховною Радою України за поданням Кабінету Міністрів України (з питань статистики, еко¬логії, 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,

ко¬мерційна, банківська, професійна, лікарська, адвокатська таємниця тощо), розголошення якої завдає шкоди особі, суспільству і державі.

Інформація, що становить військову таємницю - це вид таємної інфор¬мації, який охоплює відомості в сфері оборони, державної безпеки та охоро¬ни правопорядку, розголошення якої може завдати шкоди інтересам держав¬ної безпеки, бойової готовності Збройних Сил України та інших військових формувань, їхніх окремих підрозділів, якщо ці відомості не належать до дер¬жавної таємниці згідно з законодавством України.

Інформація, що становить комерційну таємницю - це відомості науко¬во-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 осо¬бам, 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 таємни¬ці, та її захист визначається відповідними державними органами за умов до¬держання 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 пе¬реважає право її власника на її захист.

Особливим видом таємної інформації є державна таємниця. Вона охоплює відомості у сфері оборони, економіки, зовнішніх відносин,

держав¬ної безпеки і органів правопорядку, розголошення яких може завдати шкоди життєво важливим інтересам України і які визначені у порядку, встановле¬ному законом, державною таємницею та підлягає охороні з боку держави.

Віднесення інформації до категорії відомостей, що становлять держав¬ну 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 таєм¬ності "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 пра¬ва 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: діяль¬ність органів державної влади; діяльність народних депутатів; діяльність ор¬ганів 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 журна¬лістів 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, релігій¬ної 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 організа¬ціями в галузі інформації.

Міжнародне співробітництво в галузі інформації з питань, що станов¬лять взаємний інтерес, здійснюється на основі міжнародних

договорів, укла¬дених Україною та юридичними особами, які займаються інформаційною ді¬яльністю.

Стаття 53 закону визначає інформаційний суверенітет. Основою інформаційного суверенітету України є національні інформаційні ресурси.

До інформаційних ресурсів України входить вся належна їй інформа¬ція, незалежно від змісту, форм, часу і місця створення. Україна самостійно формує інформаційні ресурси на своїй території і вільно розпоряджається ними, за винятком випадків, передбачених законами і міжнародними догово¬рами.

Інформаційний суверенітет України забезпечується:

виключним правом власності України на інформаційні ресурси, що формуються за рахунок коштів державного бюджету;

створенням національних систем інформації;

встановленням режиму доступу інших держав до інформаційних ре¬сурсів України;

використанням інформаційних ресурсів на основі рівноправного спів¬робітництва з іншими державами.

Узагальнена класифікація інформації у відповідності до Закону України "Про інформацію" надана на рис. 1.2.

Рис. 1.2. Класифікація інформації у відповідності до Закону України «Про інформацію»

В статті 10 Закону України “Про основи національної безпеки України“, визначені основні функції суб’єктів забезпечення національної безпеки України (інформаційна сфера окремо не виділена):

- вироблення і періодичне уточнення Стратегії національної безпеки України і Воєнної доктрини України, доктрин, концепцій, стратегій і про¬грам, планування і здійснення конкретних заходів щодо протидії і нейтралі¬зації загроз національним інтересам України;
- створення нормативно-правової бази, необхідної для ефективного функціонування системи національної безпеки;
- удосконалення її організаційної структури;
- комплексне кадрове, фінансове, матеріальне, технічне, інформаційне та інше забезпечення життєдіяльності складових (структурних елементів) си¬стеми;
- підготовка сил та засобів суб’єктів системи до їх застосування згідно з призначенням;
- постійний моніторинг впливу на національну безпеку процесів, що ві¬дбуваються в політичній, соціальній, економічній, екологічній, науково- технологічній, інформаційній, воєнній та інших сферах, релігійному середо¬вищі, міжетнічних стосунках; прогнозування змін, що відбуваються в них, та потенційних загроз національній безпеці;
- систематичне спостереження за станом і проявами міжнародного та інших видів тероризму;
- прогнозування, виявлення та оцінка можливих загроз, дестабілізую¬чих чинників і конфліктів, причин їх виникнення та наслідків прояву;

- розроблення науково-обгрунтованих пропозицій і рекомендацій щодо прийняття управлінських рішень з метою захисту національних інтересів Ук¬раїни;
- запобігання та усунення впливу загроз і дестабілізуючих чинників на національні інтереси;
- локалізація, деескалація та врегулювання конфліктів і ліквідація їх наслідків або впливу дестабілізуючих чинників;
- оцінка результативності дій щодо забезпечення національної безпеки та визначення витрат на ці цілі;
- участь у двосторонньому і багатосторонньому співробітництві в галу¬зі безпеки, якщо це відповідає національним інтересам України;
- спільне проведення планових та оперативних заходів у рамках міжна¬родних організацій та договорів у галузі безпеки.

Стаття 11 закону визначає загальні повноваження суб'єктів національ¬ної безпеки щодо контролю за здійсненням заходів забезпечення національ¬ної безпеки.

Необхідно відзначити, що цей закон був базовим для прийняття "Кон¬цепції національної безпеки України", схваленої Постановою Верховної Ра¬ди України від 16 січня 1997 року N 3/97-ВР.

Концепція визначала основні засади державної політики в сфері націо¬нальної безпеки України та напрями її подальшого розвитку.

В її розділі III "Загрози національній безпеці України" у ряді загроз на¬ціональній безпеці в інформаційній сфері виділено витік інформації, яка ста¬новить державну та іншу, передбачену законом, таємницю, а також конфіде¬нційної інформації, що є власністю держави.

В розділі IV “Основні напрями державної політики національної без¬пеки України” для усунення цієї загрози запропоновано розробку і впрова¬дження необхідних засобів та режимів отримання, зберігання, поширення і використання суспільно значущої інформації, створення розвиненої інфра¬структури в інформаційній сфері.

В розділі V концепції було сформульовано напрями та заходи для фор¬мування збалансованої державної політики та ефективного проведення ком¬плексу узгоджених заходів щодо захисту національних інтересів у політич¬ній, економічній, соціальній, воєнній, екологічній, науково-технологічній, інформаційній та інших сферах створюється система забезпечення націона¬льної безпеки України.

Визначена система забезпечення національної безпеки - як організова¬на державою сукупність суб'єктів: державних органів, громадських організа¬цій, посадових осіб та окремих громадян, об'єднаних цілями та завданнями щодо захисту національних інтересів, що здійснюють узгоджену діяльність у межах законодавства України.

ТЕМА 3. ЗАГРОЗИ ДЛЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ, СУСПІЛЬСТВА ТА ОСОБИ

ПОНЯТТЯ ІНФОРМАЦІЙНОЇ НЕБЕЗПЕКИ. ВИДИ ІНФОРМАЦІЙНИХ СПОТВОРЕНЬ.

На сьогоднішній день своєчасна та об'єктивна інформація є важливим фактором виробництва, який розглядають, як один з основних ресурсів розвитку суспільства. Сучасні інформаційні системи та технології є засобом підвищення продуктивності та ефективності роботи працівників.

Проте глобальна комп'ютеризація у багатьох сферах управління та виробництва супроводжується появою принципово нових загроз інтересам особистості, підприємства, суспільства, держави.

Паралельно з розвитком і ускладненням засобів, методів, форм автоматизації процесів обробки інформації підвищується залежність суб'єктів підприємництва від ступеню безпеки використовуваних ними інформаційних технологій.

Можна виділити цілу низку джерел загроз інформаційній безпеці сучасного підприємства:

протизаконна діяльність деяких економічних структур у сфері формування, поширення і використання інформації;

порушення встановлених регламентів збору, обробки та передачі інформації;

навмисні дії та ненавмисні помилки персоналу інформаційних систем;

помилки в проектуванні інформаційних систем;

відмова технічних засобів і збої програмного забезпечення в інформаційних і телекомунікаційних системах тощо.

На сьогоднішній день фахівцями досліджується досить широкий перелік загроз безпеці інформаційних систем, які класифікують за рядом ознак (рис.1.)

Захист інформації – галузь науки і техніки, яка динамічно розвивається, пропонує ринку широкий спектр засобів для захисту даних. Проте жоден з них окремо взятий не може гарантувати адекватну безпеку інформаційної системи. Необхідною умовою ефективного захисту є проведення комплексу взаємодоповнюючих заходів.

Комплексне забезпечення інформаційної безпеки автоматизованих систем – це сукупність криптографічних, програмно-апаратних, технічних, правових, організаційних методів і засобів забезпечення захисту інформації при її обробці, зберіганні та передачі з використанням сучасних комп'ютерних технологій.

З липня 2003 р. в Україні введена кримінальна відповідальність за незаконне втручання в роботу комп'ютерів і комп'ютерних мереж, а також за поширення комп'ютерних вірусів, що призвело до спотворення, зникнення, блокування інформації чи її носіїв.

Досвід показує, що практично кожне підприємство має антивірусні засоби захисту, системи ідентифікації користувачів, системи управління доступом до інформаційної системи тощо. Тобто потенціал засобів захисту є, але він не реалізується фірмами повністю. Більше того, володіючи складними апаратними засобами захисту інформації, більшість підприємств навіть наполовину не використовують їх потенціал. Переважна більшість вимог стандартів інформаційної безпеки можуть бути реалізовані наявними у фірм засобами захисту.

Сучасне підприємство повинно вміти належним чином будувати політику інформаційної безпеки, тобто розробляти і ефективно впроваджувати комплекс превентивних заходів по захисту конфіденційних даних та інформаційних процесів. Така політика передбачає відповідні вимоги на адресу персоналу, менеджерів і технічних служб.

Головними етапами побудови політики інформаційної безпеки є:

рішення з боку вищого керівництва щодо необхідності захисту інформації з урахуванням цінності інфоресурсів, потреб та аналізу ризиків, виділення необхідних ресурсів та коштів;

реєстрація всіх ресурсів, які мають бути захищені;

аналіз та створення переліку можливих загроз для кожного ресурсу;

оцінка ймовірності появи кожної загрози;

вжиття заходів, які дозволяють економічно ефективно захистити інформаційну систему.

Більшість фахівців у галузі захисту інформації вважають, що інформаційна безпека підтримується на належному рівні, якщо для всіх інформаційних ресурсів системи підтримується відповідний рівень конфіденційності (неможливості несанкціонованого отримання будь-якої інформації), цілісності (неможливості навмисної або випадкової її модифікації) і доступності (можливості оперативно отримати запитувану інформацію).

Можна виділити такі підсистеми ефективного захисту інформації на підприємстві:

Підсистема антивірусного захисту шлюзів входу в мережу Інтернет, файлових серверів, робочих місць користувачів, централізованого управління, періодичного оновлення антивірусних баз даних.

Підсистема управління контролем доступу та ідентифікацією в інформаційній системі.

Підсистема міжмережного екранування, яка дозволяє реалізувати безпеку міжмережної взаємодії через використання програмних і програмно-апаратних міжмережних екранів.

Підсистема криптографічного захисту, яка гарантує безпеку передачі інформації завдяки шифруванню даних.

Підсистема забезпечення цілісності інформації та програмного середовища шляхом застосування відповідних засобів для фіксації та контролю стану програмного комплексу, управління зберіганням даних для резервного копіювання та архівування.

Підсистема захисту від інсайдерів, яка контролює дії порушників, реалізує інформаційну безпеку при управлінні доступом і реєстрації.

Підсистема захисту систем управління базами даних.

Підсистема виявлення вторгнень і спроб несанкціонованого доступу до інформаційних ресурсів підприємства. Підсистема забезпечує реалізацію захисних заходів з протидії атакам хакерів і поширенню спаму.

Підсистема захисту мобільних пристроїв.

Підсистема моніторингу подій інформаційної безпеки, яка дозволяє своєчасно виявляти загрози інформаційній системі та оперативно реагувати на них.

Сьогодні спеціалізовані фірми пропонують широкий спектр засобів захисту інформаційних систем з урахуванням їх вартості та функціональних можливостей. Найбільш прийнятним підходом при виборі того чи іншого варіанту є дотримання принципу «розумної достатності», суть якого полягає в тому, що визначальними при проектуванні політики інформаційної безпеки повинні бути: розмір підприємства, його ресурсні та фінансові можливості, поточний рівень інформаційної безпеки, стадія функціонування фірми.

