МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Київський національний університет будівництва і архітектури

Є.Є. Шабала, В.В. Клюєва

ІНФОРМАЦІЙНА КУЛЬТУРА

Конспект лекцій
для студентів спеціальностей
123 «Комп’ютерна інженерія»
та 125 «Кібербезпека»

Київ 2023

УДК 007:304
Ш-12

Рецензенти: Терентьєв О.О. – д-р техн. наук, професор
Котенко А.М. – канд. техн. наук, доц., доцент

Затверджено на засіданні вченої ради факультету автоматизації і інформаційних технологій, протокол №9 від 1 лютого 2023 року.

Шабала Є.Є.

Ш-12 Інформаційна культура: конспект лекцій / Є.Є. Шабала, В.В. Клюєва - Київ: КНУБА, 2023. – 100 с.

Розглянуто основні визначення інформації та інформаційної культури та як вони допомагають кібербезпеці.

Призначено для студентів спеціальностей 123 «Комп'ютерна інженерія» та 125 «Кібербезпека»

УДК 007:304

ЗМІСТ

ТЕМА 1. ВИЗНАЧЕННЯ ІНФОРМАЦІЇ ТА ІНФОРМАЦІЙНОЇ КУЛЬТУРИ

Існує багато визначень «інформаційної культури», втім, як і категорії «культура» (на початку 90-х років XX ст. тільки у філософській літературі було понад 500 визначень поняття «культура»).

Інформація – сукупність відомостей (даних), які сприймають з оточуючого середовища (вхідна інформація), повертають в оточуюче середовище (вихідна інформація) або зберігають всередині певної системи.
Інформація існує у вигляді документів, креслень, малюнків, текстів, звукових та світлових сигналів, енергетичних та нервових імпульсів і так далі.

Отже, властивості інформації:

1. Достовірність. Достовірність інформації - властивість інформації бути правильно сприйнятою і відображати дійсне положення справ. Достовірність характеризується величиною рівною доповненню вірогідності виникнення помилок в інформаційній системі до одиниці. Заданий рівень достовірності інформації забезпечується контролем і виправленням виявлених помилок. Недостовірна інформація може привести до неправильного розуміння або ухвалення неправильних рішень. Достовірна інформація з часом може стати недостовірною, оскільки вона володіє властивістю застарівати, тобто перестає відображати дійсне положення справ.

2. Повнота. Інформація повна, якщо її досить для розуміння і ухвалення рішень. Як неповна, так і надмірна інформація стримує ухвалення рішень або може спричинити помилки.

3. Точність. Точність інформації визначається ступенем її близькості до реального стану об'єкту, процесу, явища і тому подібне

4. Своєчасність. Тільки своєчасно отримана інформація може принести очікувану користь. Однаково небажані як передчасна подача інформації (коли вона ще не може бути перероблена), так і її затримка.

5. Цінність. Цінність інформації залежить від того, наскільки вона важлива для вирішення завдання, а також від того, наскільки надалі вона знайде застосування в яких-небудь видах діяльності людини.

6. Корисність. Ефект від використання інформації повинен перевищувати витрати на її отримання.

7. Зрозумілість. Інформація зрозуміла, якщо вона виражена мовою, яка відома приймачу інформації. Якщо цінна і своєчасна інформація виражена незрозумілим чином, вона може стати даремною.

8. Доступність. Форма викладу інформації повинна відповідати рівню її сприйняття. Тому одні і ті ж питання по різному висловлюються в шкільних підручниках і наукових виданнях.

9. Стислість. Інформацію по одному й тому ж питанню можна викласти коротко, стисло, без неістотних деталей (довідник) або детально, багатослівно.

Складовою частниною інформацією є дані, які під час інформаційного процесу перетворюються з одного виду в інший за допомогою методів.

Основні операції над даними:

- **Збір даних.** Накопичення інформаціїїї з метою забезпечення достатньої повноти для прийняття рішень.
- **Формалізація даних.** Приведення даних, що надходять з різних джерел, до однакової форми, щоб зробити їх сумірними (який можна виміряти однаковою з будь-якою мірою; спільномірний) і підвішити рівень доступності.
- **Фільтрація даних.** Відсіювання «зайвих» даних, які не є важливими для прийняття рішень. Після фільтрації достовірність і адекватність даних повинні зростати.
- **Сортування даних.** Впорядкування даних за заданою ознакою з метою зручностівикористання та підвищення доступності інформації.
- **Архівація даних.** Організація збереження даних в зручній та легкодоступній формі. Це потрібно для зниження економічних витрат на зберігання даних і підвищує загальну надійність інформаційного процесу в цілому.
- **Захист даних.** Комплекс заходів, що скеровані на запобігання втрат, відтворення та модифікації даних.
- **Транспортування даних.** Прийом та передача даних між віддаленими учасниками інформаційного процесу.
- **Перетворення даних.** Переведення даних з однієї форми в іншу або з однієї структури в іншу.

Робота з інформацією є доволі місткою, то му її прагнуть автоматизувати.

Становлення інформаційної культури людини відбувається в її повсякденній діяльності під впливом засвоєних побутових знань та умінь, інформації засобів масових комунікацій, у процесі самоосвіти, під час навчання, в сім'ї та на роботі».

Згідно з трактуванням професора Ю. Зубова, **інформаційна культура – це систематизована сукупність знань, умінь, навичок, що забезпечує оптимальне здійснення інформаційної діяльності, спрямованої на задоволення як професійних, так і непрофесійних потреб.** Є. Медведєва

визначає інформаційну культуру як «рівень інформаційної підготовки, який дозволяє людині не тільки вільно орієнтуватися в потрібному інформаційному середовищі, а й брати участь у його формуванні та перетворенні, сприяти інформаційним контактам». За визначенням Є. Семенюка, «інформаційна культура – це ступінь розвиненості інформаційної взаємодії та всіх інформаційних взаємовідносин у суспільстві».

Широко розповсюджене уявлення, згідно з яким інформаційну культуру людини слід розуміти як уміння користуватися комп'ютерною технікою та здатністю формалізувати знання таким чином, щоб вводити їх в автоматизовані системи. Але інформація існує не тільки в комп'ютері у вигляді даних (або знань), а й всюди навколо нас. Комп'ютер є лише засіб для оперативної й автоматичної (а тому зручної для користувача) обробки інформації, якого б виду вона не була (текстовою, числовою, графічною, музикальною, комбінованою). Таким чином, феномен, що розглядається, включає як традиційні способи роботи з інформацією, так і ті, що пов'язані з використанням комп'ютерної техніки та мереж комунікацій. Крім того, будьяка культура людини передбачає наявність у неї не тільки умінь, але й певних знань, навичок, здібностей, ціннісних орієнтацій.

З такої позиції вміст визначення цього виду культури на рівні особистості можна подати так: інформаційна культура людини – це системне утворення особистості, яке інтегрує знання про основні методи інформаційних технологій, уміння використовувати наявну інформацію для вирішення прикладних завдань, навички використання персонального комп'ютера і технологій зв'язку, здібності представити інформацію в зрозумілій для усіх формі, орієнтує на розширення та поновлення знань.

Якщо представити це поняття в стислій формі, то інформаційна культура людини – це інтеграція здібностей, навичок, знань, ціннісних орієнтацій особистості, які детермінують свідоме намагання до придбання нових знань.

Сутність інформаційної культури виявляється через її компоненти. Умовно ці компоненти можна поділити на декілька груп:

- загально пізнавальні;
- алгоритмічної культури;
- ті, що пов'язані з навичками оволодіння комп'ютерною технікою;
- які включають знання етичних та юридичних норм у галузі інформаційних технологій;
- інформаційні.

Деталізація цих компонентів може мати наступну структуру:

1. Загально пізнавальні компоненти складають:

- загальнокомунікативні вміння;
- уміння організувати пошук інформації з різних джерел, користуватися алфавітним та тематичними каталогами у бібліотеці;
- знання періодичних видань, навички роботи з енциклопедіями та довідниками у фаховій та суміжних галузях, уміння складати конспект;
- використання прийомів і методів ефективного читання;
- уміння обирати і ставити мету, здійснювати постановку завдань, формулювати обґрунтовані гіпотези, систематизувати факти, осмислювати і аналізувати висновки, узагальнювати спостереження, передбачати наслідки рішень, що приймаються, та власних дій, вміти їх оцінювати та ін.

2. Компоненти алгоритмічної культури включають наступні уміння:

- уміння правильно, чітко та однозначно формулювати власні думки у зрозумілій для співрозмовника формі;
- добирати послідовність операцій у пізнавальній діяльності, розробляти програму спостереження, дослідження, експерименту;
- аналізувати знання та інтерпретувати отримані результати та ін.

3. Компоненти, які пов'язані з навичками оволодіння комп'ютерною технікою, включають:

- уміння достатньо швидко вводити інформацію з клавіатури та робити з графічним інтерфейсом програми з використанням миші;
- здібності використовувати засоби операційної системи та прикладне програмне забезпечення загального та предметно-орієнтованого призначення, системи телекомунікацій;
- звичку звертатись до комп'ютера для вирішення завдань з будь-якої предметної галузі за умови, що такий спосіб доступу до інформації є найбільш раціональним, та ін.

4. компоненти, які включають знання етичних та юридичних норм у галузі інформаційних технологій:

- знати і не порушувати закони про авторські права на комп'ютерні програми (тобто виконується чинне законодавство стосовно охорони інтелектуальної власності, яке забороняє нелегальне копіювання та використання програмного забезпечення);
- дотримуватись етичних норм при опублікуванні інформації в Internet, при роботі з електронною поштою і участі в телеконференціях (комп'ютерною спільнотою засуджується розміщення на сторінках Internet насильства, пропаганда наркотиків і порнографії).

Аналіз вищезазначеного показує, що формування інформаційної культури здійснюється через опанування людиною знаннями та уміннями, які включаються до її компонентів. Ці компоненти опановуються у процесі навчання усім предметам, які вивчаються у закладах освіти. Особлива роль при цьому належить освітньому предмету "інформатика", основним об'єктом дослідження якого є інформація, тому в процесі його вивчення формуються додаткові, в порівнянні з іншими предметами, інформаційні компоненти, котрі, на нашу думку, потрібні лише спеціалістам у галузі інформатики:

- розуміння сутності інформації та інформаційних процесів, їх ролі в пізнанні оточуючої дійсності і творчої діяльності людини, в керуванні технічними і соціальними процесами, їх ролі в забезпеченні зв'язку живого з оточуючою дійсністю;
- розуміння проблем передачі, оцінки і виміру інформації, її сприйняття і осмислення, сутності процесу формалізації, усвідомлення зв'язку між змістом і формою, а також ролі інформаційного моделювання в сучасній інформаційній технології;
- уміння формалізувати наявні знання та будувати інформаційні моделі досліджуваних процесів і явищ;
- розуміння сутності штучного інтелекту [1] .

Отже, можна зробити такі узагальнення: **Інформаційна культура** (від лат. cultura — освіта, розвиток та informatio — роз'яснення) – це:

1) сукупність досягнень певного людського суспільства (групи людей, нації, народу, суспільства, держави, міжнародного співтовариства) у сфері інформаційних відносин (у тому числі мистецтва, науки, техніки тощо);

2) відповідний рівень розвитку інформаційних відносин на певний момент часу у певному колі осіб, що визначається порівняно з попередніми показниками інформаційної культури;

3) сукупність практичних, матеріальних і духовних надбань суспільства, які відображають історично досягнутий рівень розвитку суспільства і людини у сфері інформаційних відносин та втілюються в результатах інформаційної діяльності;

4) сфера духовного життя суспільства, що охоплює насамперед систему виховання, освіти, наукової та мистецької творчості, у контексті інформаційних відносин, а також установи й організації, що забезпечують функціонування їх (школи, вищі навчальні заклади, клуби, музеї, театри, творчі спілки, товариства тощо);

5) ступінь (рівень) довершеності в оволодінні знаннями у галузі суспільних інформаційних відносин та діяльності;

6) метод формування високого рівня інформаційних відносин;

7) сукупність умов, що забезпечують високий рівень, продуктивність, безпеку інформаційних правовідносин;

8) рівень фахової підготовки працівників (працівника) у сфері інформаційних правовідносин та особистої організованості їх;

9) рівень відповідності норм, встановлених у суспільстві, нормам інформаційних правовідносин;

10) галузь загальної культури (як науки), що вивчає проблеми 23 унормування суспільних інформаційних відносин;

11) сукупність духовних цінностей у сфері інформаційних відносин, створених людством упродовж його історії;

12) рівень, ступінь досконалості певної галузі розумової діяльності.

Отже, як бачимо, зміст поняття «інформаційна культура» трактується по-різному і співвідноситься з такими категоріями, як «загальнолюдська культура», «освітня діяльність», «інформаційна діяльність». Сьогодні є всі підстави говорити про формування нової інформаційної культури, яка повинна стати елементом загальної культури людства.

Якщо роздивлятись поняття питань культури з погляду сучасності, то насамперед вони пов’язані із самовизначенням народів (зокрема людини) та їх мовним розвитком (як засоби спілкування). У зв’язку з цим інформаційну культуру в нових формах її передачі, зокрема в навчанні, можна розуміти, як систему з чотирьох **базових компонентів**, а саме:

- культури організації подання інформації;
- культури сприймання та користування інформацією;
- культури використання нових інформаційних технологій (НІТ);
- культури спілкування через засоби ІТ.

Два останні компоненти формують так званий мережевий етикет. Оскільки відсутнє загальноприйняте тлумачення поняття «інформаційна культура», то під нею ми розумітимемо систематизовану сукупність знань, умінь, навичок, що забезпечує оптимальне здійснення індивідуальної інформаційної діяльності, спрямованої на задоволення як професійних, так і непрофесійних потреб в інформації.

Інформаційна культура особистості — одна зі складових загальної культури людини; це — динамічна єдність світоглядної, інформаційно-технологічної, комунікативної й інтелектуально-творчих компонентів;

сукупність інформаційного світогляду та системи знань і вмінь, що забезпечують цілеспрямовану самостійну діяльність з оптимального задоволення індивідуальних інформаційних потреб з використанням як традиційних, так і нових інформаційних технологій [1].