Постійна робота в сфері підтримки інформаційної безпеки на належному рівні є необхідною умовою ефективності підприємницької діяльності.

Водночас безпека інформаційної системи має розглядатися як важлива складова загальної безпеки підприємства. Причому необхідна розробка концепції інформаційної безпеки, в якій слід передбачити не тільки заходи, пов’язані з інформаційними технологіями (криптозахист,

програмні засоби адміністрування прав користувачів, їх ідентифікації та автентифікації, брандмауери для захисту входів-виходів мережі тощо), але і відповідні заходи адміністративного та технічного характеру.

Метою захисту інформації має бути збереження цінності інформаційних ресурсів для їх власника. Виходячи з цього, безпосередні заходи захисту спрямовують не так на самі інформаційні ресурси, як на збереження певних технологій їх створення, обробки, зберігання, пошуку та надання користувачам. Ці технології мають враховувати особливості інформації, які роблять її цінною, а також давати змогу користувачам різних категорій ефективно працювати з інформаційними ресурсами.

НАЙБІЛЬШ ПОШИРЕНІ СПОТВОРЕННЯ ІНФОРМАЦІЙНИХ ВІДНОШЕНЬ У РІЗНІ ІСТОРИЧНІ ПЕРІОДИ.

Звісно, що питання належної якості роботи з інформацією постали перед людною та суспільством з моменту виникнення людства, навіть коли ще не існувало соціальних відносин в сучасному розумінні. Дійсно в умовах міжвидової конкуренції виживав та залишав потомство найбільш сильний та гнучкий вид, якій мав змогу пристосовуватись до викликів та змін оточуючого середовища.

З розвитком людства та соціальних відносин до міжвидової конкуренції додалась внутрівидова конкуренція за життєво важливі ресурси – їжу, територію, і таке інше. Звісно – зявилися конфлікти інтересів як індивідумів так і соціальних груп, які супроводжують людство на всіх етапах його розвитку. При цьому одним із важливий ресурсів стає саме інформаційний ресурс, вміле використання якого було

запорукой виживання та перемоги в конкурентній боротьби. Таким чином індивіди та соціальні групи, які були здатні забезпечити цілісність та доступність своїх інформаційних ресурсів для власних потреб та їх недоторканність з боку конкурентів (ворогів) мали більш шансів на виживання та продовження роду. Ті індивидуми, які користувалися для прийняття важливих рішень спотвореною, хібною або неповною інформацією мали менш ансів на виживання. При цьому слід розуміти, що спотворення інформації можливе як за рахунок злого умислу, навмісне, так і за рахунок неповноти «картини миру», не достатку знань, освіти, наявному розвитку системи знань людства взагалі. В другої половини XX століття виникла теорія розвитку особистості та людства - Спіральна динаміка Грейвза, яка являє собою найбільш адекватну модель змін парадигм ммислення людини та суспільства на різних етапах розвитку.

Спроби дослідити як людина працює з інформацією, звісно були з давніх часів.

Одну з перших спроб класифікувати різні різновиди спотворення інформації зробив арабський мислитель Абд-ар-Рахман аль-Джавбарі в своїй книзі "Зірвані покриви". Він класифікує спотворення інформації, виходячи з соціального становища людини.

У роботі описуються хитрощі не тільки реально існуючих людей, а й міфічних істот - ангелів і джинів. Абд-ар-Рахман аль-Джавбарі виділяє певні категорії людей, для яких обман став засобом для існування: цигани, фокусники, уявні каліки і т.д. Недоліком цієї класифікації є той факт, що, по-перше, один і той же спосіб спотворення інформації може бути використаний людьми різних соціальних верств, а по-друге, в цій класифікації були враховані також неіснуючі фігури (джини та ін.).

Ще одну класифікацію спотворення інформації пропонує англійський філософ Френсіс Бекон. У своїй роботі "Новий Органон" він розділив помилки і назвав їх "ідолами". Таких ідолів було кілька.

"Ідоли роду" - це помилки, пов'язані з природою людського розуму.

"Ідоли печери" - це помилки людей, які пов'язані з їх індивідуальним життєвим досвідом.

"Ідоли площі" - це помилки, які засновані на неправильному тлумаченні слів. Оскільки слова часто мають кілька різних значень, партнери по спілкуванню можуть вкладати в них різний зміст. "Ідоли площі" ділилися Беконом на дві групи - імена неіснуючих речей (наприклад, доля) і імена існуючих, але недостатньо чітко визначених речей (наприклад, вологість, хмарність).

"Ідоли театру" - це помилки, що виникають із-за неправильних наукових теорій або помилкових понять.

Сходознавець А. А. Ігнатенко пропонує класифікацію, яку він розробив при вивченні древніх східних трактатів. Автор поділяє спотворення інформації:

- На дезінформацію або обман,
- Амфібол (двозначність висловлювання),
- Підміну (речей, людей),
- Лжесвідчення,
- Порушення клятви,
- Помилкові листи (підроблені і підкидні),
- Обмова,
- Свідомо фальшиві передбачення,
- Удавання,
- Провокації,

- Створення помилкових обставин.

І хоча перераховані фактори актуальні і в сучасному житті, в даній класифікації відсутня єдина підстава оцінки дій спотворюють інформацію.

Ю. В. Щербатих запропонував дві різні класифікації. В одній з них підставою для класифікації є наявність або відсутність вигоди від спотворення інформації. В її основу покладено "прагматичний" підхід, звертається увага на те, хто в основному отримує вигоду з неістинного повідомлення:

• обманювач отримує вигоду за рахунок нанесення шкоди іншій людині;

• обманювач отримує вигоду без нанесення шкоди іншій людині;

• обман без отримання вигоди;

• обман на користь іншої людини;

• ніхто не має вигоди від обману (фантазії).

Ю. В. Щербатих також пропонує ще одну, "полярну" класифікацію обману. В її основу покладено кількість об'єктів комунікації:

• Самообман. Сюди можна включити ілюзії і ситуації, коли людина обманює сам себе, і що може бути формою психологічного захисту.

• Якщо в комунікації беруть участь двоє людей, то причина спотворення інформації може бути в трьох ланках: в тому, хто передає неправдиве повідомлення, в каналі передачі інформації і в тому, хто інформацію неправильно сприймає. Кожен з цих пунктів можна розбити ще на кілька підпунктів. Наприклад, помилки каналу передачі інформації можуть виникнути на вербальному (коли співрозмовник неправильно

розуміє слова) і на невербальному (коли неправильно сприймаються жести) рівнях.

• Груповий обман - одна людина обманює багатьох.

• Масовий - одна група вводить в оману іншу групу людей.

• Двоє людей вводять в оману один одного.

• Взаємний обман, при якому негативні або позитивні емоції спотворюють взаємне сприйняття людей один одним, в результаті чого об'єктивна оцінка стає неможливою.

В сучасної літературі по ЗІ виділяють три види мотивації зловмисника:

Користь, чи зле намагання з метою отримати матеріальну вигоду.

Необачність.

Самореалізацію.

Щодо особливостей роботи людського мозку виділяють наступні особливості, які так чи інакше приводять до спотворення обїективної реальності:

Упущення інформації.

Узагальнення інформації.

Спотворення інформації.

Ці особливості були сформовані в результаті еволюційних процесів. В певних контекстах ці особливості роботи мозку мають позитивні наслідки, в певних – негативні, але пересічна людина самостіно дуже рідко може усвідомлювати ці прояви. Основним завданням освіти та

розвитку особистості з метою підвищення ефективноті стає саме в тому, щоб формувати навик ефективного мислення, коли ці три особливості не впливають істотно на прийняття важливих рішень. Також слід зазначити загально відомий факт, що підвищена емоційність під час прийняття рішень також приводить до підвищення вірогідності прийняття неефективного рішення, що виражається в низці поговорок та прислив'ях.

Цікаву класифікацію спотворення інформації пропонує також В. В. Костиков:

• Ідеологічний обман - це самий фатальний вигляд, який призводить до найбільш катастрофічних наслідків.

• Передвиборний обман, коли на людей вихлюпується все те, що накопичилося з правди, брехні, напівправди.

• Імітація соціальної політики, коли люди роблять вигляд, що вони щось роблять, а фактично життєвий рівень парода або погіршується, або стоїть на місці. Це дуже небезпечна форма обману, яку ми спостерігаємо зараз в нинішній політиці кабінету міністрів. Хоча, безумовно, кожен може на своєму робочому місці не робити нічого.

• Замовчування правди - дуже благородний вид обману.

• Блеф - досить поширений вид обману, особливо в зовнішній політиці. Це те, що зараз робить Північна Корея, погрожуючи своїм ідеологічним противникам ядерним ударом - типовий приклад такого блефу. Хоча насправді це просто демонстрація, яка створює вогнище напруженості в регіоні.

• Обман, яким займаються спецслужби - це особливий, найбільш прихований вид обману. Вони часто обманюють навіть власні уряди.

• І ще два типи обману, які між собою пов'язані - дипломатичний і зовнішньополітичний, коли посли обманюють свого міністра.

Така точка зору па спотворення інформації у владних структурах людини, який має досвід роботи в ситуаціях нещирого ділового спілкування. І хоча ця класифікація розглядає спотворення інформації тільки через призму політики, проте, вона представляє безперечний інтерес для більш глибокого розуміння даного феномена.

Ще один варіант класифікації пропонує Р. Р. Гарифуллин. Він виділяє блеф (обман, введення в оману) як дезінформацію, при якій на основі спотворення інформації когось переконують в тому, що щось бажане, але не існуюче існує. Таким чином, блеф є штучною помилкою.

Найбільш ефективним прийомом блефування Р. Р. Гарифуллин вважає прийоми напівблефу (напівправди або напівбрехні), які засновані на хитрощі і умінні скористатися дурістю інших. Р. Р. Гарифуллин виділяє сім прийомів напівблефу.

1. За замовчуванням (або передача неповної інформації), в результаті якої реципієнт робить помилку.

2. Фальсифікація (підтасовування) - це передача свідомо помилкової інформації по суті розглянутого питання (лжесвідчення, фальшиві заяви і спростування, фабрикація фактів тощо.).

3. Дезорієнтація (заміщення) - передача не має відношення до справи істинної інформації з метою відвернути увагу від суті питання, що розглядається.

4. Марнослів'я (словоблуддя) - трансляція одночасно і істинної, і неправдивої інформації, яка не належить до суті питання.

5. Маскування - спроба приховати якусь істотну інформацію за допомогою різної несуттєвою інформації. Виділяють чотири варіанти:

• маскування істотної брехні несуттєвою брехнею;

• маскування істотної істини несуттєвою брехнею;

• маскування істотної брехні несуттєвою істиною;

• маскування істотної істини за допомогою несуттєвою істини.

6. Напівправда - це змішання істотної правдивої інформації з істотною помилковою інформацією:

• ірраціональна напівправда - це будь-який хаотичне змішування правдивої і неправдивої інформації;

• раціональна напівправда - логічно впорядковане з'єднання правди і брехні на основі тієї чи іншої раціональної помилки. Це може бути підміна понять, перекручення сенсу сказаного, тенденційне тлумачення тексту;

• діалектична напівправда - це впорядкована з'єднання істини і брехні, коли сам факт з'єднання визнається в якості цілком допустимого "діалектичного" протиріччя.

7. Переформалізація - в процесі формалізації знань вносяться свідомі спотворення, наприклад, при перекладі з однієї мови на іншу; багаторазовий повтор інформації (відповідно до принципу "істина є багато разів повторена брехня"), чергування різних видів інформації (використовується для зниження рівня критичності мислення, відволікання уваги).

Однак необхідно відзначити, що в даній класифікації показані способи спотворення інформації, але не дані підстави, за яким вона проводиться, не враховується ставлення самої людини до спотворення інформації і ступінь його зацікавленості в даній дії.

Російський філософ Д. І. Дубровський в своїй класифікації виділяє:

- Навмисний обман (корисливий або безкорисливий, тобто продиктований міркуваннями боргу, тактовності або викликаний примусом, шантажем) і ненавмисні;

- Зловмисний і доброчесний;

- Напівправда;

- Самообман.