На основі наведених понять можна назвати концептуальні **функції інформаційної культури особистості:**

1. Світоглядна — формування на основі долучення інформації до категоріальних понять усесвіту і трансформації на цій основі свідомості, сфери діяльності, регулятивних норм взаємодії в суспільстві.

2. Інформаційно-технологічна — комп'ютерна й інформаційна писемність, що відповідає сучасному рівневі розвитку техніки, інформаційних і телекомунікаційних технологій, структурі та якості інформаційних ресурсів.

3. Комунікативна — характеризує культуру спілкування суб'єкта в інфосередовищі з іншими суб'єктами, з електронно-обчислювальними й електронно-інтелектуальними системами.

4. Інтелектуально-творча — визначає культуру діяльності суб'єкта в інфосередовищі, активну інтелектуально-творчу спрямованість цієї діяльності.

Суть концепції зводиться до ствердження тези про те, що масове підвищення рівня інформаційної культури суспільства можливе лише при організації спеціального навчання сучасних споживачів інформації, тобто при організації інформаційної освіти. Доступ до значних інформаційних ресурсів з метою ефективного їх використання потребує наявності високого рівня інтелекту й творчих здібностей у сучасної людини, знання основ науково-інформаційної діяльності. Лише спеціальна підготовка, інформаційна освіта гарантують людині реальний доступ до інформаційних ресурсів і культурних цінностей, зосереджених у бібліотеках, інформаційних центрах, архівах, музеях світу.

Необхідний синтез усіх цих знань, що утворюють у сукупності інформаційну культуру особистості. При цьому наявність спеціальної інформаційної підготовки, необхідний рівень ін-формаційної культури важливі такою мірою, як і наявність комп'ютерів і каналів зв'язку — не-одмінних атрибутів інформаційного суспільства. Саме ця думка є основою концепції та техно-логії формування інформаційної культури особистості. Поняття «інформаційна культура особи-стості» є вельми ємним і містить у своєму складі поняття «інформаційна писемність», відрізня-ючись від нього такими компонентами, як інформаційний світогляд і здатність людини створю-вати нові інформаційні продукти й творчо їх використовувати в різних цілях [2].

Крім того, інформаційна культура відрізняється від інформаційної писемності здатністю людини створювати нові інформаційні продукти та творчо їх використовувати в різних цілях. Під поняттям «інформаційний продукт» у цьому разі розумітимемо результат інтелектуальної діяльності людини зі створення нової інформації або смислової переробки наявної інформації, поданий у формі документа. Наприклад, викладач на основі вивчення численних публікацій, аналізу педагогічного досвіду генерує нове знання — нову методику, нову педагогічну техноло-гію та ін., оформлюючи його в інформаційний продукт своєї науково-дослідницької діяльності —статтю, методичні рекомендації. Студент у процесі своєї навчальної діяльності не створює нового знання, проте на основі вивчення й аналізу відповідної літератури готує інформаційні продукти — реферати, доповіді, курсові та дипломні роботи, в яких знайдена в різних джерелах інформація переробляється відповідно до логіки автора, підлягає зіставленню і критичній оцінці.

Здатність створювати власний інформаційний продукт на основі самостійно знайденої, критично оціненої і перетвореної інформації є найважливішою властивістю творчої (креативної) особистості, розвиток якої є основним завданням сучасної системи освіти. Отже, можна говори-ти про те, що між становленням творчої та креативної особистості і формуванням інформаційної культури особистості існує тісний зв’язок. Він виявляється в тому, що підвищення продук-тивності будь-якого виду інтелектуальної праці, суть якої полягає в роботі з інформацією (її аналізі, зіставленні, порівнянні, класифікації й узагальненні), неможливе без відповідного рівня інформаційної культури особистості.

Особливе місце в складі поняття «інформаційна культура особистості» належить інфор-маційному світогляду. **Інформаційний світогляд** — це система поглядів людини на світ інфор-мації і місце людини в ньому. Інформаційний світогляд містить переконання, ідеали, принципи пізнання і діяльності. Процеси інформатизації й глобалізації сучасного суспільства базуються на сучасних технічних можливостях і властивостях інформації, пов’язаних з її стрибкоподібним зростанням, впливом нових інформаційних технологій на розвиток інших технологій, перетво-ренням інформації на основний предмет людської праці (А. Єляков). Зазначені явища в суспіль-стві супроводжують зміни в науковому баченні світу (Ю. Юзвішин). У суспільстві формується нове ставлення до інформації, змінюються принципи пізнання і діяльності.

На основі світобачення, основою якого є поняття матерії, енергії, інформації, виникає нова оцінка людиною свого оточення і свого життя у світі,

виявляється нова система сенсів і цінностей, виробляються нові принципи уявлень про благо, істину, красу, користь тощо. У ре-зультаті формуються нові ідеали, орієнтуючись на які людина визначає цілі і завдання життя, пізнання, практичне перетворення світу та себе. Усе це містить світогляд, на основі його вироб-ляється життєва позиція людини. Світогляд є соціальною, культурно-історичною освітою і осо-бисто визначає спрямованість особистості. Основа світогляду — науковий світогляд, значна роль у формуванні якого разом з філософією відводиться інформатиці, як фундаментальній при-родній науці(Д. Колін).

Ефективна організація інформаційної освіти можлива при дотриманні таких підходів [3]:

- куль-турологічного, який базується на усвідомленні глибокої взаємодії категорій «інформація» та «культура», на уявленні про те, що інформаційна культура є невід'ємною складовою загальної культури людини. З позицій культурологічного підходу, інформаційна культура закладає світо-глядні установки особистості; формує її ціннісні орієнтації щодо інформації як елемента куль-тури; перешкоджає дегуманізації та заміні духовних цінностей досягненнями, зумовленими на-уково-технічним прогресом і безпрецедентним зростанням та розвитком нових інформаційних технологій в інформаційному суспільстві. Культурологічний підхід застосовано в аналізі інфор-маційної культури як процесу і результату культурної діяльності, культурної творчості (інфор-мація, її перехід у знання, комунікація, нові типи зв'язків, інформаційні технології, віртуальна реальність), їх вплив на менталітет, сферу освіти.
- Філософсько-культурологічний підхід є базовим для дослідження суті, динаміки інформацій-ної культури, її ролі в системі вищої освіти й освітніх структур, у формуванні особистості (на-приклад, студента) і його соціалізації в період навчання.
- Філософський підхід визначає інформаційну культуру як необхідну умову і спосіб розкриття інтегральної природи людини.
- На культурологічному рівні інформаційна культура особистості є видом культуротворчої діяль-ності з оперативного пошуку інформації, якісної її обробки і позитивного практичного використан-ня в різних системах комунікацій.

Важливу роль відіграє технологічний підхід, який дозволяє розглядати формування інформаційної культури особистості як педагогічну технологію, що містить певну сукупність методів і засобів, котрі забезпечують досягнення заданого результату. Він припускає детальне визначення кінцевого результату й

обов’язковий контроль його точності як основи отримання продукції із заданими параметрами.

Обов’язковими вимогами при цьому є масовість і відтворюваність отриманих результатів. Порушення цих вимог і відсутність хоча б одного елемента в заданому технологічному ланцюзі неминуче призведуть до зниження якості результатів.

В цілому завдання формування інформаційної культури особистості і підвищення масової інформаційної культури суспільства потребують взаємодії системи освіти з такими соціальними інститутами, що традиційно акумулюють інформаційні ресурси суспільства, як бібліотеки і служби інформації.

Засобом, який забезпечує таку взаємодію, повинен стати єдиний методологічний підхід, що передбачає єдність понятійного апарату, знання основних законів функціонування документних потоків інформації в суспільстві, прийомів і методів аналітико-синтетичної переробки інформації, критеріїв ефективного пошуку інформації та інших чинників. При цьому принципо-во важливим є одночасне підвищення інформаційної культури як тих, що навчають, так і тих, хто вчиться. Наприклад: у вищій школі способом формування інформаційної культури особистості повинен стати інтеграційний, діяльнісно-орієнтований, побудований за блоково-модульним принципом спеціальний курс у навчальному плані підготовки бакалавра, фахівця, магістра. Лише спеціальна підготовка, що припускає професійну компетентність, знання особливостей психології та методики викладання спеціального курсу, може дати позитивний результат. При цьому викладачі, що забезпечують проведення за-нять з основ інформаційної культури, повинні мати у своєму розпорядженні необхідні навчаль-но-методичні засоби.

Контрольні питання:

1. Що таке інформація? Назвіть властивості інформації.
2. Що таке дані? Які операції з даними можна виконувати?
3. Назвіть базові компоненти інформаційної культури.
4. Які уміння включають компоненти алгоритмічної культури?
5. Що таке інформаційна культура особистості? Які функції інформаційної культури особистості
6. Що таке інформаційний світогляд?
7. Назвіть підходи ефективної організації інформаційної освіти.

ТЕМА 2. ІНФОРМАЦІЙНІ РЕСУРСИ ТА ІНФОРМАЦІЙНІ СИСТЕМИ

Інформаційні ресурси - це накопичена ІНФОРМАЦІЯ про навколишню дійсність, що зафіксована на матеріальних носіях, які забезпечують передачу інформації у часі й просторі між споживачами для вирішення конкретних завдань.

Функції інформаційного ресурсу

- ❑ Ідентіфікаційна або Довідкова (напр., паспорт).
- ❑ Легітімізаційна (напр., Ліцензія, пропуск, квиток).
- ❑ Пошукова (Знаючи номер, дату, назву наказу, легко знайте сам наказ).
- ❑ Обліково-звітна.
- ❑ Статистична.
- ❑ Інспекторська.
- ❑ Навчальна

Змістовні властивості та ознаки інформаційних ресурсів

1. ***Масивність ІР.***

Інформаційні ресурси - це завжди масиви або сукупність інформації, а не окрема інформаційна одиниця. Наприклад, архіви, фонди бібліотек, бази і банки даних. Однак це не скупчення інформації, не хаотично зібрані інформаційні матеріали.

2. ***Системність або структурованість ІР.***

Як правило, інформаційні ресурси завжди систематизовані, тобто розподілені але за окремими критеріями в залежності від їх споживчих властивостей. ІР завжди являють собою упорядковану сукупність залежно від якої-небудь мети. Причому, вони повинні бути ***логічно*** пов'язані між собою. Наприклад, база даних дисертацій, тобто наукових рукописних праць. Або, наприклад, історичні архівні матеріали.

3. ***Фундаментальна цінність ІР.***

Ця властивість ІР виділяє їх як благо з незамінними якостями.

Фундаментальна цінність проявляється, як мінімум, у чотирьох складових:

• наукової та освітньої діяльності (ІР як знання);

• економічної та виробничої діяльності (ІР як нематеріальні активи підприємств, інтегрований елемент приросту доходу);

• управлінської діяльності (ІР як підстава і забезпечення прийняття рішень);

• духовно-культурній сфері (ІР як бібліотечні, архівні, музейні інформаційні цінності).

4. ***Матеріальна*** (економічна) цінність ІР проявляється в економічному або

вартісному вимірі (тобто можливості матеріальної оцінки з точки зору кількості та якості інформації).

Значне застосування ІР мають в новій галузі людської діяльності - індустрії знань.

Інформаційний продукт та Інформаційний товар

Унаслідок застосування інформаційних технологій до інформаційних ресурсів створюється певна нова інформація або інформація в новій формі. Це продукція інформаційних систем та інформаційних технологій, яка називається інформаційними *продуктами і послугами*.

Інформаційний продукт - інформація, що представляє собою результат діяльності або забезпечує інформаційну діяльність, створена і представлена у формі, придатній для споживання.

Інформаційний товар - інформація, створена і представлена у формі, придатній для обміну, продажу або споживання.

Інформаційні продукти і товари включають:

• інформацію (знання, дані, інформаційні матеріали);

• носії інформації;

• інформаційні засоби (технічні та технологічні).

Інформаційна послуга

Інформаційна послуга - область людської діяльності, спрямована на надання інформаційних продуктів в користування споживачам.

Типовою інформаційною послугою є надання доступу до інформаційно-телекомунікаційних мереж, а також діяльність з прийому, передачі, доставку повідомлень по лініях електрозв'язку або поштових відправлень.

Таким чином, продуктом, товаром або послугою є не інформація в її образному сутнісному розумінні, а окремі різновиди інформаційних ресурсів, які завжди мають яку-небудь соціально-економічну цінність.

Види інформаційних продуктів та послуг

Рис. 1 Види інформаційних продуктів та послуг

***Апаратні засоби*:**

– ЕОМ, міні-ЕОМ, індустріальні комп'ютери, портативні комп'ютери, гральні автомати, програмні приставки; комплектуючі (модулі пам'яті, процесори, материнські плати, монітори, комплектування для периферії, оргтехніки) і т.д.

– мережеве обладнання (обладнання для ЕОМ, сервери, телефони, факси, модеми, міні АТС, супутниковий зв'язок);

– оргтехніка (копіювальна, розмножувальна, обладнання для презентацій, калькулятори, записники, банківське обладнання, диктофони, торговельне обладнання, системи захисту інформації, обладнання для роботи з пластиковими картками, витратні матеріали).

Програмні продукти:

– системне програмне забезпечення (операційні системи, системи програмування, офісне програмне забезпечення, лінгвістичне програмне забезпечення, системи управління базами даних, автоматизовані системи управління підприємством, антивірусне програмне забезпечення, програми захисту);

– прикладне програмне забезпечення (мережеве програмне забезпечення, комунікаційне програмне забезпечення, програмне забезпечення для Інтернет, інформаційно-пошукові системи, комп'ютерна графіка, мультимедіа, навчальні, ігрові програми, видавничі систем).

Інформаційні продукти:

– фотодокументи: діапозитив, мікрофільм, мікрокарта тощо; магнітні фонограми для запису зображення та звуку;

– електронні документи: дискети, диски, мікросхеми, картки флеш-пам'яті тощо.