Г. В. Грачов та Н. К. Мельник пропонують для визначення брехні і обману в негативному аспекті такі компоненти:

- Навмисність (свідомість) дії;

- Спотворення реальності (дійсності, фактів, інформації);

- Соціально не схвалювану, неблагородну, перш за все корисливу мету, в результаті досягнення якої набувається перевага однією людиною або групою осіб над іншою людиною або групою осіб, яким завдається шкода.

Хоча далі вони відзначають, що виділення в якості критерію оцінки соціальної схвалюваності (неодобряемості) цілей суб'єкта, який вдається до спотворення інформації як формі поведінки, є досить уразливим

Американський вчений П. Екман поділяє спотворення інформації на дві основні форми - замовчування і спотворення. При замовчуванні правдива інформація приховується, але не повідомляється помилкова. При спотворенні (фальсифікації) не тільки ховається правда, по і представляється натомість помилкова інформація.

Найбільш змістовний аналіз даної категорії було проведено в роботах В. В. Знакова. Проведений аналіз існуючих понять і визначень дозволив структурувати і узагальнити поняття, що входять в категорію "спотворення інформації". І хоча в даній класифікації не відображені

різні наміри суб'єкта, такі як досягнення корисливих цілей або ж справедливості, щоб уникнути власного покарання або захист іншої людини, тим не менш, дана класифікація представлена найповніше висвітлює позиції спотворює інформацію суб'єкта.

Так, В. В. Знаків пропонує характеризувати відмінності за трьома основними ознаками:

- Фактична істинність або хибність твердження;
- Віра говорить в істинність або хибність твердження
- Наявність або відсутність у мовця наміру ввести в оману слухача.

.

ТЕМА 4. ПРИНЦИПИ ПОБУДОВИ ДЕРЖАВНОЇ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ. ІНФОРМАЦІЙНА ВЗАЄМОДІЯ РІЗНИХ ГІЛОК ВЛАДИ, СУСПІЛЬСТВА, ГРОМАДЯН.

Сьогодні державна інформаційна політика спрямована на розбудову якісно нового вітчизняного інформаційного суспільства, що є запорукою політичного і соціально-економічного руху України вперед, зміцнення її статусу, як незалежної держави. Значну кількість питань, пов'язаних із розвитком інформаційного суспільства, досі не врегульовано на законодавчому рівні. Це стосується, зокрема, проблем інфраструктури, діяльності ЗМІ, інформаційно-аналітичних установ тощо. Суттєвим недоліком чинного інформаційного законодавства є те, що воно носить надто загальний характер, не визначає способи врегулювання проблем, що виникають під час використання інформаційного простору. Також залишається недосконалим понятійний апарат, що значно ускладнює реалізацію завдань та взаємодію суб'єктів інформаційної сфери. Ця ситуація веде до частого уточнення та зміни законів шляхом введення попревок та розробки інших подзаконих актів.

В Україні ще недосконале правове регулювання функціонування міжнародних інформаційних систем, однією з яких є мережа Інтернет. Продовжує зберігатися неповнота правового регулювання питань інформаційної безпеки, що, в свою чергу, породжує нові виклики і загрози національній безпеці України. Особливо ситуація загострюється під час міжнародного інформаційного обміну через глобальні соціальні мережі, що посилює вплив електронних і друкованих ЗМІ на соціально-політичне та культурне життя країни, моральний стан суспільства тощо.

В рамках державної інформаційної політики важливо зосередитись на формуванні в середовищі користувачів таких загальнообов'язкових норм поведінки, як інформаційна культура та відповідальне ставлення до використання інформаційного простору. Реалізація цих завдань передбачає удосконалення системи управління всіма видами інформаційних ресурсів та інформаційно-телекомунікаційною інфраструктурою, надання державної підтримки процесу формування ринку інформаційних технологій, засобів та продукції. Подальшого удосконалення потребують форми і напрями співпраці держави з електронними і друкованими мас-медіа.

Метою державної інформаційної політики має стати побудова в країні демократичного інформаційного суспільства, інтегрованого у світове інформаційне співтовариство. Для реалізації цього завдання необхідно сконцентрувати зусилля на формуванні необхідних умов і механізмів, спрямованих на створення, розвиток й забезпечення ефективного використання інформаційних ресурсів у всіх сферах діяльності. В числі пріоритетних завдань державної інформаційної політики має бути створення сприятливих умов для формування, розвитку, модернізації і використання національних інформаційних ресурсів, інформаційно-телекомунікаційної інфраструктури та технологій. Цьому має передувати детальний аналіз наявної нормативно-правової бази та визначення шляхів і напрямів її удосконалення з урахуванням сучасних реалій. Необхідно окреслити основні засади і механізми проведення обліку інформаційних ресурсів, створених за рахунок держбюджету, та критерії для об'єктивної оцінки їх якості й можливостей. Також слід подбати про реформування інформаційного забезпечення в системі органів державної влади. Інформаційна політика

держави повинна сприяти розвитку вітчизняного ринку інформаційних і телекомунікаційних систем та технологій, орієнтованих на роботу у внутрішніх комп'ютерних мережах. Для цього необхідно удосконалити механізми та віднайти ресурси щодо забезпечення державної підтримки перспективних вітчизняних досліджень, спрямованих на створення власних інформаційних і телекомунікаційних систем та технологій. Особливої уваги потребує удосконалення практики визначення перспективних наукових розробок з метою їх подальшого фінансування з бюджету та забезпечення мінімального впливу людського фактору на прийняття таких рішень.

Необхідно забезпечувати вільний обіг інформації та конституційне право громадян на її пошук, отримання, виробництво і розповсюдження. На особливу увагу заслуговує розвиток співпраці держави з мас-медіа, оскільки ЗМІ найчастіше є первинними джерелами інформації і виконують роль важливої соціальної інституції в реалізації державної інформаційної політики. Існує нагальна потреба в розробці правових, економічних і організаційних механізмів для забезпечення в діяльності ЗМІ балансу інтересів особистості та держави, недопущення їх монополізації, сприяння ефективному виконанню функції об'єктивного і неупередженого інформування суспільства про події внутрішнього та міжнародного життя. Також потребують регулювання проблеми, пов'язані з доступом до інформації журналістів, правовою охороною особистої таємниці в ЗМІ, захистом громадян і суспільства від недостовірної і недобросовісної інформації. В процесі формування та вдосконалення інформаційної політики держави необхідно на законодавчому рівні унеможливити підпорядкування ЗМІ будь-яким кон'юнктурним інтересам, вжити заходів щодо недопущення спроб

вчинення на них тиску, а також спроб надання суб'єктами інформаційних відносин для мас-медіа неповної, викривленої або недостовірної інформації. Варто зазначити, що все більшої актуальності набуває проблема визначення в державній інформаційній політиці засад протидії зовнішньому впливу на внутрішньополітичну ситуацію в Україні.

Держава в процесі реалізації своїх функцій із забезпечення інформаційно- психологічної безпеки громадян України повинна:

– організовувати і проводити об'єктивний та всебічний аналіз і прогнозування загроз інформаційно-психологічної безпеки України, розробляти заходи та механізми забезпечення інформаційно-психологічної безпеки громадян України;

– організовувати роботу органів державної влади щодо реалізації комплексу заходів, спрямованих на запобігання, парирування і нейтралізацію загроз інформаційно-психологічної безпеки України, локалізації та ліквідації наслідків їх прояву;

– організовувати взаємодію органів законодавчої та виконавчої влади з громадськими організаціями та громадянами в процесі виявлення загроз інформаційно-психологічної безпеки громадян України і визначення правових механізмів протидії цим загрозам;

– підтримувати законну діяльність громадських об'єднань у галузі протидії загрозам інформаційно-психологічної безпеки громадян України, а також забезпечення в встановлюваних законодавством рамках громадського та державного контролю діяльності засобів масової інформації;

– організовувати розробку вимог з безпеки сучасних інформаційних технологій для психічного здоров'я громадян та інформувати про них суспільство;

– здійснювати контроль діяльності органів державної влади щодо реалізації державної політики забезпечення інформаційно-психологічної безпеки України;

– здійснювати необхідну протекціоністську політику щодо організацій, що беруть участь у формуванні відкритих інформаційних ресурсів загального користування та надають інформаційні послуги російським громадянам на основі цих ресурсів;

– забезпечувати захист психіки дітей та молоді від впливу інформації, здатної завдати шкоди їх психічному здоров'ю;

– забороняти протиправну діяльність громадських організацій і релігійних об'єднань, що завдає шкоди психічному здоров'ю людини і суспільства.

Активний розвиток інформаційного суспільства породжує величезну потребу громадян в інформації. Необхідність задоволення цієї потреби і обумовлює особливу роль засобів масової інформації (ЗМІ) в житті суспільства. При цьому повною мірою проявляються такі властивості ЗМІ як масовість, періодичність, використання постійно поповнюваних інформаційних ресурсів, виконання ЗМІ функцій первинних джерел інформації, застосування сучасних інформаційних технологій і засобів телекомунікацій. ЗМІ є дієвим каналом інформування суспільства про діяльність влади і інформування влади і суспільства про життя суспільства і його реакції на дію влади. Ці особливості роблять ЗМІ найважливішим соціальним інститутом і необхідним об'єктом державної інформаційної політики. Сучасні ЗМІ не лише оперативно представляють світові події, але значною мірою займаються аналізом інформації, її попередньою фільтрацією та цілеспрямованим відбором. Саме тому належний розвиток ЗМІ може бути забезпечений тільки в рамках

державної інформаційної політики, орієнтованої на демократичний розвиток українського суспільства і держави. Основними напрямами державної інформаційної політики, що реалізовують вказаний шлях розвитку, мають бути:

– недопущення підпорядкування ЗМІ кон'юнктурним інтересам влади і бізнесу (унеможливлення прямого тиску, передачі засобам масової інформації неповної, невизначеної, спотвореної або неправдивої інформації, відвертої дезінформації тощо);

– регулювання рівня концентрації і монополізації ЗМІ (перешкоджання зменшення незалежних джерел інформації, зосередження ЗМІ в руках представників економічної еліти, безправ'я журналістів тощо);

– сприяння розвитку регіональних та місцевих ЗМІ;

– удосконалення національного законодавства в частині гарантій свободи слова і інформації, вільного поширення масової інформації, забезпечення плюралізму ЗМІ, доступу до офіційної інформації.

Щодо установлення та попередження загроз у сфері інформаційної безпеки виділимо три основні завдання:

1) створення державної системи забезпечення інформаційної безпеки;

2) забезпечення інформаційно-психологічної безпеки громадян України;

3) налагодження міжнародного співробітництва з питань інформаційної безпеки.

Створення державної системи забезпечення інформаційної безпеки. Відзначимо, що проблеми забезпечення безпеки в інформаційній сфері носять як концептуальний, так і практичний характер. З практичної точки

зору, в Україні повинна бути створена система забезпечення інформаційної безпеки, якою необхідно ефективно управляти. Сьогодні ж в Україні існує конгломерат окремих відомчих систем, які вирішують окремі завдання захисту інформації в системах і мережах тільки в межах своєї компетенції і в своїх відомчих інтересах. Отже, необхідне узгодження зусиль всіх підсистем та координація їх діяльності.

Також підкреслимо, що в сучасних умовах підтримання необхідного рівня інформаційної безпеки вимагає постійного відстеження політичних, соціальних, економічних, науково-технічних та інших змін як за кордоном, так і всередині країни. Ці зміни можуть породжувати нові інформаційні загрози. Тому система забезпечення інформаційної безпеки повинна швидко реагувати на ці зміни і перманентно перевіряти можливості відображення реальних або потенційних загроз. Створення такої системи дозволить:

– суттєво покращити підготовку та прийняття рішень на державному, регіональному та місцевому рівнях за рахунок використання системи повних, достовірних і доступних баз даних по всіх об'єктах управління, а також розвитку інтелектуальних інформаційних систем;

– забезпечити реалізацію всіх базових функцій стратегічного і поточного управління (аналіз і прогноз ситуацій, обмін інформацією, планування та координація діяльності, контроль за виконанням прийнятих рішень тощо);

– розробити систему моніторингу надзвичайних ситуацій (природних, техногенних та антропогенних катастроф і аварій), а також ризикованих соціально-політичних ситуацій, і побудувати систему швидкого реагування на такі ситуації;

– швидше реагувати на зовнішні негативні інформаційні впливи.