Інформаційна система (ІС)

Інформаційна система (ІС) – це система, яка організує зберігання і маніпулювання інформацією про проблемну область. Під терміном «маніпулювання» маються на увазі процедури збору, обробки, пошуку, передачі інформації, необхідної в процесі прийняття рішень в будь-якій області. У основі функціонування будь-якої системи лежить процес, а в основі інформаційної системи – процес виробництва інформації. Тому призначення інформаційної системи – це виробництво інформації для потреб організації в забезпеченні ефективного управління її діяльністю.

Інформаційна система — взаємозалежна сукупність засобів, методів і персоналу, які використовуються для зберігання, обробки йподання даних, відомостей з метою вирішення користувачем окреслених завдань

Процеси, що забезпечують роботу інформаційної системи будьякого призначення, умовно можна представити у вигляді схеми, що складається з блоків (Рис. 6):

Рис. 2 Інформаційна система

– введення відомостей, даних із зовнішніх або внутрішніх джерел;

– опрацювання вхідних матеріалів й подання їх у зручному вигляді;

– виведення результатів опрацьованих матеріалів, або передача в іншу систему;

– аналіз отриманих результатів;

– зворотній зв'язок — відомості, які опрацьовані та проаналізовані для корекції вхідних даних.

Інформаційна система має такі властивості:

– будь-яка інформаційна система може піддаватися аналізу, бути побудована й керована на основі загальних принципів побудови систем;

– інформаційна система є динамічною і може розвиватися;

– при побудові інформаційної системи необхідно користуватися

системним підходом;

– вихідною продукцією інформаційної системи є відомості, на основі якої приймаються рішення;

– інформаційну систему потрібно сприймати як систему обробки даних [4].

Види інформаційних систем (ІС)

Залежно від сфери застосування виділяють наступні види інформаційних систем:

1. Наукові ІС призначені для автоматизації діяльності науковців, аналізу статистичної інформації, управління експериментом.

2. ІС автоматизованого проектування або САПР – системи автоматизованого проектування (CAD/CAM – Computer Aided Design / Computer Aided Manufacturing) призначені для автоматизації функцій інженерів-проектувальників, конструкторів, архітекторів, дизайнерів при створенні нової техніки або технології.

Такі ІС допомагають здійснювати: розробку нових виробів і технологій їх виробництва; різні інженерні розрахунки (визначення технічних параметрів виробів, витратних норм — трудових, матеріальних і т. ін.); створення графічної документації (креслень, схем, планувань); моделювання проектованих об'єктів; створення програм, що управляють, для верстатів з числовим програмним управлінням.

3. Інформаційні системи організаційного управління призначені для автоматизації функцій управлінського персоналу. Враховуючи найбільш широке застосування і різноманітність цього класу систем, часто будь-які інформаційні системи розуміють саме в даному тлумаченні. До цього класу відносяться інформаційні системи управління як промисловими підприємствами, так і непромисловими організаціями (банки, біржі, страхові компанії, готелі і т. ін.) і окремими офісами (офісні системи).

4. ІС управління технологічними процесами або АСУТП – автоматизовані системи управління технологічними процесами (SCADA – Supervisory Control And Data Acquisition) призначені для автоматизації різних технологічних процесів (гнучкі виробничі процеси, металургія, енергетика і т. ін.).

5. Інтегровані (корпоративні) ІС використовуються для автоматизації всіх функцій фірми і охоплюють весь цикл робіт від проектування до збуту продукції.

6. Локальні системи призначені, в основному, для автоматизації обліку за одним або декількома напрямами (бухгалтерія, збут, склади, персонал і т. ін.).

Локальною системою може скористатися практично будь-яке підприємство, що потребує управління фінансовими потоками і автоматизації облікових функцій.

7. Фінансово-управлінські системи (малі інтегровані системи). Такі системи гнучко настроюються на потреби конкретного підприємства, добре інтегрують діяльність підприємства і призначені, насамперед, для обліку й управління ресурсами невиробничих компаній. Хоча у багатьох системах даного класу присутні базові можливості управління виробництвом. Як правило, вони універсальні, функціональні можливості таких систем ширші, ніж локальних.

8. Середні інтегровані системи призначені для управління виробничим підприємством й інтегрованого планування виробничого процесу. Облікові функції пропрацьовано глибоко, але вони виконують допоміжну роль.

9. Великі інтегровані системи відрізняються від середніх набором вертикальних ринків і глибиною підтримки процесів управління великими багатофункціональними групами підприємств (холдингами або фінансово-промисловими угрупованнями). Такі системи мають найбільшу функціональність, включаючи управління виробництвом, управління складними фінансовими потоками, корпоративну консолідацію, глобальне планування і бюджетування тощо.

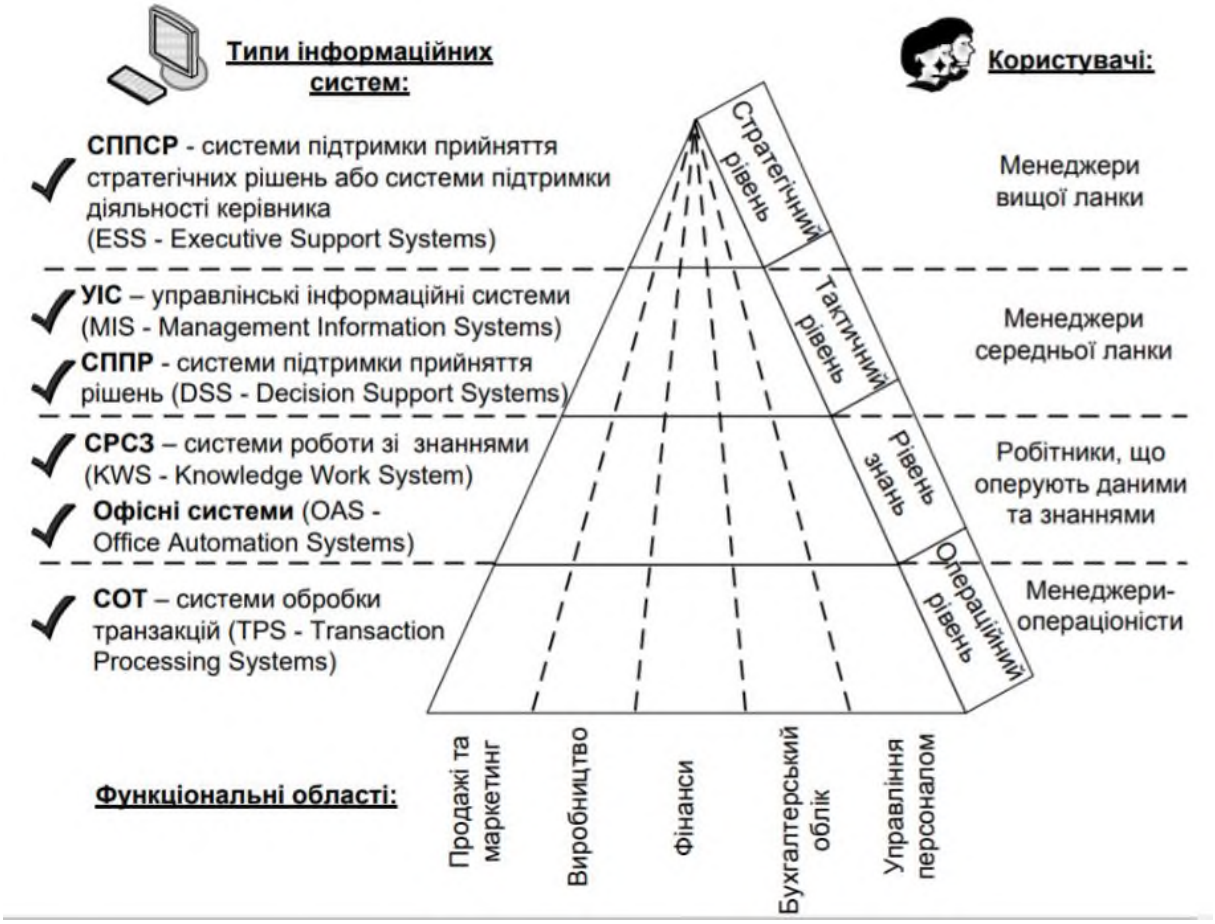

Рис. 3 Типи інформаційних систем

Операційний (експлуатаційний) рівень. Клас ІС на цьому рівні – системи обробки транзакцій (СОТ). ІС даного рівня підтримує фахівців-виконавців, обробляючи дані про господарські операції (рахунки, накладні, зарплату, кредити, потік сировини і матеріалів). Призначення ІС на цьому рівні – відповідати на запити про поточний стан підприємства і відстежувати потік операцій в організації, який відповідає оперативному управлінню.

До інформаційних систем оперативного рівня відносяться: складський облік; торговельний зал; банківські депозити; обробка замовлень; продаж авіаквитків; зарплата і т. Ін

Рівень знань. Клас ІС на цьому рівні – системи роботи зі знаннями (СРЗЗ) і офісні системи. ІС цього рівня допомагають фахівцям, що працюють з даними, підвищують їх продуктивність і продуктивність роботи інженерів і проектувальників. Завдання подібних інформаційних систем — інтеграція нових відомостей в організацію і допомога в обробці паперових документів. Такі системи, особливо у вигляді робочих станцій і офісних систем, найшвидше розвиваються сьогодні в бізнесі.

Системи роботи зі знаннями вбирають в себе знання, необхідні інженерам, юристам, ученим при розробці або створенні нового продукту. Їх робота полягає в створенні нової інформації і нового знання.

Так, наприклад, існуючі спеціалізовані програмні продукти для інженерного і наукового проектування дозволяють забезпечити високий рівень технічних розробок. Як приклади відомих програмних продуктів із формування і управління корпоративними знаннями можна назвати: продукт «Microsoft SharePoint Portal» як засіб управління знаннями; система формування і управління знаннями Excalibur Retrieval Ware групи компаній АСК; лінійка продуктів eDOCS компанії Hummingbird.

Тактичний рівень (або рівень менеджменту). Клас ІС на цьому рівні – управлінські ІС (УІС) та системи підтримки прийняття рішень (СППР). Інформаційні системи даного рівня використовуються працівниками середньої управлінської ланки для моніторингу (постійного стеження), контролю, прийняття рішень і адміністрування.

Стратегічний рівень Клас ІС на цьому рівні .– системи підтримки прийняття стратегічних рішень (СППСР) (інша назва – системи підтримки діяльності керівника). У зв'язку з переходом до ринкових відносин питанню стратегії розвитку і поведінки фірми стали приділяти велику увагу. Це сприяло корінній зміні в поглядах на інформаційні системи. Вони стали розцінюватися як стратегічно важливі системи, які впливають на зміну вибору цілей організації, її

завдань, методів, продуктів, послуг, дозволяючи випередити конкурентів, а також налагодити тіснішу взаємодію зі споживачами і постачальниками. Системи підтримки прийняття стратегічних рішень— це ІС, що забезпечують підтримку прийняття рішень стосовно реалізації стратегічних (перспективних) цілей розвитку організації.

Контрольні питання

1. Що таке інформаційні ресурси?
2. Класифікація інформаційних ресурсів?
3. Змістовні властивості та ознаки інформаційних ресурсів?
4. Дайте визначення поняттям **Інформаційний продукт, Інформаційний товар, Інформаційна послуга.**
5. Що таке інформаційна система?
6. Види інформаційних систем?

ТЕМА 3. ІНФОРМАЦІЙНІ ВІЙНИ

Комунікаційна сфера взагалі і засоби масової комунікації в тому числі завжди були активними учасниками збройних конфліктів. В наш же час виникнення таких понять як «інформаційна війна», «інформаційна безпека» свідчить про тісний зв'язок сучасної боротьби на інформаційному полі та безпосередньо військових дій.

В наш час засоби масової інформації відіграють все більшу роль як в вирішенні збройних конфліктів, так і безпосередньо в їх ході. Журналісти вже стали третьою стороною майже кожного озброєного конфлікту, та від того яку сторону вони підтримують залежить і результат його вирішення. На думку вчених, які досліджують вплив інформаційних процесів на хід сучасних озброєних конфліктів «політичні, ідеологічні та геополітичні погляди формуються у значної частини суспільства виключно на основі телекомунікації. Мас-медіа в сучасному суспільстві відіграють вже не суто допоміжну роль, як раніше, а й стають сильним самостійним фактором, що здатен здійснювати вагомий вплив на історичні долі народів».

В даний час Інтернет все активніше і масштабніше використовується в інтересах інформаційного протиборства сторін, що є учасниками різноманітних конфліктів. Інтернет надає широкі можливості щодо надання впливу на формування суспільної думки, прийняття політичних, економічних та воєнних рішень, дії на інформаційні ресурси супротивника та розповсюдження спеціально підготовленої інформації або дезінформації. Неврегульованість правових відносин при розповсюдженні інформації в Інтернет призводить за собою повну свободу розповсюдження будь-якої, в тому числі і заздалегідь недостовірної інформації. Все це призводить до того, що факти тієї чи іншої події можуть бути суттєво викривлені. Такі засоби допомагають дозволити досить широкому колу зацікавлених осіб чи груп реалізувати складний процес регулювання суспільного сприйняття чи організовувати пропагандистські компанії для підриву довіри до певної політичної сили, уряду та інше. Разом з впливом на формування суспільної думки, на позиції офіційних осіб, що приймають важливіші рішення, використання глобальної мережі для деструктивних дій може привести до порушення нормальної роботи чи довготривалому виводу з ладу життєво важливих об’єктів і систем в окремих районах, країнах чи регіонах.

Також, однією з переваг Інтернету в даному контексті є те, що розміщення і регулярне оновлення інформації на сторінках, форумах і конференціях не потребує значного часу на підготовку матеріалів в електронному вигляді. При

цьому користувачі отримують її в режимі реального часу. Крім того, цілеспрямована дія на інформаційні ресурси протидіючої сторони може здійснюватися не тільки в запланований час, але й по мірі виникнення необхідності.