ТЕМА 5. КЛАСИФІКАЦІЯ ІНФОРМАЦІЙНИХ РЕСУРСІВ ПО ВИДАМ ВЛАСНОСТІ ТА ТИПАМ ДОСТУПУ.

Якщо подивитися на поняття інформації або інформаційних ресурсів у самому широкому тлумаченні цих термінів, їх можна охарактеризувати як якісь відомості про навколишній світ, процеси, що відбуваються в ньому, людей, предмети, події, явища, факти і т. п., незалежно від форми подання, одержувані людиною з подальшим відображенням у своїй свідомості.

Виходячи з цього, інформаційними ресурсами прийнято вважати масиви документів або окремо взяті документи, які зберігаються у відповідних системах (банки даних, інтернет, бібліотеки, фонди, архіви, канали зв'язку та ін). Класифікація інформаційних ресурсів проводиться із застосуванням деяких основних критеріїв або ознак, що дозволяють розділити ІР на кілька великих класів, і насамперед, за ступенем доступності: відкриті (публічні), закриті (з обмеженим доступом), особиста інформація. Але тільки цими критеріями поділ ІР на основні типи не обмежується.

Види інформаційних ресурсів та їх класифікація

У більш розширеному варіанті поділ на групи може здійснюватися з урахуванням додаткових критеріїв. І в першу чергу тут потрібно відзначити, що на сучасному етапі розвитку суспільства поняття інформації, або ІР, нерозривно пов'язане з документуванням (це так звана документована інформація). Мається на увазі, що дані будь-якого типу

фіксуються або зберігаються на певному типі носія (друковані, комп'ютерні носії, сервери, канали зв'язку тощо).

Крім того, окремо застосовуються такі параметри для класифікації інформаційних ресурсів, як поділ їх на стаціонарні і пересувні.

Основні напрями в класифікації ІР

Якщо говорити про основні напрямки в поділі ІР на класи за якимись критеріями, можна зустріти досить багато різних уявлень. Однак серед всіх тих ознак, за якими проводиться класифікація інформаційних ресурсів, можна виділити найосновніші:

за джерелом створення;

за ступенем доступу;

за цільовим призначенням;

за способом подання та виду носія;

за формою власності;

за методом організації та зберігання;

за змістом;

за мовною і національно-територіальною або географічною ознакою;

за рівнем компетенції і т. д.

Самим великим класом серед всіх є ознака змісту.

Розглянемо інші розділи. Серед джерел створення ІР розрізняють первинні і вторинні. Сюди ж відноситься поділ на правову і неправову (недокументовану) інформацію, яка залишається поза полем регулювання з точки зору юридичних норм.

В поділі на основі доступу це може бути публічна або приватна інформація з обмеженим доступом (наприклад, державна, службова,

комерційна таємниця або особисті дані). В цільовому призначенні найчастіше виділяють наступні інформаційні ресурси:

особисті;

корпоративні;

бізнес-ресурси;

ЗМІ;

політичні;

освітні;

культурні;

ресурси організацій і установ;

послуги і сервіси;

розваги;

спорт;

відпочинок;

дошки оголошень;

зберігання і мультимедіа і т. д.

Класифікація інформаційних ресурсів за способом подання.

Як правило, сюди включаються поняття твердих копій (книги, газети, журнали машинопечатние документи), магнітні та електронні (цифрові) носії (аудіо - і відеозапису, фото - і кіноплівка, компакт-диски, знімні пристрої пам'яті, жорсткі диски комп'ютерів) та засоби зв'язку (радіо, телебачення, мережі).

Серед форм власності виділяються приватна (особиста, корпоративна), державна і спільна (колективна), національне надбання. У сенсі організації і зберігання класифікація інформаційних ресурсів частково пов'язана з типами носіїв (друковані видання та цифрові носії), а також передбачає поняття бібліотек, фондів, архівів, баз даних, масивів

документів і автоматизованих форм. З національно-територіальною приналежністю, здається, все зрозуміло, а ось в плані ступеня компетенції поділ проводиться за ознакою орієнтування на масового або професійного користувача.

Типи суб'єктів у понятті ІР

Що стосується суб'єктів ІР, тут є три основних типи:

громадяни держав або особи без громадянства;

організації;

органи влади держави будь-якого рівня.

Класифікація за змістом

Розглянемо найбільший розділ розподілу ІР - за змістом - як приклад класифікації інформаційних ресурсів за заданим критерієм. В загальному випадку вона включає в себе наступні великі групи:

тематичні та наукові публікації;

довідкова інформація;

реклама;

новини;

бібліографічні публікації.Якщо подивитися на ці аспекти дещо ширше, в якості прикладу можна навести ще один поділ:

ділова інформація (економіка, фінанси, комерція, бізнес, статистика);

соціально-політична і юридична інформація;

науково-технічна інформація;

споживча та інша масова інформація;

електронні угоди;

обчислювальна техніка та комунікації.

Головні типи електронної інформації

Класифікація інформаційних ресурсів (інформатика прямо на це вказує) у самому загальному випадку передбачає два основних типи IP за критерієм режиму використання:

онлайн – безпосередній доступ до документів на серверах мережі;

офлайн – використання документів, баз даних або їх фрагментів у вигляді копій первинної інформації з сервера, що зберігається на електронному носії.В деякому сенсі класифікація електронної інформації дещо схожа на поділ за змістом, однак додатково тут присутній поділ ринку програмного забезпечення:

комерційне;

вільно розповсюджуване ПЗ (безкоштовний), включаючи продукти з відкритим вихідним кодом (ліцензія GNU GPL);

умовно-безкоштовне програмне забезпечення (shareware).В якості ще одного доповнення деякі джерела вказують сектор інформаційних послуг і обслуговування.

Поняття електронного документа

Під документом такого типу в більшості випадків розуміють документовану інформацію, представлену в електронному вигляді, для сприйняття якої використовуються електронно-обчислювальні системи, а для передачі – комунікаційні та мережеві інструменти.

Інформація такого типу може бути представлена у вигляді окремих файлів, баз даних і масивів або автоматизованих систем. Крім того, особливе значення має юридичний аспект правомірного використання тих чи інших документів, сертифікація та атестація систем, а також захист інформації будь-якого рівня доступу та виду.

Класифікація інформації в інтернеті

Класифікація електронних інформаційних ресурсів була б абсолютно неповною, якщо б не порушувалися питання інтернету, оскільки сьогодні більшість електронних документів доступно саме там. Тут представлено кілька основних критеріїв:

форма подання (веб-сторінки, інформаційні і файлові сервери, бази даних, телеконференції);

мовний і територіальна ознака;

зміст і т. д.

Типи інтернет-ресурсів

Види та класифікація інформаційних освітніх ресурсів у навчальному процесі розглядаються досить докладно. Проте можна навести і деякі доповнення, включивши в розподіл ІР поняття додаткових типів інтернет-ресурсів.

Як правило, серед критеріїв виділяють наступні:

повнота і функціональний зміст;

принцип взаємодії з користувачем (інформативне, інтерактивне);

ступінь доступності.

У змістовній частині сайти розподіляють на візитки (лаконічні сторінки з основною інформацією), блоги (персональні сторінки), промоушн-сайти (реклама товарів і послуг), електронні магазини і сервіси, інформаційні сайти з певною тематикою, веб-портали (великі ресурси або інтернет-спільноти), корпоративні представництва (системи автоматизації діяльності компаній), системи управління підприємствами, інтегровані в інтернет і інтранет (зовнішні та внутрішні мережі). При взаємодії з користувачем можна виділити такі типи ІР, як інформаційні (мережеві видання, ЗМІ, телебачення, радіо), прикладні (онлайн-бібліотеки і бази даних, сховища з можливістю скачування, пошукові

системи), безпосередньо-комунікаційні (соціальні мережі, інтернет-спільноти), розважальні (ігри, музика, відео, анекдоти і т. д.), комерційні (сайти з платними послугами та інтернет-магазини), презентаційні ІР рекламного характеру. Якщо говорити про ступінь доступності, цей критерій дозволяє розділити ІР на публічні (відкриті всім користувачам без винятку), внутрішньомережеві (доступ мають тільки співробітники будь-якої організації всередині мережі інтранет), екстра-мережеві (розміщуються в інтернеті, але має доступ обмежене коло користувачів).

Інформаційні послуги

Нарешті, окремо варто сказати про інформаційні послуги. У першу чергу в цій категорії виділяють сервіси з пошуку і обробці інформації, видачу за запитом документів будь-якого типу і зберігання інформації. Другим за значимістю розділом є надання послуг з використання інтернету, БД та АІС, за доступу до інтернету або мереж і передачі інформації, а також по використанню електронної пошти та надання хостингу (формування особистих сторінок).

Захист ІР

І, само собою зрозуміло, будь-які ІР повинні захищатися на найвищому рівні, причому абсолютно без різниці, до якого типу вони належать, незалежно від носія, на якому вони зберігаються.

Крім того, під захистом можна розуміти і юридичний аспект (авторське право, законодавство, ліцензування, атестація), і програмні засоби у вигляді антивірусів або міжмережевих екранів (файрволів – програмних або "залізних"), криптографічних технологій шифрування даних або з'єднання і таке інше.

ТЕМА 6. КІБЕРПРОСТІР І КІБЕРБЕЗПЕКА — ГОЛОВНІ ОЗНАКИ НОВОЇ ІНФОРМАЦІЙНОЇ ЦИВІЛІЗАЦІЇ. ЗАХОДИ УКРАЇНИ ІЗ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ НАЦІОНАЛЬНОЇ ІНФОСФЕРИ ТА ПРОТИДІЇ ПРОЯВАМ КІБЕРЗЛОЧИННОСТІ

Процеси формування та розвитку сучасного інформаційного суспільства, факт створення якого офіційно визнали представники держав Великої вісімки в ході Окінавської зустрічі в липні 2000 року, базуються, як відомо, на синтезі двох технологій — комп'ютерної і телекомунікаційної. Ці процеси підпорядковуються двом простим, але дуже змістовним законам. **Перший закон** сформулював один із засновників корпорації Intel Гордон Мур: Кількість транзисторів у процесорах збільшуватиметься вдвічі протягом кожних півтора року. Цей закон фактично пояснює виникнення нових, специфічних за формою і способами функціонування суб'єктів та об'єктів інформаційної інфраструктури, гарантоване зростання швидкості обчислень і обсягів оброблюваної інформації, а також формування на рубежі тисячоліть інформаційного простору — глобального інформаційного середовища, яке в реальному масштабі часу забезпечує комплексну обробку відомостей про протиборчі сторони та їх навколишнє оточення з метою підтримання ухвалюваних рішень щодо створення оптимального задля досягнення поставлених цілей складу сил і засобів та їх ефективного застосування в різних умовах навколишньої обстановки.