Таким чином на думку Л. Польских, розвиток глобальної мережі Інтернет супроводжується все більш широким використанням наданих нею можливостей для здійснення інформаційного протиборства, ростом координації, масштабів та складності дій її учасників, в якості яких виступають як держави чи їх коаліції, так і окремі організовані групи. Об'єктом інтернет-нападів все частіше стають інформаційні ресурси, виведення з ладу чи ускладнення функціонування котрих може нанести протидіючій стороні значний економічний збиток чи визвати великий суспільний резонанс. [6]

Під інформаційною війною розуміють всеохоплюючу і цілісну стратегію, обумовлену зростаючою значущістю і цінністю інформації в питаннях політики, економіки, оборони та безпеки держави.

Спрямованість інформаційного впливу

Виділяють наступні категорії спрямованості інформаційно-психологічного впливу:

- інформаційні війни між державами;
- інформаційні війни між фінансово-промисловими групами;
- інформаційні війни між владою і фінансово-промисловими групами;
- інформаційні війни між владою й опозицією, які, в свою чергу, підтримують певні фінансово-промислові групи (іноземні держави);
- інформаційні війни, інспіровані протистоянням різних сегментів влади, які підтримують різні фінансово-промислові групи (іноземні держави).

Форми ведення інформаційної боротьби

Основними формами ведення інформаційної боротьби є:

- *інформаційний вплив* - це організоване застосування сил і засобів інформаційної боротьби для розв'язання завдань завоювання (підтримання) інформаційної переваги над протилежною стороною;
- *інформаційна атака* являє собою сукупність активних інформаційних впливів сил і засобів окремих підрозділів на елемент або групу елементів інформаційних систем сторони, що протистоїть, з метою виконання поодиноких тактичних завдань інформаційної боротьби;
- *інформаційна битва* - це сукупність об'єднаних спільним задумом інформаційних впливів і атак, які проводяться спеціально виділеними силами й за-

собами та спрямовані на виконання одного оперативного завдання інформаційної боротьби;

- *інформаційна операція* - сукупність узгоджених за метою, завданням, місцем і часом інформаційних впливів, атак і битв, які здійснюються за єдиним задумом і планом для виконання завдань інформаційної боротьби на стратегічному чи оперативному напрямку.

Інформаційна зброя і технології її використання

Особливості інформаційної зброї.

Інформаційна зброя принципово відрізняється від усіх інших засобів ведення війни тим, що з її використанням можна вести неоголошені і найчастіше невідомі світу війни. Особливої небезпеки інформаційній зброї надає багатоваріантність форм і способів її застосування, потайливість і радикальність впливу, висока економічність використання.

Види інформаційної зброї

- засоби масової інформації та спеціальні засоби інформаційно-пропагандистської спрямованості;
- глобальні комп'ютерні мережі й програмні засоби розповсюдження в них пропагандистських інформаційних матеріалів;
- засоби, що нелегально модифікують інформаційне середовище, на підставі чого людина приймає рішення;
- засоби створення віртуальної реальності;
- чутки;
- засоби підпорогового психосемантичного впливу;
- засоби генерування акустичних та електромагнітних полів.

Пропагандистські прийоми і методи

1) *використання незаперечних істин.* Наприклад, до певного часу всі вважали, що Сонце обертається навколо Землі, тому ідеї Г.Галілея сприймалися як щось не тільки неправдоподібне, а й нерозумне;

2) *посилання на авторитет.* Будь-яка культурна, а тим більше наукова традиція базується на авторитеті;

3) *звернення до загальновживаного* - усі так міркують;

4) *використання гри слів,* зокрема, гра семантичними контекстами, заміна негативно забарвлених висловів на позитивні та навпаки. Приклад: моджахеди (борці за віру) - душмани (бандити).

Функції інформаційного впливу під час інформаційної боротьби

- виявляти воєнний, економічний, політичний і культурний потенціал;
- протидіяти будь-яким видам розвідки противника;

- спотворювати, руйнувати, нейтралізувати, знищувати чи захищати інформацію;
- забезпечувати комп'ютерне відтворення реальної чи віртуальної неадекватної обстановки та візуалізації поля бою;
- здійснювати інформаційно-психологічний, легальний або нелегальний фізичний вплив на особовий склад, об'єкти, бойову техніку, зброю, лінії зв'язку й управління;
- концентруватися на демонстративних діях і введенні в оману;
- виконувати радіоелектронне придушення;
- знижувати помітність об'єктів, бойової техніки та зброї;
- захищати особовий склад, об'єкти, бойову техніку, зброю, органи управління та різні радіоелектронні засоби від впливу на них електромагнітної чи іншої спрямованої енергії;
- відводити самонавідну зброю від найбільш важливих цілей та ін.

Способи ведення боротьби

- Можна поділити на *три основні категорії способів*:
- *силові,* до яких належать способи, які базуються на застосуванні традиційних способів боротьби і зброї до об'єктів інформаційної боротьби різних видів. Застосування силових способів дає змогу досягти інформаційної переваги в обсязі інформації, необхідної для виконання управління військами (силами);
- *інтелектуальні способи* мають на меті реалізацію рефлексивного управління противником. Їх застосування робить можливим досягнення переваги на основі інформації, яка використовується для управління військами (силами);
- *до комбінованих* належать способи, що забезпечують досягнення інформаційної переваги як в обсязі, так і якості інформації про поточну обстановку.

Особливості інформаційної боротьби

Ефективності реалізації технологій інформаційного впливу значною мірою сприяють особливості інформаційної інфраструктури, а саме:

- простий доступ до неї;
- розмитість кордонів, міжконтинентальний характер і, як наслідок, практична неможливість чіткого розмежування внутрішніх і зовнішніх джерел загрози для безпеки країни;
- можливість маніпуляції інформацією та управління її сприйняттям (мережа Internet може виступати засобом поширення пропагандистських матеріалів різної спрямованості для політичної підтримки своєї діяльності, дезінформації, впливу на суспільну думку, підрив довіри громадян до уряду тощо);

- недостатність інформації щодо реальних і потенційних загроз національним інтересам і каналів їх реалізації;
- надзвичайна складність оперативного запобігання інформаційному впливу та оцінювання реального і ймовірного збитку;
- невизначеність, зумовлена тим, що події, зовні схожі з наслідками ведення інформаційних операцій проти держави, можуть бути лише наслідками дій «хакера-одинака» або несприятливого збігу обставин.

Сучасні методи та прийоми, що використовуються в інформаційних війнах

Методів і правил пропаганди існує безліч. Їхні переліки можна знайти в багатьох виданнях. Наведемо деякі з них:

- *Голодування.* Ефективний прийом емоційного впливу на електорат і психологічного тиску на владу;
- *«Тримай злодія».* Ціль прийому - змішатися з Вашими переслідувачами. Цей же прийом використовується і для дискредитації, коли винні, почуваючи провал, першими здіймають галас і спрямовують гнів народу в інший бік.
- *Ефект ореолу.* базується на психологічній властивості - мислити аналогіями. Складається з двох розповсюджених стереотипів-оман. Перший стереотип - «поруч - значить разом». Іншими словами, перебування поруч зі знаменитою або високопоставленою особою підвищує статус в очах навколишніх. Другий стереотип засвідчує: люди, які досягли вагомих успіхів у якійсь конкретній сфері, в очах оточуючих виглядають здатними на більше і в інших справах.
- *Ефект первинності.* Й.Геббельс ввів у сучасну пропаганду один із ключових принципів: людина, яка сказала світові перше слово, завжди має рацію.
- *Ефект присутності* - це ряд трюків, які повинні імітувати реальність. Їх постійно використовують під час «репортажів з місця подій» або в кримінальній хроніці, фабрикуючи заднім числом зйомку «реального» захоплення злочинців або автокатастрофи.
- *Інформаційна блокада.* Позбавити противника можливості привселюдно висловити свою позицію - одне з головних завдань пропагандистської війни.
- *Відвернення уваги.* Повідомлення, спрямовані проти деякої думки або установки, стають більш ефективними, якщо в момент їхньої передачі одержувача відволікають від змісту повідомлення.
- *«Очевидці» події.* Дуже ефективний прийом. Опитується багато випадкових людей, зі слів яких формується необхідний значеннєвий ряд. Особливо сильний ефект справляють крикливі баби, заплакані діти, молоді інваліди.

Сучасні методи та прийоми, що використовуються в інформаційних війнах

- *Переписування історії.* Метод ефективний у тривалій перспективі, коли потрібно поступово формувати потрібний світогляд.
- *Повторення* - головний засіб несумлінної пропаганди. Тому воно служить гарною ознакою її наявності. Коли раптом починають щодня мусолити одну і ту ж тему і вживати одні й ті ж словесні конструкції - справа нечиста.
- *Підміна* - це один з варіантів горезвісних «подвійних стандартів».
- *Напівправда.*
- *Принцип контрасту.* На тлі злих і несправедливих людей добра людина завжди сприймається з особливою симпатією.
- *Сенсаційність або терміновість.* Під прикриттям сенсації можна або замовчувати важливу подію, про яку публіка знати не повинна, або припинити скандал, який стався - але так, щоб про нього більше ніхто не згадував.
- *Зсув акцентів.* Використовується, наприклад, при повідомленні останніх новин.
- *Створення асоціацій.* Об'єкт в очах громадськості штучно прив'язується до чого, що сприймається масовою свідомістю як дуже погане (або навпаки - хороше). «Сталін - це Ленін сьогодні» (радянська пропаганда); «С.Хусейн - арабомовний Гітлер» (американська пропаганда);
- *Створення загрози.* Головне завдання - за будь-яку ціну змусити боятися. Деморалізовані та залякані люди роблять або хоча б схвалюють дії, які їм зовсім не вигідні.

Контрольні питання:

1. Які існують форми ведення інформаційної боротьби?
2. Назвіть особливості інформаційної зброї.
3. Які існують види інформаційної зброї?
4. Назвіть пропагандистські прийоми і методи.
5. Які існують сучасні методи та прийоми, що використовуються в інформаційних війнах?
6. Назвіть функції інформаційного впливу під час інформаційної боротьби.

ТЕМА 4. ВИКОРИСТАННЯ ЗМІ В ІНФОРМАЦІЙНИХ ОПЕРАЦІЯХ

Принципи використання ЗМІ для використання інформаційних війн:

- конструюється «множинність думки» за допомогою фактів, розповідей, відтак створюється враження, що про це говорять усі;
- на другому етапі газети (вечірні та ранкові) висловлюють уже більш визначену думку про подію, що сталася, супроводжуючи її «очікуваними результатами» і, тим самим, «думки пересічних громадян починають згущатися у тверду масу»;
- на третьому етапі в суперечках відкидаються аргументи на користь одного визначеного і незмінного рішення;
- четвертий етап - впровадження факту або оцінки події, що видається за загальне «переконання» в інтересах пересічних громадян.

Коментарі

- Практично коментар є маніпуляцією. До *маніпуляцій* відносяться спеціальні дії для формування стереотипів і створення певного враження або ставлення до того чи іншого факту, події. Способи маніпулювання суспільною думкою спираються на використання законів психології, некритичного сприйнятті, політичної недосвідченості, міфів.
- Створення образу слабкого ворога і сильного свого.
- Гордий чеченець, слабкий російський солдат.
- Сильний козак – лях боягуз.
- Сигнали – однім боротися -
- Іншим здаватися.

Фреймінг

- Наголос робиться на вибірковість уваги людини. Так. наприклад, інформація, надрукована в газеті дрібним шрифтом, не привертає такої уваги, як надрукована великим або жирним шрифтом. Інформація, розміщена на першій і останній сторінках газети, має значно більше шансів привернути увагу читача, ніж розміщена на внутрішніх сторінках. Цього ж ефекту досягають і розміщенням поруч із «неважливою» інформацією помітного матеріалу або фотографій.
- На радіо- і в телепередачах зниження важливості інформації досягається тим, що повідомлення ставлять наприкінці передачі. Тут враховується те, що люди, як правило, асоціюють важливість інформації з порядком її викладу. Новини на телеекрані ранжуються завжди в залежності від їхньої значущості. Телеведучі часто використовують негативні теми і повідомлення для того, щоб

домогтися визначеного результату, наприклад, новині програми телеканалів дуже часто починаються з негативних подій.

Як розкрутити мляву, але бажану тему

Інформаційний шум щільною стіною встає на шляху будь-якої новини, яку журналіст намагається «проштовхнути» через канали ЗМІ і «впровадити» у сферу актуальної суспільної свідомості. Важливо не лише «побороти» інформаційний шум і вивести свою новину на орбіту масової комунікації. Необхідно домогтися, щоб ця новина протрималася на цій орбіті максимально довго, тобто щоб тема «крутилася».

Інформаційний шум

В умовах інформаційного шуму практично неможливо «запускати» на орбіту суспільної уваги «важкі» теми, навантажені пропагандистським змістом і насичені суб'єктивними журналістськими емоціями. Тому потрібно вибрати з маси елементів лише ті найбільш яскраві і «гострі» тематичні фрагменти пропагандистської інформації, яким можна надати видимість об'єктивного факту, суспільно-значущої новини або сенсаційності для привернення читацької уваги. В такий спосіб відбувається своєрідне трансформування теми в більш дешевий і « солодкий» інформаційний продукт.

Це можна здійснити трьома способами:

- *тема вище особи* - пропагуємо не персональний імідж, а пов'язані з ним теми;
- *факт вище думки* - використовуємо лише ті тематичні фрагменти пропаганди, які за зовнішніми ознаками можуть подаватися як такі, що мають суспільну інформаційну цінність;
- *сенсація вище емоції* - використовуємо лише ті тематичні фрагменти, які мають виражений потенціал «сенсаційності». Мова йде не про «сенсації» у кращому розумінні цього слова (ексклюзив, гарячі новини, викриття, великий скандал), а про так званий «дух сенсаційності».

Вказані трансформації здійснюються за допомогою таких прийомів:

1) *Солодкий контекст.* Публікуємо серію матеріалів на тему, яка заявлена « дружнім» кандидатом як ключова тема його передвиборної кампанії. При цьому принципово важливо жодного разу (!) не згадати даного кандидата.

2) *Закладання шашок.* Приклад: якщо «улюблений» кандидат N планує днями різко виступити проти возз'єднання України з Польщею, необхідно до появи цієї заяви опублікувати серію матеріалів про жахи майбутньої інтеграції, бідність у Польщею, жахливу епідемію грипу в Варшаві і загрозу її поширення на схід. При цьому не можна жодним словом обмовитися про кандидата № I

лише добре підготувавши суспільну думку, друкуємо статтю «Кандидат N Протестує Проти Жахів Інтеграції з Польщею».

3) *Завищення інформаційного приводу.* Приклад: поважна газета (на відміну від рекламного проспекта) не може просто так, голослівно, затверджувати, що «кандидат А - високоморальна і віруюча людина». Потрібно цю ідею зробити актуальним об'єктом, знайшовши для цього придатний інфопривід: або програмний («кандидат А хоче ввести обов'язкову молитву в школах»), або кампанійний («кандидат А виступив на мітингу в недільній школі»), або особистісний («кандидат А заборонив своїй дочці робити аборт»).

3.1) *Кластеризація (деталізація).* Замість того, щоб викладати всю програму кандидата, ми «подрібнюємо» її на тематичні фрагменти, кожен з яких можна логічно «прив'язати» до інтересів конкретного соціального, культурного, національного, релігійного, вікового, професійного зрізу населення. Американці називають ці «осередки» електорату «кластерами». Звідси і назва прийому: «кластеризація» програми кандидата. Приклад: «План підкупу кожної категорії виборців. Що потрібно зробити для американців ірландського походження? - Випити з ними пива. - Що для китайців? - Провести вечір у Чайна-тауні. - Для євреїв? - Вибрати правильний момент для поїздки в Єрусалим. - Які слова знайти для медиків, перукарів, а які - для жінок-вчених?»

3.2) *Анімація (пожвавлення).* Замість кампанійного інфоприводу використовуємо особистісний: спробуємо глянути на кандидата «як на особистість» навіть у той момент, коли він просто виконує рутинну роботу. Приклад: президенту потрібно «просунути» тему необхідності війни в Албанії, тому його літак спеціально садять в місті, де йде дощ, щоб він міг, спустившись з трапу, зняти плащ і накинути його на плечі літньої «албанки», яка «випадково» опинилася в натовпі.

4) *Канонізація соцопитування.* Посилання на всілякі опитування допомагають журналістам вирішувати завдання позитивної пропаганди;

5) *Канонізація фокус-групи.* Примітивну «фокус-групку» можна створити прямо в редакції, кафе чи пивному барі. Приємно, що ніхто і ніколи не змусить вас включити в кишенькову «фокус-групу» людину із «незручною» думкою;

6) *Пластиковий експерт.* Дозволяє маскувати пропаганду в строгих формах «авторитетної думки» якого-небудь експерта. Експерти з великим задоволенням відгукуються на будь-який дзвінок з редакції солідного видання.

7) *Наша людина в натовпі.* Під час показу маніфестацій загострюється пропагандистська насиченість «випадкових» деталей, «вдало помічених» окремих образів, вихоплених «з глибин народного моря».

8) *Бокс попупи («splendid generalities»)*. Замість того, щоб прямо і чесно висловити власну думку, журналіст прикривається загальними словами: «як свідчить загальна думка», «для всіх українців», «сьогодні Україна розуміє», «Воля», «Демократія», «Незалежність», «Цивілізація», «Західна культура», «Майбутнє», «Наші діти» тощо.

9) *Штучний супутник.* Це будь-яка знаменитість, яка погодилася трохи «покрутиться» на орбіті передвиборного іміджу нашого улюбленого політика - тобто підтримати його і привселюдно похвалити в пресі.

10) *Фальшивий витік.* Посилання на горезвісні «добре поінформовані» анонімні джерела.

Як непомітно «задушити» небажану тему

1) *Глушилка.* «Глушіння» небажаної теми можна здійснювати двома способами: паралельно і послідовно. При паралельному глушінні ми оточуємо невеликий матеріал з коротким звітом про небажану подію кількома об'ємними публікаціями на суміжну («дисонуючу») тему. Послідовне глушіння здійснюється в рамках окремої статті - спочатку коротко заявляється небажана тема, потім різко звучить суміжна дисонуюча тема.

2) *Заниження інфоприводу.* Якщо інформаційний привід для публікації слабкий, краще відмовчатися. Однак коли «противник» усетаки розродився «гарячою» рекламною новиною, то нав'язуємо небажаній темі «незручний» інформаційний привід.

2.1) *Програмування (замуровування).* Немає нічого страшного за посушливий вітер колючих цифри. Чим більше цифр, тим краще.

2.2) *Театралізація подвигу (шельмування).* Якщо «недружелюбний» нам кандидат намагається організувати яскраву подію «як особистість» (знімає плащ і накриває ним жінок похилого віку, які стоять у натовпі під дощем), то потрібно впевнено і різко переводити тему в кампанійний інфопривід: «усе, що відбулося - лише частина передвиборного шоу!»

Як м'яко «переламати» небажану тему

- Ми не просто «перекриваємо» голос далекого ньюсмейкера, «викрикуючи» будь-яку іншу інформацію із суміжної теми. Силове «переламування» теми припускає, що журналіст відгукується на небажану тему конкретними контраргументами.
- *Ложка меду.* Найпоширеніший вид «ложки меду» - це так зване «розкрити очі». Спочатку автор статті вдає, що підтримує небажану ідею, заявлену в першому абзаці - і лише в процесі заглиблення в тему починає сумніватися в її

правильності, а на кінець статті, зрозуміло, приходить до остаточного засудження «ворожої» тези.

- *Шекспірівський сонет.* Журналіст спочатку довго і завзято розвиває тему в невигідному для себе ключі (наприклад, критикує). Однак він береже «на потім» деякий найсильніший (єдиний!) контраргумент, який «закладається» у останню фразу статті - і це вмить «перевертає» зміст усього сказаного раніше з ніг на голову!
- *Фонтан бруду (заборонений).*
- *Групове зґвалтування*. Фокус-групу краще застосовувати не для «розкручування» тем, а саме для їх «переламування».
- *Ворог народу.* Прийом має два різновиди. В першому випадку автор статті посилається на думку конкретної більшості. Другий варіант - ототожнення позиції журналіста з позицією абстрактної більшості (народів, нації в цілому, «всіх розумних людей»).
- *Сонячне затемнення.* Запрошена зірка може мимоволі «перехопити» в кандидата увагу глядачів і преси.

Як непомітно підмінити тему

За допомогою технічних прийомчиків цю тему можна підмінити непомітно для читача - отже, «поховати».

- *Фальшивий заголовок.* Тема, заявлена в заголовку, розвиватиметься лише в перших 2-3 абзацах.
- *Переключення стрілок.* При «склеювання» різнопланових фрагментів журналістського тексту перехід на іншу тему: спочатку мова на тему, а після підзаголовка чи фотографії - тема зовсім інша.

Як замаскувати пропаганду (мікрорівневі технології)

«Мікрочастинки» пропаганди - це, насамперед, цитати кандидатів і їхніх консультантів, тенденційні фактики, швидкі коментарі, «шпильки», спеціально відібрані фрагменти. Треба сховати їх у текст «інформаційної» статті.

- *Крапля дьогтю.* Щоб продати публіці цистерну рекламного меду, доводиться додавати краплю дьогтю.
- *Пізанська вежа.* Статті треба будувати за принципом «перевернеої піраміди». Журналісти намагаються «заганяти» вигадку в кінець тексту, маскуючи його під «об'єктивну передісторію питання».
- *Дев'ять з половиною слів.* Розмір кожної конкретної «пропагандистської» цитати не повинен перевищувати... дев'яти слів.

- *Витончений аромат сумніву.* Якщо журналіст, аналізуючи виступ політика, говорить, що «політик думає (стверджує, розраховує, сподівається), що переможе на виборах», то в читача з'являється сумнів щодо цього.
- *Битися писанками (яйцями).* Журналісти «зіштовхують лобом» кандидатів. Створюється ілюзія чесної сутички, але журналіст виставляє позицію «нелюбого» політика ніби «під кутом».
- *Нарізання цитати.* Велика цитата відразу відлякує від теми. Довга цитата подрібнюється на найтонші «зрізи» - причому ідеологічна м'якоть цитати постійно перемежовується «жирними» абзацами непрямого цитування.

Пропагандистські прийоми телевізійної пропаганди

Активні дослідження прийомів телевізійної пропаганди розгорнулися в США в 70-х роках. Аналізуючи американське телебачення початку 70-х років XX ст., Е.Ефрон визначила наступні характерні пропагандистські прийоми:

- *Читання думок.* Журналіст читає думки пересічних людей, але насправді вкладає в їхні вуста свої міркування.
- *Анонімність.* Полягає у використанні анонімного або фактично анонімного джерела повідомлень.
- *Вилучання.* Суть прийому зводиться до фільтрування думок співрозмовника. Розрізняють чотири типи вилучань:
- *відхилення.* Ведучий стверджує, що надає слово обом сторонам, тоді як у повідомлення потрапляє лише одна;
- *перспектива.* Висвітлюючи певний конфлікт, комунікатор надає слово лише одній стороні;
- *підміна.* Полягає у використанні слабких, сприятливих визначень для позначення насильницьких дій;
- *останнє слово.* Комунікатор передає зміст дискусії коректно, проте завершує її акцентом на позиції однієї сторони;

4) *Звеличення*

Виокремлюють шість видів «звеличення»:

- *похвала.* Комунікатор позитивно змальовує певну дію або характеристику;
- *придушення негативу;*
- *найменування і звеличення негативів.* Для виправдання негативного факту знаходять жорстко позитивно емоціонально закріплені терміни, наприклад «національна гордість», «солідарність трудящих» тощо;
- *ігнорування негативних характеристик.* Використання позитивних епітетів для характеристики людини;

- *збільшення значущості.* Характерний приклад - «іконостас» радянських марксистських вождів (К.Маркс, Ф.Енгельс, В.І.Ленін, Й.В.Сталін) плюс сучасний керівник;
- *обзивання опонентів аморальними особами.* Зміст подібного прийому у використанні моралізаторської критики опонентів.

5) *Приниження*

Існує сім різноманітних видів приниження:

- *пряма атака;*
- *непряма атака;*
- *атака за допомогою подвійного стандарту.* Використовуються спеціальні правила гри для об'єкта звинувачення;
- *гумор, сарказм, сатира, іронія.* Одним із найпоширеніших прийомів приниження є використання гумору;
- *аргумент.* Повідомивши про позицію однієї сторони, журналіст детально її аналізує і розбиває вщент, ніби це робить протилежна сторона;
- *звинувачення за асоціацією.* Об'єкт прив'язується до чогось зовсім поганого, наприклад, фашизму;
- *код.* Не маючи можливості критикувати відкрито, комунікатор звертається до мови Езопа.

6)*Підроблений інтелект*

Штучно створюється враження про нейтралітет комунікатора, який насправді ангажований однією зі сторін. Шість варіантів цих прийомів:

- *фальшивий комплімент;*
- *фальшива критика;*
- *фальшиві серії.* Комунікатор критикує опонентів за схожі помилки, але забуває про критику, коли доходить черга до його протеже;
- *фальшивий прототип.* Комунікатор знаходить представника певної групи і постійно надає йому слово від її імені;
- *напівдебати.* Комунікатор активно і постійно стверджує, що він надає слово обом сторонам. Насправді дозволяє дуже детально висловлювати позицію лише своєму протеже, повністю ігноруючи опонентів;
- *подвійна бесіда.* Комунікатор на початку виступу стисло розповідає про певний позитив щодо опонентів, а потім тривалий час присвячує спростуванню власного твердження.

Повна фальсифікація.

Комунікатор цитує висловлювання (читай позицію) сторони зі значними неточностями і навіть помилками для посилення позицій опонуючої сторони.

8). *Редагування структури*

Психологічний вплив за рахунок структуризації текстів:

- *«отруйний сандвіч «.* Комунікатор подає позитивне повідомлення між негативною передмовою та негативним висновком;
- *«цукровий сандвіч».* Негативне повідомлення маскується позитивним вступом і позитивними висновками;
- *перебільшення деталі.* Комунікатор знаходить, а потім акцентує увагу на маленькій, але негативній, деталі.

9). *Інша техніка:*

- *суперузагальнення.* Комунікатор, не базуючись на об'єктивних фактах, робить надзвичайно широке узагальнення;
- *недоведена теорія.* Прийом ґрунтується на авторитеті наукового знання як такого;
- *навідне запитання.* Репортер запитує співрозмовника, висловлюючи вже сформовану думку щодо проблеми;
- *однослівна журналістика.* Комунікатор використовує одне слово або лаконічну фразу для визначення своєї позиції. Залежно від семантичного потенціалу слова, ним можна передавати як схвальне, так і негативне ставлення.

Форми і напрямки контролю власного інформаційного простору

Вирізняють *дві основні форми жорсткого державного контролю (цензури):*

- *прямий контроль* (цензура у вузькому розумінні), який, в свою чергу, поділяється на попередній і наступний контроль. *Попередній контроль* полягає у тому, що відповідний урядовець (цензор) переглядає пресу до її виходу у світ і дозволяє або не дозволяє публікацію. Прямий *наступний контроль* з використанням засобів судового переслідування застосовується у багатьох сучасних державах;
- *опосередкований контроль* передбачає застосування економічних важелів щодо ЗМІ з метою коригування їхньої політичної лінії.

Відомо три *основні напрямки* розв'язання проблеми *контролю національного інформаційного простору* в нових умовах:

1) встановлення контролю над приймальними пристроями через неможливість встановити повний контроль над засобами передачі інформації, наприклад, у разі їхнього знаходження на території іншої держави;

2) використання методів глушіння радіосигналу, створення перешкод для поширення його інформаційної складової; до цієї групи методів належить і такий

технічний прийом як зміна діапазону поширення радіосигналів (вітчизняний стандарт УКХ і західний БМ не повністю збігаються);

3) ведення контрпропаганди, тобто створення модифікованого інформаційного потоку з метою послаблення, а в ідеалі - повної ліквідації ефекту від пропаганди противника.