Другий закон належить Роберту Меткалфу — винахідникові мережі Інтернет: Цінність мережі перебуває у квадратичній залежності від кількості вузлів, що входять до її складу. Отже, цей закон констатує, що основу сучасного інформаційного суспільства становлять мережі різного функціонального призначення, сукупність і взаємозв'язок яких, власне, і створюють інформаційний простір, а також новітні інформаційно-телекомунікаційні (ІТ) технології, які останнім часом:

1) стали важливою складовою суспільного розвитку та розвитку світової економіки в цілому, змінивши значною мірою механізми функціонування багатьох суспільних інститутів та інститутів державної влади;

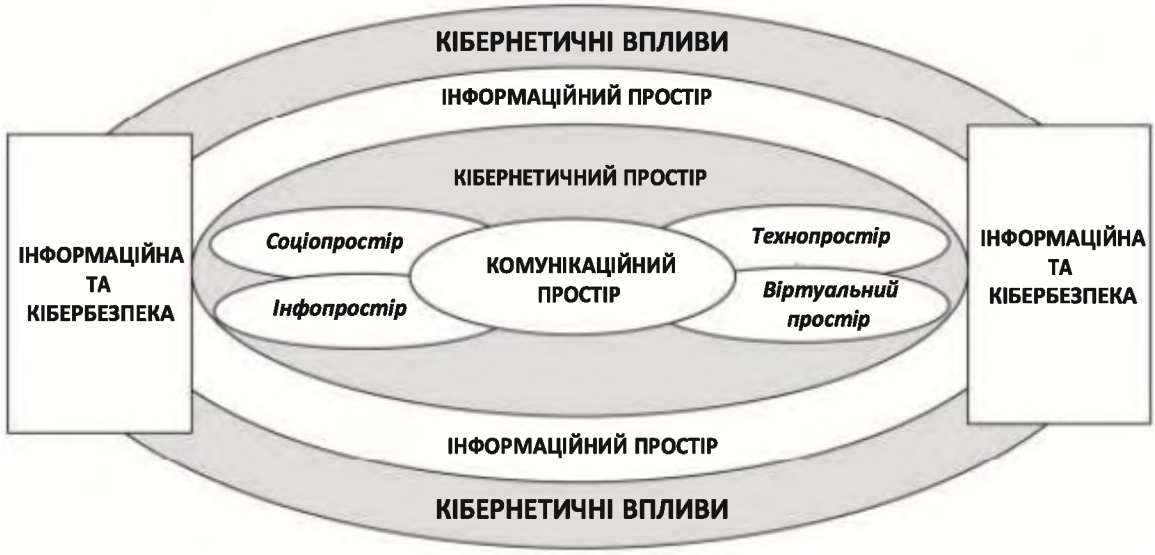
2) увійшли до групи найбільш істотних факторів, що впливають на формування сучасного високоорганізованого інформаційного середовища й дають змогу на якісно новому рівні інформаційного обслуговування як у віртуальному, так і в реальному просторі вести повсякденну оперативну роботу, здійснювати аналіз стану і перспектив діяльності інформаційно-аналітичних підрозділів, а також добувати вихідні дані, необхідні для ухвалення раціональних і науково-обґрунтованих управлінських рішень.

Поступове й доволі умовне поєднання віртуального і реального просторів за допомогою ІТ-систем (ІТС) і мережних технологій різного функціонального призначення, які в процесах обробки, передавання та зберігання інформа- ції використовують електромагнітний спектр і діють як єдине ціле, а також відповідного програмного забезпечення (ПЗ) призвело, зрештою, до форму- вання кіберпростору (КбП) — високорозвиненої моделі об'єктив- ної 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.



. Взаємозв'язок інформаційного та кіберпросторів

Уперше термін «кіберпростір» було використано у згаданій раніше Окінавській хартії глобального інформаційного суспільства та 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.

Наприклад:

відповідно до міжнародного стандарту, кіберпростір — це середовище існування, що виникло в результаті взаємодії людей, програмного забезпечення і послуг в інтернеті за допомогою технологічних пристроїв і мереж, під'єднаних до них, якого не існує в будь-якій фізичній формі;

відповідно до нормативної бази США, кіберпростір — це сфера, що характеризується можливістю використання електронних та електромагнітних засобів для запам'ятовування, модифікування та обміну даними через мережні системи та пов'язану з ними фізичну інфраструктуру;

відповідно до офіційних документів Євросоюзу, кіберпрострір — це віртуальний простір, в якому циркулюють електронні дані світових персональних комп'ютерів (ПК);

відповідно до офіційних документів Великобританії, кіберпростір — це всі форми мережної, цифрової активності, що включають у себе контент та дії, здійснювані через цифрові мережі;

відповідно до офіційних документів Німеччини, кіберпростір — це вся інформаційна інфраструктура, доступна через інтернет поза будь-якими територіальними кордонами.

Серед інших варто також відзначити й такі визначення поняття КбП:

поліморфний віртуальний простір, що генерує інформаційна система(ІС) 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 — електронними обчислювальними машинами, 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 і 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.

Як випливає зі щойно викладеного, 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 незлічених 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 (АСУ) протилежної сторони, систем управління її транспортом і енергетикою, економікою й фінансовою системою тощо (поряд із наземною, морською й повітряно-космічною сферами) і своєрідної сполученої 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;

схарактеризувати злочини, втручання і загрози, пов'язані з особливостями існування та передавання інформації;

визначитись із можливими його дійовими особами;

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.

Дійові особи кіберпростору та їхній вплив на інфо- та кібербезпеку

Важливість кіберпростору підтверджується появою концепцій ведення боротьби в ньому та створенням у складі збройних сил багатьох країн світу спеціальних структур на зразок:

• об'єднаного Кіберкомандування (U. S. Cyber Command-USCYBERCOM) та спеціалізованого кібернетичного розвідувального центру у США;

• Управління мережних операцій у Німеччині;

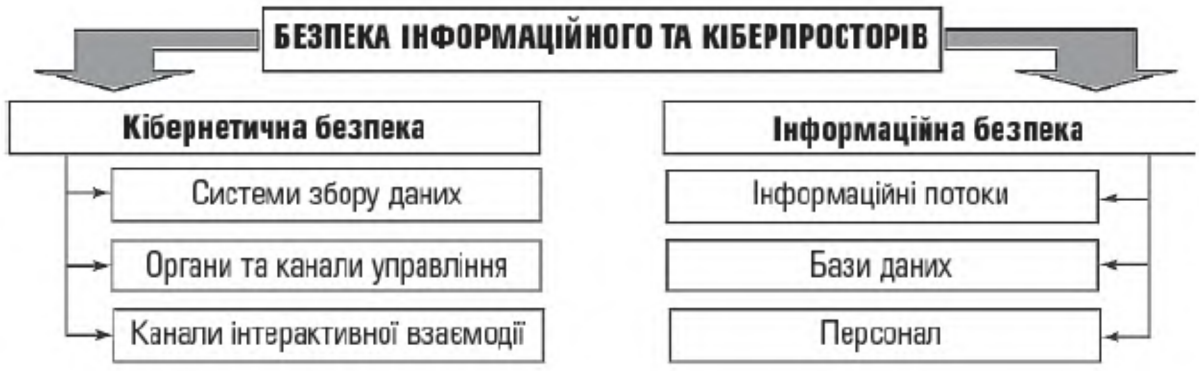
• Центрального управління з кібербезпеки, Оперативного центру забезпечення кібербезпеки (CSOC) та Центру державного зв'язку (GCHQ) у Великобританії;

• Центру інформаційних систем Служби безпеки (CISSS) та Національного агентства безпеки інформаційних систем (ANSSI) у Франції;

• спеціалізованого центру захисту національного кіберпростору Tehila в Ізраїлі;

• кіберпідрозділів у складі Федеральної служби безпеки Росії (негативні наслідки роботи якого на протязі останіх років ми бачимо зараз).

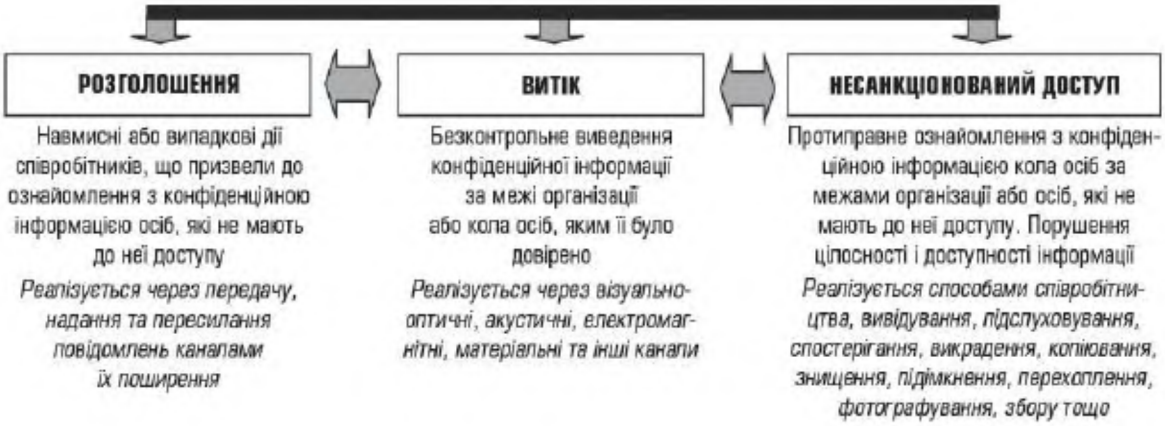
Усі ці підрозділи призначено для ведення кіберборотьби — *комплексу заходів, спрямованих на здійснення управлінського і/або деструктивного впливу на автоматизовані IT-системи протиборчої сторони та захисту від такого впливу власних інформаційно-обчислювальних ресурсів завдяки використанню спеціально розроблених програмно-апаратних засобів, а також проведенню системи спеціалізованих навчань.*



Об'єкти впливу в інформаційному та кіберпросторі

Інформаційну безпеку (ІБ) у 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 формування, використання й розвиток національної інфосфери в інтересах оборони

Головні загрози, які можуть спричинити порушення цих категорій, а також негативно вплинути на компоненти ІС, призвівши навіть до їх втрати, знищення чи збою функціонування, такі: розголошення інформації, її витік або несанкціонований доступ до такої інформації



Методи завдяки яким цьому можна запобігти, забезпечивши відповідний рівень ІБ:

• *сервіси мережної безпеки* (механізми захисту інформації, оброблюваної в розподілених обчислювальних системах і мережах);

• *інженерно-технічні методи* (мають на меті забезпечення захисту інформації від витоку по технічних каналах);

• *правові та організаційні методи* (створюють нормативну базу для організації різного роду діяльності, пов'язаної із забезпеченням ІБ);

• *теоретичні методи забезпечення* (розв'язують завдання формалізації різного роду процесів, пов'язаних із забезпеченням ІБ).

Кібербезпека - стан захищеності кіберпростору держави в цілому або окремих об'єктів її інфраструктури від ризику стороннього кібервпливу, за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, запобігання й нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним та/або національним інтересам.

Такий стан є вірогіднисним, високий ступінь якої досягається завдяки сукупності різних заходів, серед яких активні захисні і розвідувальні дії, що у процесі інформаційного протиборства зусиллями поодиноких інсайдерів або організованих кіберугруповань розгортаються навколо інформаційних ресурчів (ІР), інформаційно-комунікаційних технологій (ІКТ) та інформаційно-технічних систем (ІТС).

Такі дії спрямовуються на досягнення і утримання потенційними протиборчими сторонами переваги у протидії новим загрозам безпеці для власних об’єктів критично важливої фізичної, інформаційної та кіберінфраструктури.

Головні проблеми забезпечення кібернетичної безпеки постають з 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 унаочнює схема:

ОСНОВНІ НАПРЯМКИ СТВОРЕННЯ ЗАГАЛЬНОДЕРЖАВНОЇ СИСТЕМИ КІБЕРЗАХИСТІ ТА ПОДАЛЬШОГО СПІВРОБІТНИЦТВА УКРАЇНИ З НАТО:

1. Формування культури та проведення інформаційно-пропагандистської кампанії про значущість проблематики кібербезпеки держави за допомогою:

• активного інформування про кібернетичні втручання і загрози, про потенційні уразливості ІТ-систем і мереж, а також способи їх компенсації;

• розширення співпраці державних органів з ІТ-компаніями, некомерційними організаціями з метою популяризації та впровадження на практиці безпечної поведінки в кіберпросторі;

• стимулювання заходів боротьби з кіберзлочинністю і кібертероризмом, кібершпіонажем і кіберактивізмом;

• підвищення рівня безпеки електронних послуг, що надаються державою власному населенню;

• організації профілактичної роботи з потенційними жертвами кіберзлочинів, керівниками малого і середнього бізнесу.