Стратегії контпропаганди

Контрпропаганда має бути наступальною, оперативною, конкретною, гнучкою, комплексною і враховувати характеристики аудиторії. Відомо, що найкраща оборона - це наступ.

Вимога наступальності контрпропаганди викликає появу найцікавішої проблеми - яким чином необхідно спростовувати «вигадування» опонента, щоб не сприяти їхньому поширенню.

Існує декілька основних підходів контпропаганди:

1) *Замовчування.* Ця стратегія ефективна за чіткого виконання двох умов:

- дотримання жорсткого контролю за поширенням пропаганди противника і захист аудиторії від впливу пропаганди;
- чітка послідовність замовчування: у жодному з матеріалів немає навіть натяків на ці події.
- Якщо ситуація не задовольняє хоча б одній із вказаних умов, стратегія виявляється вкрай неефективною.

2) *Спростування фактів, вміщених в тексті опонента.* Умовою застосування цієї стратегії є впевненість, що пропаганда дійшла до всіх членів аудиторії і була сприйнята ними. Два основні варіанти спростувань:

- повне і беззастережне (якщо повідомлення опонента від самого початку побудоване на хибних засадах і це можна довести);
- часткове (необхідно чітко збалансувати кількість погоджень з інформацією противника та її заперечень).

3) *Переключення уваги аудиторії на опонента.* В цьому випадку намагаються діяти за принципом «сам дурень». Його ефективність висока лише тоді, коли нова запропонована тема для обговорення набагато гостріша, ніж початкова.

Кібернетична війна як різновид інформаційної війни

Кібернетична війна - це дії, спрямовані на приведення в стан недієздатності комп’ютерних систем збору, опрацювання та розповсюдження інформації, а також оснащених комп’ютерами систем управління збройними силами противника.

Засоби кібернетичної зброї

До *кібернетичної зброї* відносяться засоби, спрямовані на пошкодження:

- комп'ютерних програм та інформації: комп'ютерні віруси, «черв'яки», «троянські коні», логічні бомби, прорахунки в програмах і системах комп'ютерної безпеки (випадкові або навмисні), спеціальні функції чіпів;
- апаратної частини комп'ютерів: мікроскопічні машини і мікроби, які знищують електронні схеми, високоенергетичні мікрохвильові випромінювачі, електромагнітні імпульси.

Види кібернетичної зброї:

1) *Комп'ютерні віруси* - це фрагмент коду, який копіює себе в іншу програму, змінюючи її. Вірус запускається лише тоді, коли починає виконуватися ця програма. Розмножуючи себе, він заражає інші програми. Небезпека комп'ютерних вірусів зростає через доступ більшості комп'ютерів до мережі Інтернет.

2) *«Черв'яки»* - це незалежна програма, яка розповсюджується через повне самокопіювання з одного комп'ютера на інший, найчастіше через мережу. На відміну від вірусів, вони зазвичай не змінюють інших програм. Небезпека «черв'яків» у тому, що вони запрограмовані на знищення інформації в комп'ютері або зниження ефективності роботи комп'ютера.

3) *«Троянські коні»*- це фрагменти коду, які містяться всередині програми і виконують деяку приховану функцію. Цей механізм часто використовують для приховування вірусів або «черв'яків». Троянський кінь може бути замаскований під «корисну програму». «Троянські коні» важко визначити, оскільки вони не спричиняють руйнівного ефекту і майже непомітні в роботі.

4) *Логічні бомби* - це певна функція в програмі (вмонтована розробником або програмістом), або незалежна програма (троянський кінь або вірус), яка активізується за певних умов. Наприклад, такими умовами може стати певний час або існування на комп'ютері документа із деякою назвою (наприклад «Наркотики») з наступною передачею цього файлу Службі безпеки. Крім того, логічні бомби можуть бути активовані ззовні, наприклад, шляхом передачі через електронну пошту певного змісту тощо.

5) *Прорахунки в програмах і системах.* В епоху масового програмного забезпечення, яке випускається на ринок навіть без достатнього тестування на наявність помилок, ці прорахунки не є рідкістю і найчастіше визначаються і виправляються в процесі використання програми. Якщо ж дехто виявив такий прорахунок раніше за розробника, він зможе використати його для отримання конфіденційної інформації без відома користувачів подібних систем. Більше того, прорахунки можуть вмонтовуватися в програми навмисне (спеціально

вмонтовані прорахунки називаються «люками») для отримання можливості в потрібний момент «відключати» комп'ютери.

6) *Спеціальні функції чіпів.* аналогічно до «прорахунків» в програмах, вмонтування аналогічних функцій може здійснюватися і в інтегральні схеми (комп'ютерні мікрочіпи). Сценарії активізації таких функції різноманітні: від певного набору програмних кодів до спеціального радіосигналу на заданій радіочастоті.

7) *Мікроскопічні машини і мікроби.* Мікроскопічні машини (nano machines) - мікроскопічних розмірів роботи, які можуть проникати всередину комп'ютера і спричиняти електронні замикання і псування обладнання. Аналогічні ефекти можуть мати спеціально вирощені мікроби (бактерії, гриби), які, наприклад, можу призводити до швидшого окислення міді на контактних пластинах і відтак зменшення струмопровідності.

8) *Високоенергетичні радіопередавачі* - це пристрої, спроможні випромінювати направлений концентрований радіосигнал високої потужності на певний електронний прилад для виведення його з ладу. Ціллю такого передавача може бути комп'ютер в приміщенні, локальна корпоративна мережа тощо.

9) *Електромагнітні імпульси.* В даному випадку розглядаються електромагнітні імпульси великої потужності, спроможні вивести з ладу електронні пристрої. Джерелом такого імпульсу може бути, наприклад, ядерний вибух. На відміну від високоенергетичних передавачів, електронні імпульси не мають направленого характеру і використовуються для знешкодження не конкретного пристрою, а електронного обладнання на певній території (наприклад, у штабі командування противника).

Контрольні питання:

1. Що таке фреймінг? Для чого він може використаний?
2. Як розкрутити мляву, але бажану тему?
3. Як непомітно підмінити тему?
4. Як замаскувати пропаганду (мікрорівневі технології)?
5. Назвіть види методів звеличення та приниження.
6. Які існують форми і напрямки контролю власного інформаційного простору?
7. Назвіть стратегії пропаганди.
8. Назвіть засоби та види кібернетичної зброї.

ТЕМА 5. АВТОРСЬКЕ ПРАВО

Авторське право, як і право інтелектуальної власності в цілому – це сукупність немайнових (особистих) та майнових прав автора, що надаються йому законом, оголосити себе автором твору: доводити його до відома публіки, відтворювати та розповсюджувати або використовувати його будь-якими іншими способами і засобами, а також дозволяти іншим особам використовувати твір певними способами.

У законодавстві Україні не закріплено визначення поняття «авторське право». У ст. 433 ЦКУ ст. 8 ЗУ «Про авторське право і суміжні права», закріплено, що до об'єктів авторського права відносяться: літературні та художні твори (романи, поеми, статті, та інші письмові твори; лекції, промови,проповіді та інші усні твори; драматичні, музично – драматичні твори, пантоміми, хореографічні, інші сценічні твори; інші групи об'єктів); комп'ютерні програми; компіляції даних (бази даних), якщо вони за добором або упорядкуванням їх складових частин є результатом інтелектуальної діяльності; інші твори.

Відповідно до ст.434 ЦКУ та ст. 10 ЗУ «Про авторське право і суміжні права», не є об'єктом авторського права:

а) повідомлення про новини дня або поточні події, що мають характер звичайної прес-інформації;

б) твори народної творчості (фольклор);

в) видані органами державної влади у межах їх повноважень офіційні документи політичного, законодавчого, адміністративного характеру (закони, укази, постанови, судові рішення, державні стандарти тощо) та їх офіційні переклади;

г) державні символи України, державні нагороди; символи і знаки органів державної влади, Збройних Сил України та інших військових формувань; символіка територіальних громад; символи та знаки підприємств, установ та організацій;

д) грошові знаки;

е) розклади руху транспортних засобів, розклади телерадіопередач, телефонні довідники та інші аналогічні бази даних, що не відповідають критеріям оригінальності і на які поширюється право sui-generis (своєрідне право, право особливого роду)

Крім того, що об'єкти авторського права знаходяться в постійному розвитку, вони потребують якісної охорони. Особливо сильно це питання стало після розвитку і розповсюдження світової мережі Інтернет. Глобальна система стала невід'ємної частиною розвитку суспільства і світу. Насправді, з

використанням Інтернету з'являються різноманітні види відносин. Але крім створення нових відносин, реалізацію ряду інших відносин і при всіх інших корисних напрямків, Інтернет став простором порушення прав осіб і авторських прав в першу чергу.

Дані, що наповнюють глобальну мережу Інтернет, тобто контент, є об'єктами авторських прав. Але для отримання доступу до цієї комп'ютерної мережі, необхідно скористатися різноманітним програмним забезпеченням, яке, в свою чергу, є також об'єктом авторського права. За підрахунками спеціалістів, загальний обсяг інформації, яка перебуває в мережі Інтернет, становить понад 500 млрд. гігабайт, причому цей показник невпинно зростає.

Авторське право в Україні регулюється Цивільним кодексом та Законом України «Про авторське право та суміжні права». Відповідно до нещодавно внесених доповнень розміщення твору в оцифрованому вигляді в Інтернет вважається публікацією твору або його поширенням і тому потребує дозволу власника авторського права. Розміщення в Інтернет копії твору чи його частини без дозволу автора є порушенням Закону і може бути оскаржене в суді з вимогою відшкодування моральної шкоди та завданих матеріальних збитків (упущеної вигоди).

Через особливості функціонування Інтернету, а саме: анонімності користувачів, екстериторіального характеру, свобод та швидкості поширення інформації – порушення авторських прав стало настільки буденним і поширеним явищем, що особа, вчиняючи протиправні дії, просто не усвідомлює їх сутності, а навпаки гадає, що діє в рамках закону.

Найпоширенішими видами порушень в мережі Інтернет є: незаконне відтворення і копіювання музичних, художніх, літературних творів чи комп'ютерних програм без попереднього надання на це згоди автором чи правовласником. Це виражає порушення матеріальних прав авторів. Крім цього, все популярніше становиться такий вид порушень як плагіат. Такі порушення в мережі Інтернет порушують матеріальні і нематеріальні права авторів.

Ідентифікація об'єктів авторського права і суміжних прав здійснюється за допомогою ідентифікаційного коду ISBN, цифрового підпису, цифрової марки.

Два шляхи для захисту авторський прав в мережі Інтернет

Захист на етапі до порушення:

1) обмежена функціональність – За такого підходу, власник авторського права надає користувачеві примірник твору, який має функціональні обмеження. Такий підхід є одним із шляхів впровадження в життя таких бізнес-моделей як „спробуй, перед тим, як купити" та „продавай поліпшені версії";

2) встановлення так званого „таймеру”– Аналогічно до прийому з функціональними обмеженнями, за цього підходу власник авторських прав розповсюджує функціонально повноцінний об’єкт інтелектуальної власності, але встановлює дату, після якої доступ до нього буде неможливим. Один з варіантів такого підходу передбачає закриття продавцем доступу до твору після певної кількості користувань (наприклад, після перегляду комп’ютерного файлу 10 разів його буде неможливо більше продивитися).;

3) захист від копіювання. За цього підходу продавець обмежує кількість разів, коли комп’ютерний файл може бути скопійований. Захист від копіювання був нормою в 1980-х роках, але пізніше вийшов з ужитку значною мірою тому, що користувачі скаржилися на незручність, а також тому, що захист копії можна було досить легко „зламати”;

4) криптографічні конверти – Криптографічні конверти – це програмне забезпечення, яке зашифровує твори так, що доступ до них може бути отриманий лише із застосуванням належного ключа до шифру. Програми, що здійснюють таку операцію, часто називають торговою маркою фірми IBM “cryptolopes”. Власники прав можуть захищати свої права на твори, розповсюджуючи їх у криптографічних конвертах і вимагаючи від користувачів плати за ключі, за допомогою яких твір можна „вийняти” з „конверта”;

5)контракти-угоди «наскрізного клацання» укладені через Інтернет, це – дозволи автора на використання творів;

6) запобіжні заходи: попередня публікація матеріалу на традиційному матеріалі, підтвердження факту існування твору на певну дату, засвідчення в нотаріуса дати створення твору, запис на лазерному диску і поміщення в архів або веб-депозитарій;

7) клірингові центри – автор надає центру право ліцензувати свої права на твір, центр приймає плату від користувача і передає її володільцеві авторських прав

Найпоширенішою є система так званих **„цифрових водяних знаків”,** впроваджуваних у твори (тексти, графічні зображення і тощо.) у мережі. Їх перевага полягає в тому, що при звичайному візуальному розгляді зображення користувач не бачить яких-небудь закодованих позначень – значка копірайта ©, імені автора, року видання. однак потім при застосуванні певного програмного засобу можна довести, що файли містять додаткову інформацію, що вказує на особу, яка її записала.

Можливе і застосування спеціальних „відбитків”. Вони також дозволяють контролювати використання творів в інформаційних мережах, а при виявленні

порушень авторського права і суміжних прав забезпечувати належну доказову базу в суді.

Цифровий водяний знак(ЦВЗ, Watermark) повинен відповідати наступним вимогам:

▶ непомітність для користувачів;

▶ індивідуальність алгоритму нанесення (досягається за допомогою стеганографічного алгоритму з використанням ключа);

▶ можливість для автора виявити несанкціоноване використання файлу;

▶ неможливість видалення неуповноваженими особами;

▶ стійкість до змін носія-контейнера (до зміни його формату і розмірів, до масштабування, стискування, повороту, фільтрації, введення спецефектів, монтажу, аналогових і цифрових перетворень).