2. Створення механізму моніторингу кібернетичних втручань і загроз, а також своєчасного ухвалення рішень щодо реагування на їх прояви за рахунок:

1) розроблення ключових моделей кібернетичних втручань і загроз, а також систем моніторингу їх реалізації;

2) формування критеріїв (наприклад, прогнозованих людських втрат, масштабів економічних збитків, загроз щодо дестабілізації суспільства), згід- но з якими об’єкти інформаційного та кіберпросторів віднесено до критичної інформаційної і кіберінфраструктури;

3) проведення активних розвідувальних дій у кіберпросторі потенційних протиборчих сторін, а також завдяки захисту власної інфосфери (рис. 1.8) від негативних чинників:

• деструктивного впливу на програмно-математичне забезпечення, комп'ю- терні мережі та телекомунікаційні засоби обміну даними;

• електромагнітного та фізичного ураження елементів ІТ-систем та мереж;

• консцієнтального (вплив на свідомість і моральний стан) та семантичного (вплив на якість інтерпретації інформації) впливу, а також електромагнітного ураження працівників органів управління;

• радіоелектронного подавлення елементів систем передавання даних і радіонавігації, систем телефонного і супутникового зв'язку, а також систем зв'язку з рухомими об'єктами;

4) зменшення вартості усунення наслідків кібернетичних втручань і загроз (створення розподілених структур, створення бекапів) тощо.

3. Забезпечення безпеки державних інформаційних ресурсів за рахунок:

• стандартизації об'єктів зберігання ІР та регламентів міжвідомчої взаємодії;

• гарантування безпеки механізмів електронної міжвідомчої взаємодії;

• мінімізації кількості шлюзів, що сполучають державні інформаційні системи з мережею Інтернет для максимізації їхньої безпеки.

4. Підвищення надійності критичної кіберінфраструктури за рахунок:

• створення механізмів моделювання і прогнозування кібервтручань та кіберзагроз;

• упровадження системи обміну інформацією щодо захисту об'єктів критично важливої інформаційної та кіберінфраструктури;

• забезпечення прийнятної автономності кореневої інфраструктури інтернету;
• розроблення механізмів протистояння використання інтернету в терористичних цілях.
5. Підтримка вітчизняних виробників програмно-апаратного забезпечення шляхом:
1) стимулювання розробки власної елементної бази і апаратних засобів, а також вітчизняного ПЗ і СПЗ, що впливатимуть на процеси:
• виявлення, проведення аналізу та своєчасного реагування на нові види кібернетичних втручань і загроз, а також ідентифікації відомих;
• ідентифікації користувачів, персоналу та можливих порушників;
• забезпечення конфіденційності, цілісності та доступності до ІР;
• несанкціонованого отримання інформації з ІТ-систем та мереж;
• формування політики безпеки щодо контролю мережного доступу;
• проектування та створення систем виявлення атак і захисту від них;
• виділення ресурсів, ранжування обраних контрзаходів за ступенем важливості з реалізацією та тестуванням найбільш пріоритетних;
• проведення аудиту та сертифікації нових СПАК, використовуваних у державній і військовій системах управління;
2) ліцензування ПЗ, що має базовий функціонал нейтралізації кібервтручань і кіберзагроз.
6. Підвищення компетентності фахівців різних сфер діяльності у питаннях кібербезпеки за рахунок:
• розроблення і впровадження програми навчання фахівців у галузі кібербезпеки, здатних до прогнозування можливих ризиків від кібернападів та оцінювання їх наслідків;

• реалізації механізмів набору персоналу необхідної кваліфікації для забезпечення кібербезпеки державних ІТ-систем і мереж тощо;

7. Вироблення і реалізація єдиної науково-технічної політики щодо захисту державних інформаційних ресурсів та ІТ-інфраструктури від деструктивного кібернетичного впливу на базі:

• формування і реалізації цільових науково-технічних програм у галузі кібербезпеки;

• цільового фінансування, підтримання та проведення НДДКР із кібербезпеки.

8. Реалізація механізмів партнерства держави, бізнесу й громадян у сфері кібербезпеки за рахунок:

• упровадження механізмів обміну інформацією державних ситуаційних центрів і центрів реагування на прояви стороннього кібервпливу з представни ками бізнесу та громадського суспільства;

• підвищення ефективності взаємодії провайдерів інтернет-послуг та користувачів в аспекті інформування про кібервтручання і загрози, потенційні уразливості ІТ-систем і мереж;

• організації співпраці державних і бізнесових інституцій, а також окремих громадян у питаннях розроблення сучасних програмно-апаратних засобів забезпечення кібербезпеки.

9. Удосконалення національного нормативно-правового та понятійно-тер мінологічного апарату кібербезпеки завдяки:

1) перегляду рекомендацій щодо придбання раціональних програмних засобів захисту від стороннього кібервпливу;

2) регулювання консультативних механізмів із питань забезпечення діяль ності у сфері боротьби з кіберзлочинністю і кібертероризмом;

3) актуалізації нормативно-правових актів України відповідно до сучасних світових загроз, практик і технологій;
4) внесення змін до низки чинних нормативно-правових актів України, які регулюють відносини й визначають загальні вимоги та організаційні засади забезпечення захисту державних інформаційних ресурсів.
10. Організація міжнародного співробітництва у сфері кібербезпеки шляхом:
1) створення міжнародного експертного центру з питань регулювання взаємовідносин у галузі телекомунікацій та зв'язку;
2) удосконалення механізмів надання взаємодопомоги в технічних і методологічних аспектах випереджувального виявлення джерел, фіксування та оперативного обміну інформацією про факти здійснення кібератак, а також запобігання їхньому деструктивному впливу на ІР;
3) удосконалення організаційно-правових норм міжнародної взаємодії у процесі боротьби з кіберзлочинністю і кібертероризмом та внесення змін і доповнень до низки чинних міжнародних нормативно-правових документів:
• Конвенції Ради Європи про кіберзлочинність 2001 року (зважаючи на те, що її положення порушують принцип державного суверенітету та узаконюють проведення наступальних міждержавних кібератак під виглядом оперативно-розшукових заходів);
• Рекомендацій Міжнародного союзу електрозв'язку (серія Х: Мережі передавання даних, взаємозв'язок відкритих систем та безпека. Безпека електрозв'язку. Огляд кібербезпеки), в яких вперше визначено зміст термінів «кіберсередовище» і «кібербезпека»;
• Положень Женевських і Гаазьких конвенцій (з урахуванням нових меж кібервоєн конкретні пропозиції щодо коригування цих Положень внесли

фахівці з Нью-Йоркського інституту EastWest на щорічній конференції Munich Security Conference).

Реалізація перелічених заходів має відбуватися в кілька етапів за неухильного дотримання таких принципів:

1) верховенства права, законності та пріоритету додержання прав і свобод людини і громадянина;

2) партнерства держави та приватного сектору з метою вироблення нових, більш оптимальних рішень;

3) пріоритетного розвитку та підтримки вітчизняного кібернетичного (або інформаційного) сектору;

4) відповідальності суб'єктів забезпечення кібернетичної безпеки за захист національної інформаційної інфраструктури, дієвості, комплексності і постійності заходів забезпечення кібербезпеки держави;

5) участі інституцій громадянського суспільства в забезпеченні кібернетичної безпеки держави.

Відповідну роботу слід проводити поетапно.

На першому етапі з урахуванням досвіду інших країн та особливостей українських реалій має бути вдосконалено понятійно-термінологічний та нормативно-правовий апарат, створено ключові елементи Єдиної загальнодержавної системи кібербезпеки, проведено заходи з підготовки структурних підрозділів спецпризначення та ЗС України до ведення дій в умовах кібервійни, сформовано базис підготовки спеціалізованих кадрів, створено міжвідомчі та центральні органи, а також удосконалено підрозділи власної інформаційної (кібернетичної) безпеки державних установ (відомств) та комерційних організацій (структур).

На другому етапі — удосконалено міжнародні правила поведінки держав у кіберпросторі та відповідне нормативно-правове підґрунтя,

упроваджено програми підтримання вітчизняної інноваційної продукції щодо протидії сторонньому кібернетичному впливу, розгорнуто мережі CERT по всій Україні.

На третьому етапі — проведено коригування Стратегії за результатами оцінювання ефективності її реалізації та нових викликів.

Інциденти у сфері високих технологій: характерні ознаки та проблемні аспекти. Процедура обрання раціонального варіанта реагування на кібернетичні втручання і загрози

Із розвитком ІКТ, ІТС та глобальної мережі Інтернет світове співтовариство, отримавши небачені досі можливості в плані обміну інформацією, стало надзвичайно вразливим щодо стороннього кібернетичного впливу, а саме щодо фактично неприхованих спроб впливу протиборчих сторін на інформаційний і кіберпростори один одного за рахунок використання засобів сучасної обчислювальної і/або спеціальної техніки й відповідного програмного забезпечення — кібервтручань, а також інших проявів їхнього дестабілізуючого впливу на той чи інший об’єкт, здійснюваного за рахунок технологічних можливостей інформаційного і кіберпростору, зі створенням небезпеки — так званих кіберзагроз, як для цього простору, так і для свідомості кожної людини.

Нині з метою уникнення багатозначності тлумачень відповідних термінів інструктивні матеріали Інтерполу поділяють їх на групи, що охоплюють:

• власне комп’ютерні інциденти, які полягають, наприклад, у втручанні в роботу обчислювальних систем, порушенні авторських прав на

програмне забезпечення, а також у розкраданні даних і комп'ютерного часу;

• інциденти, пов'язані з комп'ютерами, що супроводжують здебільшого протиправні дії з фінансового шахрайства;

• мережні інциденти, що призводять до укладання незаконних угод.

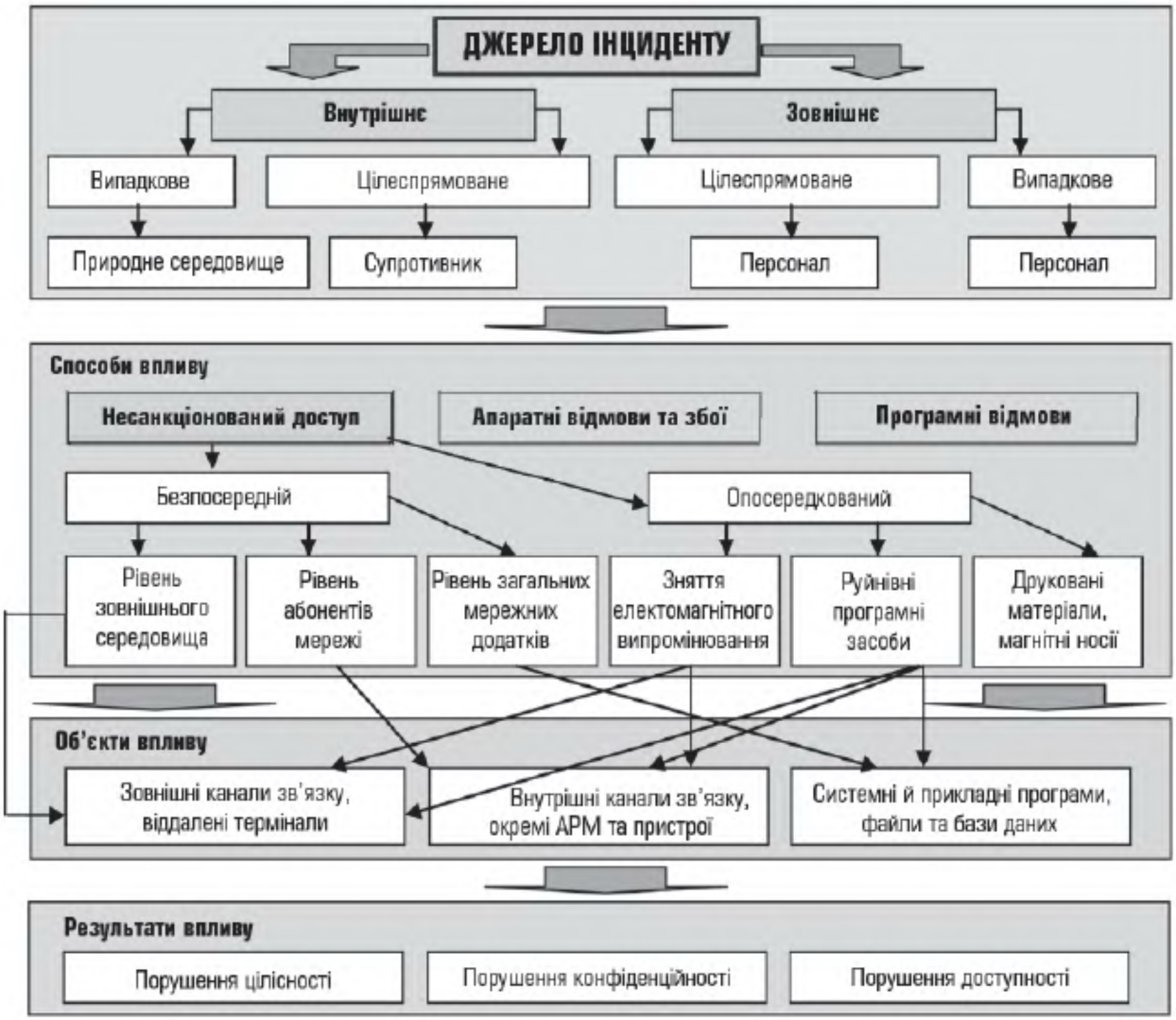
Під інцидентами у сфері високих технологій розумітимемо події, що полягатимуть в реалізації певної загрози та порушенні встановленого рівня безпеки інформаційно-комунікаційних систем (рис. 1.13).

Процесом управління інцидентами називатимемо процес реєстрації інформації про стан безпеки та рівноваги ІКС, передавання інформації в пункти її нагромадження,

переробки й аналізу, з ухваленням прийняття рішення та формуванням певного керуючого впливу на об'єкт управління.

Інша класифікація таких дій визначає сім основних їх груп, які характеризують передусім способи, що їх використовують зловмисники для здійснення нападу, а саме: перехоплення паролів інших користувачів; «соціальна інженерія»; використання помилок ПЗ і програмних закладок, а також помилок механізмів ідентифікації користувачів і недосконалості протоколів передавання даних; одержання інформації про користувачів стандартними засобами операційних систем; блокування сервісних функцій системи, що зазнає атаки.

Діаграма виникнення інцидентів у сфері високих технологій



Класифікація джерел інцидентів, а також способів, об'єктів та результатів їхнього впливу

ТЕМА 7. БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ ЛЮДИНИ В ІНФОРМАЦІЙНОМУ ПРОСТОРІ

Проблема інформаційної безпеки суспільства й особистості та їх захист від інформації має в своїй основі питання інформаційної стійкості і самоорганізації людини. Підхід, згідно з яким особистість являє собою самоорганізуючу систему, що має в своїй основі єдність стійкості і мінливості, дозволяє більш адекватно осмислювати актуальні проблеми її становлення й розвитку в інформаційному контексті.

Самоорганізація як шлях захисту особистості в інформаційному просторі

Загальноприйняте розуміння розвитку особистості – це стійкі зміни в структурі її життєдіяльності. Діалектика розвитку особистості полягає в тому, що вона завжди зберігає стан і одночасно змінюється в межах цього стану. Особистість може бути цілісною системою, коли вона має такі ознаки як стійкість і мінливість. Порушення цієї єдності в сторону стійкості веде до блокади самоорганізації; зміщення в бік мінливості руйнує цілісність системи.

Самоорганізація полягає в самоускладненні системи. Вона являє собою спрямовані зміни в організації й рівнях ієрархії системи, які відбуваються відносно інваріантно стосовно самої системи.

Самоорганізація визначається як найвища форма збереження живого, яка сприяє самоприскореному розвитку систем, їх прогресу.

Зростання стійкості соціальних систем, розвиток їх самоорганізації обумовлюється активною взаємодією з оточуючим світом, змінами, які в ньому відбуваються.

Активність соціальних систем визначає стійкість їх організації, яка виявляється в здатності до збереження свого стану при зовнішніх, у тому числі й інформаційно-психологічних впливах. Зв'язок між стійкістю і розвитком полягає в тому, що стійкі стани є моментами розвитку системи. Стійкість індивідуального розвитку є основою спрямованості змін. Стійкий стан виступає як результат перетворень.

Стійкість є результатом дій і вчинків суб'єкта, в основі яких лежить свобода вибору, активність суб'єкта при прийнятті рішень, критичне ставлення до оточуючого світу.

В начальному посібнику Хмельницького О.О. «Інформаційна культура: підготовка кадрів до інформаційної роботи» дано визначення поняттю соціальна стійкість.

Соціальна стійкість – це суспільна характеристика, що визначає внутрішню здатність особистості до дії й проявляється як більш-менш спрямована й усвідомлена діяльність, зміст якої полягає як у перетворенні існуючої дійсності, так і в особистісному формуванні індивіда. Соціальна стійкість відображається когнітивно, реалізується в структурі спонукань, змісті діяльності, формах поведінки.

Соціально-стійка особистість – це самоорганізуюча, саморозвиваюча система відношень з гранично вираженою суспільною спрямованістю, яка являє собою динамічну цілісність сукупності стійких структур.

Основою соціальної стійкості особистості є її інформаційна стійкість. Різноманітна інформація по-різному може впливати на особистість. Вона може виступати як фактор, що стимулює самоорганізацію особистості і сприяє її стійкості, а може здійснювати дезорганізуючий, руйнівний

вплив на людину. Інформаційна стійкість – це здатність людини протистояти деструктивному інформаційному впливу на свою свідомість і психіку. Підвищенню інформаційної стійкості повинен сприяти високий рівень інформаційної культури. Інформаційна стійкість є критерієм цілісності особистості. Не існує абсолютно стійких в інформаційному контексті живих систем. Інформаційна стійкість має межу, яка й детермінує цілісність особистості як складної системи. Заходи щодо захисту від інформації повинні спрямовуватися саме на підвищення інформаційної стійкості, її фундаментом має бути природне почуття, інстинкт самозбереження.

Адже, як писав відомий американський розвідник Ален Далес, «прагнення мати завчасну інформацію, без сумніву, породжено інстинктом самозбереження». Саме останній повинен захистити людину від надлишку інформації і деструктивного впливу з її боку.

Інформаційна культура (ІК) індивіда повинна надати йому чітке уявлення щодо того, споживання якої інформації є бажаним, а якої – ні. У цьому контексті однією з основних функцій ІК є формування інформаційно-стійкої особистості шляхом усвідомлення нею існуючих загроз від інформації. Суб'єкт, який усвідомлює загрози і володіє необхідними засобами для протидії їм, знаходиться на найвищому ступені інформаційної безпеки. І навпаки, суб'єкт, який не усвідомлює існування інформаційних загроз, насамперед підпадає під їх дію. Підвищенню інформаційної стійкості особистості повинна сприяти і така складова інформаційної безпеки, як інформованість. Остання припускає можливість отримання всієї необхідної інформації, а також можливість її переробки в заданий проміжок часу, а також класифікацію й осмислення

з метою напрацювання стратегічних та тактичних мотивацій і визначення конкретних проявів реалізації стратегії, що використовується.

Безпосередньо інформаційний вплив здійснюється шляхом обґрунтування, переконання, навіювання, спрямованого на аудиторію чи окрему особистість. Обґрунтованість являє собою осмислення логічних основ, які дають особистості впевненість у правильності свого розуміння. Тобто обґрунтованість – це спроба знайти «точки дотику» інформації і ціннісних настанов й орієнтацій особистості, на яку вона спрямована.

Впевненість може розглядатися як потік інформації, що знижує ступінь психічного опору особистості, яка піддається інформаційному впливу. Впевненість породжує переконання. Останнє формує певні настанови й через них – думки, погляди, відносини, які не завжди співпадають, а досить часто й суперечать особистісним настановам, які діяли раніше. Через переконання людина приходить до переконаності, яка розглядається як непорушна впевненість в істинності певних ідей і уявлень, в реальності засвоєних понять, образів і їх зв'язків з дійсністю. Впевненість дозволяє виробляти чіткі однозначні рішення.

Для усунення й нейтралізації різноманітних інформаційних загроз необхідно зосередити зусилля на активізації особистісних якостей, до яких, окрім вищезгаданих, слід додати ще одне – системність. Системне сприйняття інформації має велике значення для формування в особистості цілісної картини світу. Системний підхід дозволяє найбільш адекватним чином інтерпретувати та класифікувати всю інформацію, яка надходить до людини. При цьому виявляються явні й приховані фактори, причинно-наслідкові зв'язки, внутрішня логіка подій. Системний аналіз

сукупності окремих елементів дозволяє виявити ті з них, що мають патогенну спрямованість і становлять загрозу особистості.

Крім того, слід запропонувати ряд більш глобальних організаційних і педагогічних заходів. Перш за все необхідна розробка та реалізація цілісної концепції ідеологічної й пропагандистської дії, орієнтованої на встановлення пріоритету національних і культурних цінностей і світоглядних орієнтирів в противагу тим, що розповсюджуються з-за кордону. При цьому вказана концепція повинна стати основою для створення цивілізованого інформаційного простору країни, надання йому таких властивостей, як цілеспрямованість, системність, стійкість, безпечність. Однак тут повинен використовуватися не абстрактний підхід, як це було раніше, коли потужна ідеологічна система працювала сама на себе й при цьому повністю ігнорувала життєві інтереси та потреби особистості, а підхід, орієнтований на конкретних людей – громадян країни, на захист їх духовного здоров'я, попередження інформаційних загроз, збереження цілісної особистості як стійкої системи, що розвивається. Через загальнодержавні ідеологічні, педагогічні, організаційні та інші заходи слід сформувати в особистості захисний інформаційний прошарок, генетичну основу якого складатимуть загальнолюдські цінності й орієнтири. Саме він повинен захистити особистість від згубної інформаційної дії, а також від вищеперерахованих інформаційних загроз.

При цьому основи інформаційної безпеки особистості мають закладатися на початкових стадіях її формування. Процес виховання повинен ґрунтуватися на традиціях і принципах, що не суперечать діючим нормам і правилам суспільної поведінки, культурним ідеалам.

Людина повинна розуміти та приймати норми й традиції свого народу і своєї країни. Прилучаючись до досягнень світової культури, вона повинна віддавати пріоритет вітчизняним зразкам, які також входять до складу світової культури. До того ж важливим елементом в системі виховання є патріотизм, який сприяє формуванню стійкої в соціальному, психологічному й інформаційному аспекті особистості, а також визначає особливості інформаційного сприйняття.

Успішна реалізація заходів інформаційної безпеки особистості можлива лише за умови принципово нових підходів до системи освіти, а також методів передачі й формування масивів знань. Осмислюючи новітні наукові досягнення в області синергетики, геоглобалістики, ноосферології, теорії фізичного вакууму, а також нові підходи до вирішення комунікативних, соціальних і екологічних проблем, учені приходять до висновку про необхідність переходу до нової стратегії розвитку сучасної системи освіти, в основу якої покладена ідея випереджаючої освіти. Діюча система освіти реалізує концепцію так званої підтримуючої освіти, суть якої полягає в тому, що підготовка спеціалістів здійснюється на основі вимог сьогодення без урахування того, що очікує цих фахівців у майбутньому.

Концепція системи випереджаючої освіти полягає в її принциповій орієнтації на майбутнє. Вона повинна створюватися на основі синтезу новітніх знань різних наук. Однією з пріоритетних цілей такої системи повинно бути формування в людей таких якостей, які дозволять їм успішно адаптуватися в умовах інформаційного суспільства. При формуванні концепції випереджаючої освіти є виключно важливим зрозуміти, якими саме якостями повинні володіти люди, для того щоб

швидко адаптуватися в мінливому світі, використовувати його нові можливості й захищати себе від нових інформаційних загроз. До таких якостей в першу чергу належать:

 ноосферна свідомість;

 системне мислення;

 інформаційна культура;

 економічна культура;

 творча активність;

 толерантність;

 висока моральність.