Захист на етапі після порушення:

1) агенти – це комп'ютерні програми, які автоматично виконують попередньо визначені команди, наприклад, пошук у мережі контрафактних примірників творів;

2) стенографія – процес приховування інформації у файлах, наприклад «водяного знаку» автору твору, що буде доказом авторства цієї особи щодо цього твору;

3) «маячок» – це особлива мітка, яка розміщується в творі і спрацьовує під час несанкціонованого використання, надаючи можливість знайти порушника авторських прав;

4) використання кодових слів. Оригінальний метод контролю за використанням об'єктів авторського права. Полягає у введенні у текст рідкісних та «екзотичних» слів за якими можна відстежити використання власного твору.

Україна – лідер у рейтингу держав-порушників права інтелектуальної власності. Такі дані містить опублікований на початку лютого Спеціальний щорічний звіт Міжнародного альянсу інтелектуальної власності щодо захисту прав власності (IIPA – International Intellectual Property Alliance), відомий також як «список 301».

Міжнародний альянс інтелектуальної власності (IIPA) – це коаліція організацій приватного сектора, утворена в 1984 році комерційними асоціаціями, що представляють американський бізнес, заснований на авторському праві. Він працює над покращенням міжнародного захисту та охорони авторського права і суміжних прав. На основі звіту IIPA складається Список 301, де США зазначає найбільш «піратські» країни світу [7].

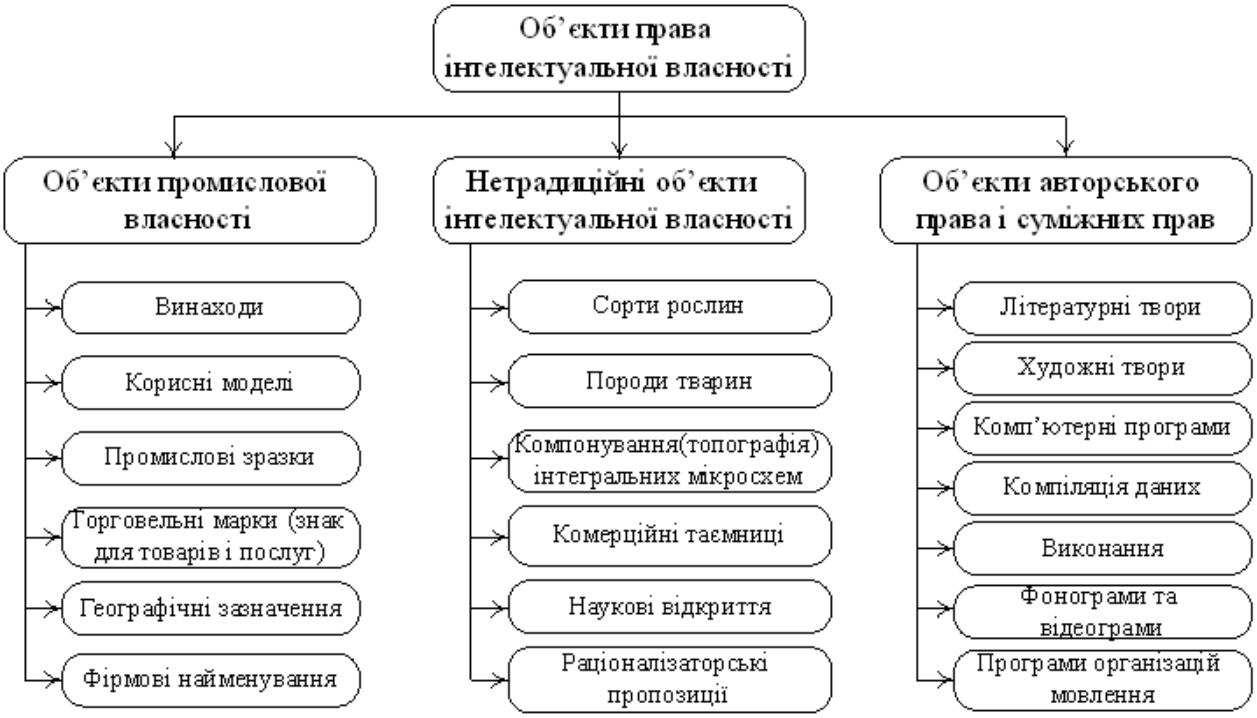

Рис. 4 Об'єкти права інтелектуальної власності

Об'єкти промислової власності

Винахід (*корисна модель* (КМ)) - це результат інтелектуальної діяльності людини в будь-якій сфері технології. Винахід (корисна модель) може бути секретним, якщо містить інформацію, віднесену до державної таємниці. Якщо винахід (корисна модель) створений працівником у зв'язку з виконанням службових обов'язків чи за дорученням роботодавця за умови, що трудовим договором не передбачено інше, або з використанням досвіду, виробничих знань, секретів виробництва і обладнання роботодавця, то він вважається службовим винаходом (корисною моделлю).

Промисловий зразок (ПЗ) - це результат творчої діяльності людини у галузі художнього конструювання.

Під *торговельною маркою* (ТМ) - розуміють позначення, за яким товари і послуги одних осіб відрізняються від товарів і послуг інших осіб.

Географічне зазначення - це назва географічного місця, яке вживається для позначення товару, що походить із цього географічного місця та має певні якості, репутацію або інші характеристики, в основному зумовлені характерними для даного географічного місця природними умовами чи людським фактором або їх поєднанням. Сутність фірмового найменування витікає з самої назви цього об'єкта. Але, на відміну від попередніх об'єктів, поки що не існує закону, який би охороняв права на нього.

Нетрадиційні об'єкти інтелектуальної власності

Сорт рослин - це окрема група рослин (клон, лінія, гібрид першого покоління,популяція) в рамках нижчого із відомих ботанічних таксонів. Під породою тварин зазвичай розуміють селекційні досягнення у тваринництві.

Зафіксоване на матеріальному носії просторово-геометричне розміщення сукупності елементів інтегральної мікросхеми та з'єднань між ними визначене законом як *топографія інтегральної мікросхеми* (ІМС).

Комерційна таємниця - це технічна, комерційна, організаційна та інша інформація, що здатна підвищити ефективність виробництва або іншої соціально доцільної діяльності або забезпечити інший позитивний ефект. Відкриттям визнається встановлення невідомих раніше закономірностей властивостей і явищ матеріального світу.

Раціоналізаторською пропозицією є визнана юридичною особою пропозиція, яка містить технологічне (технічне) або організаційне рішення у будь-якій сфері її діяльності.

Ознаки нетрадиційних об’єктів права інтелектуальної власності:

- кожному нетрадиційному об’єкту притаманний творчий характер, тобто він повинен бути створений в результаті діяльності, завдяки якій створюється матеріальна чи духовна цінність для людини
- він повинен бути виражений у будь-якій об’єктивній формі;
- має потребу у відповідному правовому регулюванні.

Зазначені вище ознаки притаманні також і традиційним об’єктам права інтелектуальної власності, але те, що предметом правової охорони нетрадиційного об’єкта можуть виступати властивості, закономірності, явища матеріального світу, закріплення різного порядку правової охорони відповідно до специфіки об’єктів а також матеріальної винагороди авторів, та потреба кожного нетрадиційного об’єкта в особливому, притаманному лише йому законодавчому регулюванні, дає підставу віднести зазначені вище об’єкти до особливого інституту охорони «нетрадиційних об’єктів права інтелектуальної власності».

Охорона прав на нетрадиційні об’єкти інтелектуальної власності регламентується Цивільним кодексом України, а на такі нетрадиційні об’єкти інтелектуальної власності, як сорти рослин та топографії інтегральних мікросхем спеціальними законами України: «Про охорону прав на сорти рослин», «Про охорону прав на топографії інтегральних мікросхем». Що ж стосується інших нетрадиційних об’єктів інтелектуальної власності (породи тварин, комерційні таємниці, ноу-хау,наукові відкриття, раціоналізаторські пропозиції), на цей час

ще неприйняті спеціальні закони щодо їх правової охорони, хоча ряд питань регулюється нормативними актами різної галузевої належностіта різної юридичної сили. Слід зазначити, що охоронні документи на нетрадиційні об’єкти інтелектуальної власності, як правило видаються Урядовими органами державного управління до ведення яких віднесені спеціалізовані види діяльності за напрямом яких створюються ці нетрадиційні об’єкти інтелектуальної власності.

Отже, нетрадиційні об’єкти права інтелектуальної власності мають схожі риси з традиційними об’єктами, і потребують правове регулювання нарівні з традиційними, оскільки вони є передумовою нових рішень у різноманітних сферах людської діяльності [8].

Об'єкти авторського права і суміжних прав

Ці об'єкти права інтелектуальної власності, у свою чергу, поділяються на дві групи - власне *об'єкти авторського права*: твори літератури і мистецтва, комп'ютерні програми, компіляції даних (бази даних) і *об'єкти, суміжні з авторськими правами***,** до яких відносяться виконання творів, фонограми і відеограми, програми (передачі) організацій мовлення.

Перелік об'єктів права інтелектуальної власності, наведений на рисунку, не є вичерпним. З розвитком людської цивілізації будуть з'являтися все нові й нові об'єкти права інтелектуальної власності, насамперед у галузі інформаційних технологій, генної інженерії тощо.

Суб'єкти права інтелектуальної власності

Суб'єктами права інтелектуальної власності є: творець (творці) об'єкта права інтелектуальної власності (автор, виконавець, винахідник тощо) та інші особи, яким належать за заповітом або за договором особисті немайнові та (або) майнові права інтелектуальної власності.

Суб'єктами права на винаходи, корисні моделі, промислові зразки є автори або фізичні чи юридичні особи, до яких право авторів перейшло за договором чи заповітом.

Суб'єктами права на торговельні марки, зазначення походження товарів можуть бути юридичні особи, а також фізичні особи, якщо вони здійснюють підприємницьку діяльність.

Суб'єктом правовідносин, що виникають у процесі створення і використання сортів рослин, може бути будь-яка юридична чи фізична особа.

Суб'єктом права на раціоналізаторську пропозицію є раціоналізатор, тобто автор раціоналізаторської пропозиції, що створив її творчою працею.

До суб'єктів авторського права відносяться:

- ✓ автори творів;
- ✓ спадкоємці й інші правонаступники;
- ✓ організації, що керують майновими правами авторів на колективній основі.

Авторами визнаються особи, творчою працею яких створений твір. Авторами визнаються не тільки творці оригінальних творів, але й творці похідних (залежних) творів, таких як: переклади, переробки, копії творів мистецтва тощо.

Суб'єктами авторського права можуть бути також видавництва, театри, кіностудії та інші організації, що займаються використанням творів [9].

Суб'єкти авторського права – це особи, які володіють суб'єктивними авторськими правами на літературний, художній чи інший твір. Суб'єктів авторського права можна умовно поділити на два види.

До першого виду належать первинні суб'єкти авторського права – автори та співавтори. Автор твору – це фізична особа, яка своєю творчою працею створила твір (ст. 1 Закону України «Про авторське право і суміжні права»). За українським законодавством автором може бути будь-яка фізична особа незалежно від віку, ступеня дієздатності, громадянства чи інших правових ознак.

У ст. 435 Цивільного кодексу України зазначено, що, за відсутності доказів іншого, автором твору вважається фізична особа, зазначена звичайним способом як автор на оригіналі або примірнику твору (так звана, презумпція авторства).

Співавтори – особи, спільною творчою працею яких створено твір (ст. 13 Закону України «Про авторське право і суміжні права»).

Для співавторства необхідні певні умови:

- по-перше, твір має бути створений творчою працею двох і більше осіб;
- по-друге, твір має бути самостійним об'єктом авторського права (тобто, твором, який охороняється авторським правом);
- по-третє, має бути укладено угоду про співпрацю над твором.

Виходячи з викладених вище умов, співавторство – це правовий наслідок створення літературного, художнього чи іншого твору узгодженою творчою співпрацею двох або більше фізичних осіб.

Авторське право на твір, створений у співавторстві, належить співавторам спільно, незалежно від того, становить такий твір одне нерозривне ціле (нероздільне співавторство) чи складається з частин, кожна з яких може мати ще й самостійне значення (роздільне співавторство). Частина твору, створеного у співавторстві, визнається такою, що має самостійне значення, якщо вона може бути використана незалежно від інших частин цього твору. Кожен із співавторів

зберігає своє авторське право на створену ним частину твору, яка має самостійне значення (ст. 436 Цивільного кодексу України).

Відносини між співавторами можуть бути визначені договором.

В договорі має бути передбачено порядок використання твору, розподілу винагороди між співавторами та інші умови співпраці. Якщо договір між співавторами не укладений, слід керуватися приписами закону[10].

Контрольні питання:

1. Які існують шляхи для захисту авторський прав в мережі Інтернет?
2. Які функції виконує Міжнародний альянс інтелектуальної власності ?
3. Назвіть види об’єктів права інтелектуальної власності.
4. Що відноситься до об'єктів промислової власності
5. Що відноситься до нетрадиційних об'єктів інтелектуальної власності
6. Що таке об'єкти авторського права і суміжних прав?
7. Що відноситься до суб'єктів авторського права?

ТЕМА 6. ПУБЛІЧНА ІНФОРМАЦІЯ: ПОНЯТТЯ, КЛАСИФІКАЦІЯ, ДОСТУП

Загальна характеристика поняття «публічна інформація»

Відповідно до міжнародних стандартів, що регламентують порядок доступу до публічної інформації, до такої інформації віднесено інформацію, яка вільно збирається, отримується, зберігається, використовується та поширюється.

Правове визначення поняття «публічна інформація» міститься у статті 1 Закону «Про доступ до публічної інформації», згідно з якою **публічна інформація – це відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, що була отримана або створена в процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом.**

Слід зауважити, що інформація вважається публічною у зв'язку з тим, що вона створюється, збирається, обробляється та зберігається за рахунок бюджетних коштів, призначених на забезпечення діяльності відповідного органу влади.

Рис. 5 Розпорядники публічної інформації

За режимом доступу інформація поділяється на **відкриту та з обмеженим доступом**.