В основу концепції випереджаючої освіти покладені ідеї А.Д. Урсула, її основні принципи були сформульовані і розвинені К.К. Коліним:

 формування у людей нового, глобального типу свідомості, який, згідно з ідеями А.Д. Урсула, можна назвати ноосферною свідомістю;

 формування науково обґрунтованих уявлень про основні закономірності розвитку природи та суспільства, а також про особливу роль інформації й інформаційних процесів. Тут слід підкреслити необхідність розвитку та впровадження в систему освіти нових принципів передачі знань й інформації;

 вивчення закономірностей становлення нового постіндустріального інформаційного суспільства, а також тих проблем і загроз, з якими людині доведеться зустрічатися;

 формування в людей науково обґрунтованих уявлень про тенденції й перспективи подальшого технічного розвитку цивілізації.

Оволодіння методологією та практичними навичками системного аналізу інформаційних аспектів найважливіших соціальних, економічних і науково-технічних проблем, вивчення методів їх розв'язання на основі активізації інформаційних ресурсів;

 формування в суспільстві нового перспективного виду культури – інформаційної культури. Ця культура повинна дати людині в інформаційному суспільстві не лише інформаційну свободу, тобто вільний доступ до всієї необхідної інформації, а і забезпечити безпрецедентні можливості для розвитку людини як особистості, для практичної реалізації нею своїх громадських прав і свобод;

 формування в людей нової якості особистісної інформаційної культури, яка повинна бути заснована не лише на знанні закономірностей інформаційних процесів в суспільстві, а також і на розумінні своєї відповідальності за забезпечення інформаційної безпеки всіх членів суспільства.

У межах концепції випереджаючої освіти необхідна розробка нових форм і методів роботи з інформацією, які б дозволили людині вільно орієнтуватися у великих масивах інформації, здійснювати їх моніторинг, підвищити ефективність пошуку потрібних відомостей.

Такі форми та методи дозволять запобігти інформаційному перенасиченню й інформаційному тромбозу, підвищити якість інформаційної роботи. Для підвищення інтелектуальних і психофізичних здібностей людини щодо сприйняття інформації можна порекомендувати використання методів швидкісного читання.

Для попередження маніпулятивного впливу на особистість з боку іноземної інформаційної присутності в ЗМІ, суспільних і релігійних об'єднаннях слід звернути особливу увагу на підвищення інформаційної стійкості до патогенних текстів, які передаються різними каналами. При цьому культура, ідеологія й освіта повинні виступати єдиним комплексом, який має своєю метою стійкий розвиток людини.

. БЕЗПЕКА ДІЛОВОГО СПІЛКУВАННЯ

Для того щоб не попадатися на маніпулятивні гачки, перш за все їх треба вміти розпізнавати. У випадку ідентифікації маніпулятивних прийомів, які використовує опонент, подальші дії можуть вибудовуватися в залежності від характеру, завдань й умов конкретного спілкування.

Розглянемо деякі загальні положення, які певним чином дозволяють виявити та знизити ефект дії маніпулятивних прийомів.

На першому етапі перед дискусією необхідно з‟ясувати й чітко визначити для себе та своїх партнерів яких цілей ви хочете досягти.

Це буде тим системотвірним фактором, який має визначити весь хід та спрямованість вашої участі в дискусії. Необхідно визначити і зафіксувати які цілі декларують ваші опоненти та намагатися спрогнозувати, наскільки вони розходяться з істинними намірами. На протязі всієї дискусії необхідно постійно утримувати в “полі уваги” цілі, загальний план і хід дискусії.

Аргументацію, що використовується в ході дискусії можна поділити на так звану аргументацію доведення та контраргументацію. Для їх аналізу з метою виявлення слабких сторін, які можуть бути використані для

посилення позицій опонентами, можна використати наступні правила аналізу.

Для аналізу доказової аргументації:

1. Чи є точними дані, що використовуються нами?
2. Чи є вірними висновки?
3. Які є протиріччя в аргументації?
4. Чи можна навести зрозумілі порівняння (аналогії)?
5. Які доводи можуть виникнути у опонентів на нашу аргументацію?
6. Чи носять розбіжності принциповий характер?
7. Чи можна досягти успіху поступками щодо непринципових розбіжностей?

Для аналізу контраргументації:

1. Чи є протиріччя в опонентів?
2. Чи можна спростувати факти та положення опонентів?
3. Чи є невдалі приклади або порівняння?
4. Чи є в опонентів помилкові або невдалі висновки?
5. Чи не занадто опоненти спростили проблему та чи можна показавши її інші сторони посилити доказовість власного тезису?
6. Чи є в опонентів хибні оцінки?
7. Якщо неможливо спростувати контраргументацію в цілому, чи можливо поставити питання до окремих складових?
8. Чи можна показати протиріччя в контраргументації опонентів шляхом уточнень і питань?
9. Чи не використовують опоненти спекулятивні (недозволені) прийоми та яким чином це можна використати для посилення власної аргументації?

У випадках, коли опонент використовує недозволені прийоми, це можна відкрито обговорити з ним, як про недопустиму тактику ведення диспутів. У випадках "злісного" використання опонентом маніпуляцій можливо відповісти своїми хитрощами, які б паралізували хитрощі опонента. Це небажаний прийом, який можна виправдати, коли всі інші способи себе вичерпали.

Використання, так званого "зворотного удару" засновується на виявленні у тезах опонента доводів, які можуть бути спрямовані проти його ж доведення. Таким чином показується логічна неспроможність опонента.

Виявлення пастки може будуватися на відповіді, в якій показується неправильність подібних міркувань на якомусь яскравому прикладі.

Спосіб звинувачення полягає у тому, що показується характер пастки й звертається увага на її навмисний характер. Така поведінка буває доцільною для того, щоб осадити грубого опонента. Цим краще не зловживати.

"Метод Сократа" полягає у постановці серії питань, на які просять дати однозначні відповіді. Питання ставляться таким чином, щоб опонент, відповідаючи на них, сам спростував свої тези. Однак треба пам"ятати, що цей метод сам перетворюється на пастку, якщо на питання не можна дати однозначну відповідь.

Пастки, що базуються на викривленні смислу, нейтралізуються за допомогою уточнень висловлювань, повторень аргументів тощо.

Важливо не піддаватися на провокації, які містять особисту образу. Їх можна перевести в атаку на проблему, що обговорюється, звертаючи увагу на те, що саме цим мають займатися учасники обговорення.

Не слід намагатися "загнати опонента у кут", особливо під час публічних обговорень, бо його захисна реакція може звести до нуля досягнуті результати.

Одна із головних вимог – дотримання принципів і правил аргументації. Якщо обидві сторони їх притримуються, то ніякі інші допоміжні прийоми не потрібні. Веденню дискусій конструктивного характеру сприяє також вироблення концепції обговорення.

ВИСНОВКИ

Виокремлення інформаційно-психологічної безпеки особистості із загальної проблематики інформаційної безпеки як самостійного напрямку визначається наступними основними причинами:

- перехід до інформаційного суспільства, збільшення масштабів та ускладнення змісту й структури інформаційних потоків значно посилюють їх вплив на психіку людини. Це визначає необхідність формування нових механізмів і засобів виживання людини як особистості і активного соціального суб‘єкта в сучасному світі;
- взаємодія психіки людини з інформаційним середовищем відрізняється своєю специфікою та не має адекватних аналогів в інформаційній взаємодії інших біологічних, технічних, соціальних та соціотехничних систем;
- основною "мішенню" інформаційного впливу є людина, його психіка. Саме із окремих особистостей, їх взаємодії залежить нормальне функціонування соціальних суб‘єктів різного рівня складності, будь-

яких спільнот і соціальних груп - от малої групи до населення країни в цілому.

Загальним джерелом зовнішніх загроз інформаційно-психологічної безпеки особистості є та частина інформаційного середовища суспільства, яка в силу різних причин не адекватно відображає навколишній світ. Тобто інформація, яка вводить людей в оману, у світ ілюзій, часто видаючи бажане за дійсне не дозволяє адекватно сприймати світ і самого себе, що веде до зниженнч ефективності принятих рішень і самої особистості взагалі.

Глосарій

Використання інформації – задоволення інформаційних потреб громадян, юридичних осіб і держави.

Зберігання інформації – означає забезпечення належного стану інформації та її матеріальних носіїв.

Одержання інформації – процес набуття, придбання, накопичення інформації громадянами, юридичними особами або державою відповідно до чинного законодавства України.

Підсвідомість – сукупність активних психічних процесів (інтуїція, паніка, гіпноз, сновидіння, звичні дії тощо), які не є центром смислу діяльності свідомості, але здійснюють вплив на протікання свідомих процесів. Підсвідомість можна розглядати як неусвідомлений рівень психіки, тобто як сукупність психічних процесів, актів і станів, обумовлених оточуючим середовищем, вплив яких суб‘єкт не усвідомлює. Підсвідомість відрізняється від свідомості тим, що реальність зливається з

переживаннями суб'єкта, тому і неможливий контроль дій, що здійснює суб"єкт, а також оцінка їх результатів.

Вплив на підсвідомість являє особливо небезпечну загрозу, оскільки він ніяким чином не проявляється та не реєструється свідомістю.

Вплив на підсвідомість дозволяє змінювати мотиви та смисл діяльності людини, програмувати його поведінку на підставі персональних стереотипів, а також активізувати сприймання інформації та творче мислення.

Поширення інформації – розповсюдження, обнародування, реалізацію інформації у встановленому законом порядку. Психіка – функція головного мозку, яка полягає в активному відображенні людиною об"єктивного світу, побудові картини цього світу й саморегуляції на цій основі своєї поведінки та діяльності. В психіці представлені та упорядковані події минулого, теперішнього та можливо майбутнього часу. Головною формою психіки людини є свідомість, але вона не вичерпує підсвідомість. У людини ще є і неусвідомлені психічні процеси (див. підсвідомість).

Соціальна стійкість – це суспільна характеристика, що визначає внутрішню здатність особистості до дії й проявляється як більш-менш спрямована й усвідомлена діяльність, зміст якої полягає як у перетворенні існуючої дійсності, так і в особистісному формуванні індивіда. Соціальна стійкість відображається когнітивно, реалізується в структурі спонукань, змісті діяльності, формах поведінки.

Соціально-стійка особистість – це самоорганізуюча, саморозвиваюча система відношень з гранично вираженою суспільною спрямованістю, яка являє собою динамічну цілісність сукупності стійких структур.

Усвідомлення – це фокусування свідомості на психічних процесах, на тих чуттєвих образах дійсності, які особистість завдяки їм отримує.

В основі усвідомлення лежить узагальнення власних психічних процесів, що приводить до оволодіння ними. Іншими словами, усвідомлювати - це осягати розумом, сприймати свідомо, розуміти значення, сенс чогось.

Рекомендована література

1. Конституція України. https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text
2. Закон України Про інформацію https://zakon.rada.gov.ua/laws/main/2657-12#Text
3. Закон України Про державну таємницю https://zakon.rada.gov.ua/laws/main/3855-12#Text
4. Закон України Про захист персональних даних https://zakon.rada.gov.ua/laws/main/2297-17#Text
5. Закон України Про основні засади забезпечення кібербезпеки України https://zakon.rada.gov.ua/laws/show/2163-19#Text
6. Закон України Про національну безпеку України https://zakon.rada.gov.ua/laws/show/2469-19#n355
7. Закон України Про медіа https://zakon.rada.gov.ua/laws/show/2849-20#n2349
8. СТРАТЕГІЯ зовнішньополітичної діяльності України https://zakon.rada.gov.ua/laws/show/448/2021#n11
9. УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №447/2021 Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" https://www.president.gov.ua/documents/4472021-40013
10. Бобало Ю.Я. Інформаційна безпека: навч.посібник. – Львів, 2019. – 580 с.
11. Бурячок, В. Л.Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок,В. Б. Толубко, В. О. Хорошко, С. В.

Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.— К.: ДУТ, 2015.— 288 с

12. Сунь-Дзи. Мистецтво Війни. Переклад з давньокитайської: Сергій Лесняк. — Львів : Видавництво Старого Лева, 2015. — 108 с
13. Жарков Я.М., Дзюба М.Т., Замаруєва І.В. Інформаційна безпека особистості, суспільства, держави: Підручник. – К.: Видавничо-поліграфічний центр “Київський університет”, 2008.
14. Юдін О.К., Богуш В.М. Інформаційна безпека держави. — Харків: Консум, 2004. — 508 с.