Рис. 6 Режими доступу до інформації

Поняття доступу до публічної інформації

Міжнародні стандарти, на яких базується і український закон, розглядають доступ у пасивному і активному аспектах. На відміну від позиції, коли активний і пасивний доступ розглядається як дії особи щодо отримання публічної інформації, міжнародні стандарти розглядають аспекти доступу саме в контексті забезпечення органом влади реалізації права на доступ до публічної інформації.

Пасивний аспект доступу (з боку органу влади) передбачає відповідь органу на запит від особи/групи осіб, забезпечення їхньої участі в засіданні колегіальних органів, надання можливості ознайомитися з публічною інформацією в органі влади.

Активний аспект доступу (з боку органу влади) – обов'язок органу влади оприлюднювати інформацію про свою діяльність, ухвалені документи та проекти, що готуються, реєстр публічної інформації тощо в один або кілька способів – публікувати в ЗМІ, розміщувати на офіційних веб-сайтах, вивішувати на інформаційних стендах тощо

Рис. 7 Способи забезпечення розпорядниками доступу до публічної інформації

Права та обов'язки громадян у сфері доступу до публічної інформації

Відповідно до статті 10 Закону України «Про доступ до публічної інформації» кожна особа має право:

1) знати у період збирання інформації, але до початку її використання, які відомості про неї та з якою метою збираються, як, ким і з якою метою вони використовуються, передаються чи поширюються, крім випадків, встановлених законом;
2) доступу до інформації про неї, яка збирається та зберігається;
3) вимагати виправлення неточної, неповної, застарілої інформації про себе, знищення інформації про себе, збирання, використання чи зберігання якої здійснюється з порушенням вимог закону;
4) на ознайомлення за рішенням суду з інформацією про інших осіб, якщо це необхідно для реалізації та захисту прав та законних інтересів;
5) на відшкодування шкоди у разі розкриття інформації про цю особу з порушенням вимог, визначених законом

Захист облікової інформації та кібербезпека підприємства

Найціннішою економічною інформацією є **облікова інформація**, яка характеризує всі аспекти господарської діяльності.

Сьогодні більшість суб'єктів господарювання використовують комп'ютеризовану форму ведення бухгалтерського обліку, яка передбачає використання спеціалізованого програмного забезпечення та технічних засобів. При цьому в комп'ютерних системах зберігаються і обробляються великі обсяги облікової інформації, будь-який збій може привести до надмірних витрат, недостатніх доходів, втрати активів, санкцій тощо.

Тому головним пріоритетом захисту облікової інформації на підприємстві є розробка заходів, спрямованих на збереження інформації, що міститься у комп'ютерних базах підприємства.

Під захистом облікової інформації розуміється стан її захищеності від випадкових або навмисних впливів природного або штучного характеру, що можуть привести до нанесення шкоди власникам або користувачам цієї інформації. Якщо розглядати це поняття без конкретики, то можна говорити про інформаційну безпеку загалом. Однак коли захист інформації стосується забезпечення безпеки інформаційних баз даних, а також різних програм, що входять у комп'ютерні мережі, виникає необхідність визначити співвідношення між інформаційною безпекою та кібербезпекою.

Кібербезпека — це процес застосування заходів безпеки з метою забезпечення конфіденційності, цілісності та доступності даних.

Інший науковий погляд на сутність кібербезпеки означає наступальні дії, тобто кібербезпека відрізняється від традиційної інформаційної безпеки тим, що вона включає застосування практичних дій і засобів для атаки супротивників.

У науковій літературі під час розмежування понять «кібербезпека» та «інформаційна безпека» загрози кібербезпеці визначаються в уразливості об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак, а також у фізичній і моральній застарілості системи охорони державної таємниці та інших видів інформації з обмеженим доступом.

Об'є́кти крити́чної інфраструкту́ри — підприємства та установи (незалежно від форми власності) таких галузей, як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології та телекомунікації (електронні комунікації), продовольство, охорона здоров'я, комунальне господарство, що є стратегічно важливими для функціонування економіки і безпеки держави, суспільства та населення, виведення з ладу або руйнування яких може мати вплив на національну безпеку і оборону, природне середовище, призвести до значних матеріальних та фінансових збитків, людських жертв.

На відміну від інформаційної безпеки йдеться не про інформацію взагалі, а про ту інформацію, яка циркулює в кіберпросторі і становить важливу частину її змісту. Зрозуміло, що втрата інформації, яка зберігається в окремому комп'ютері і є важливою для користувача цього комп'ютера, не може розглядатися як загроза кібербезпеці. Однак захист інформації потрібно передбачувати, виходячи із цінності інформації не для себе, а для зловмисників, які будують відносини винятково на грошовій основі.

Кібербезпека включає в себе захист інформації, але не обмежується лише нею. Це захист від вірусів, хакерських атак, підробки даних, які можуть не тільки видалити/вкрасти дані, але і вплинути на роботу і продуктивність співробітників, використовувати інформацію проти людини або структури, а також зупинити виробництво. **Кібербезпека сьогодні відповідає за три чинники: системи, процеси, люди.**

Із позицій міжнародної організації «Міжнародний телекомунікаційний союз» (International Telecommunication Union, ITU) кібербезпека – це набір засобів, стратегії, принципи забезпечення безпеки, гарантії безпеки, керівні принципи, підходи до управління ризиками, дії, професійна підготовка, практичний досвід, страхування та технології, які можуть бути використані для захисту кіберсередовища, ресурсів організації та користувача.

У визначення «кібербезпека» за основу покладаємо розуміння поняття «безпека», що згідно з українським тлумачним словником означає стан, коли кому-небудь або чому-небудь ніщо не загрожує . Відповідно кібербезпека – це деякий стан системи, за якого нейтралізуються загрози доступності, цілісності або конфіденційності даних, що циркулюють в інформаційних системах.

У національній стратегії кібербезпеки України розкривається поняття забезпечення кібербезпеки України як стану захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, що досягається комплексним застосуванням сукупності правових, організаційних, інформаційних заходів. При цьому під кіберпростором розуміється середовище, яке виникає в результаті функціонування на основі єдиних принципів і за загальними правилами інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем.

Кіберпростір розглядають як тріаду, яка містить у собі три основні складники, такі як:

1) інформація в її цифровому поданні – статичному (файли, записані на носії даних) і динамічному (пакети, потоки, команди, запити);

2) технічна інфраструктура, програмне забезпечення, за допомогою яких здійснюється реалізація основних дій з інформацією (Інтернет і мережеві взаємозв’язки, комп’ютери, гаджети тощо);

3) інформаційна взаємодія суб’єктів із використанням інформації, одержуваної і оброблюваної за допомогою технічної інфраструктури.

З огляду на сутність поняття «захист інформації», яке трактується міжнародним стандартом ISO/IEC 27001 як забезпечення конфіденційності, цілісності та доступності інформації, під кібербезпекою облікової інформації розуміємо стан її захищеності, що створюється, зберігається, змінюється та використовується за допомогою комп’ютерної техніки, за якого забезпечується своєчасне виявлення, запобігання і нейтралізація несанкціонованого використання облікової інформації, порушення її конфіденційності, цілісності або знищення через електронні засоби, що ставить під загрозу життєво-важливі економічні інтереси підприємства.

Завдання організації кіберзахисту і безпеки даних у бухгалтерії полягає у забезпеченні комплексу організаційно-технічних заходів та кадрової роботи, спрямованої на збереження комерційної таємниці. Відповідно до цього вважаємо, що всі заходи щодо кіберзахисту облікової інформації можна умовно поділити на три групи. Більшість засобів захисту реалізуються у вигляді програм

або пакетів програм, що розширюють можливості стандартних операційних систем, а також систем керування базами даних.

До суто технічних засобів захисту бухгалтерської інформації в автоматизованій системі науковці відносять шифрування документів. На технологічному рівні заходами з кібербезпеки можуть бути контроль доступу до облікових даних, управління та безпека авторизації облікової інформації.

Основним способом попередження кіберзагроз є впровадження послідовних рівнів заходів контролю за доступом до сайту, системи та файлів. Створення механізму підзвітності дає змогу визначати, хто працює в системі та що робить у певний момент часу, і протоколювати події, що відбувалися в комп'ютерній інформаційній системі бухгалтерського обліку.

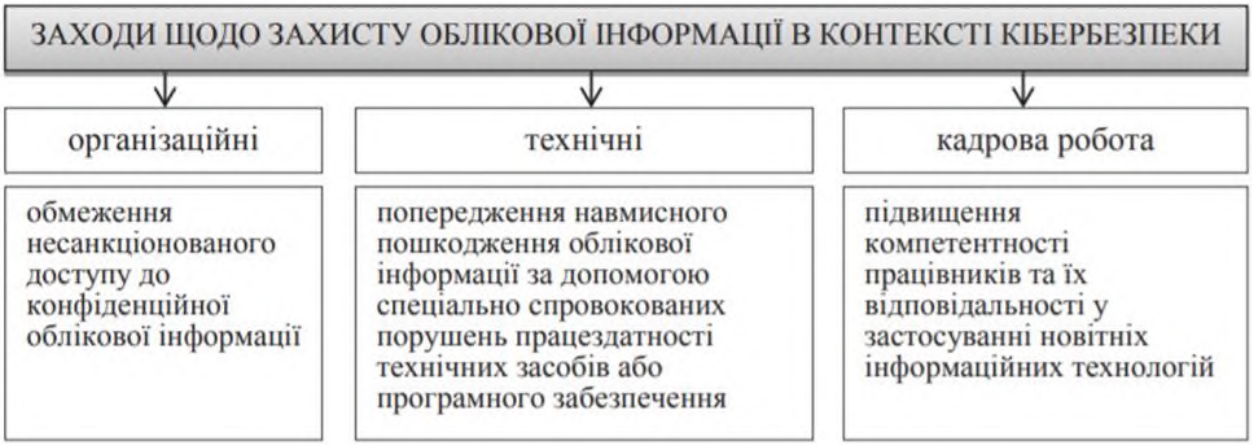

Рис. 8 Заходи щодо кіберзахисту облікової інформації

Некомпетентними діями працівників, які є загрозою втрати інформації є:

– відкриття на своєму комп'ютері файлів, надісланих електронною поштою або програмами миттєвого обміну повідомленнями від невідомих адресатів;

– встановлення неліцензійного програмного забезпечення, не потрібного для виконання функціональних обов'язків працівника;

– використання паролів «за замовчуванням», створення простих паролів або небажання змінювати паролі протягом тривалого часу, «запам'ятовування» пароля у вікнах уведення, особливо на комп'ютерах для публічного доступу;

– роботу з конфіденційними документами у місцях публічного доступу;

– повідомлення по телефону будь-яких даних про обліковий запис, логіни, паролі;

– нецільове використання мережевих ресурсів тощо.

Загалом управління кібербезпекою входить до загальної системи управління економічною безпекою підприємства, і залежно від розмірів та потужності підприємства, а також відповідно до розрахунків економічної

доцільності рівня захисту облікової інформації вирішуються організаційно-кадрові питання. Вони передбачають створення або спеціальної служби із забезпечення кібербезпеки облікової інформації, або введення посади спеціаліста з кібербезпеки, який займатиметься розробленням охоронних систем для різних комунікаційних мереж і електронних баз даних у структурі служби внутрішнього контролю підприємства або бухгалтерської служби.

Спецслужбу з кібербезпеки можуть представляти фахівці з організації інформаційної безпеки та проведення тестування на проникнення, інспектори з організації захисту секретної інформації, аналітики проектів із кібербезпеки, системні адміністратори, адміністратори комп'ютерних мереж, менеджери систем з інформаційної безпеки, аналітики систем забезпечення кібербезпеки.

Обов'язками таких фахівців є:

– виявлення уразливих місць системи та моделювання можливої ситуації стороннього кібервпливу з позиції загроз і пов'язаних із ними ризиків;

– контроль надійності функціонування системи захисту облікової інформації, розроблення заходів безпеки на випадок непередбачуваних подій;

– віднесення облікової інформації до категорії обмеженого доступу (службової і комерційної таємниць, іншої конфіденційної інформації);

– розроблення положень, політики і процедур у рамках системи безпеки облікової інформації;

– упровадження розроблених заходів безпеки та випробування системи з оцінкою її результативності, за необхідності внесення коригувань;

– встановлення користувачам комп'ютерної системи бухгалтерського обліку необхідних реквізитів захисту;

– навчання користувачів комп'ютерної інформаційної системи правилам безперервної обробки інформації;

– контроль за дотриманням користувачами комп'ютерної інформаційної системи та персоналом підприємства встановлених правил роботи з обліковою інформацією, що захищається у процесі її автоматизованої обробки.

Рис. 9 Принципи системи заходів кібербезпеки облікової інформації

Отже:

- ❑ Кіберзлочинність постійно вдосконалюється
- ❑ Проблема кібербезпеки – це проблема не лише загальнодержавного рівня, а кожного окремо взятого підприємства
- ❑ Індивідуальна відповідальність кожного працівника є найпершим і найпростішим фактором, який сприяє захисту цінної облікової інформації.
- ❑ На кожному підприємстві повинна бути створена програма визначених дій, спрямованих на створення кіберзахисту інформації, сфера застосування якого поширюється на людські ресурси і не обмежується винятково технологічними аспектами.

Контрольні питання:

1. Що таке публічна інформація?
2. Які є режими доступу до інформації?
3. Що таке об'є́кти крити́чної інфраструкту́ри? Назвіть приклади.
4. Які є типи заходів щодо кіберзахисту облікової інформації?
5. Що є некомпетентними діями працівників, які є загрозою втрати інформації?
6. Назвіть обов'язки фахівців з кібербезпеки.
7. Назвіть принципи системи заходів кібербезпеки облікової інформації.

ТЕМА 7. ЗАХИСТ ІНФОРМАЦІЇ

У ході збільшення та поширення інформації, якою може володіти людина у неї з'явилась необхідність обробки, структуризації та зберігання інформації. Відповідно до області використання даної інформації вона набуває великої цінності і втрата чи несанкціонований доступ до неї можуть нести важкі матеріальні наслідки для власника.

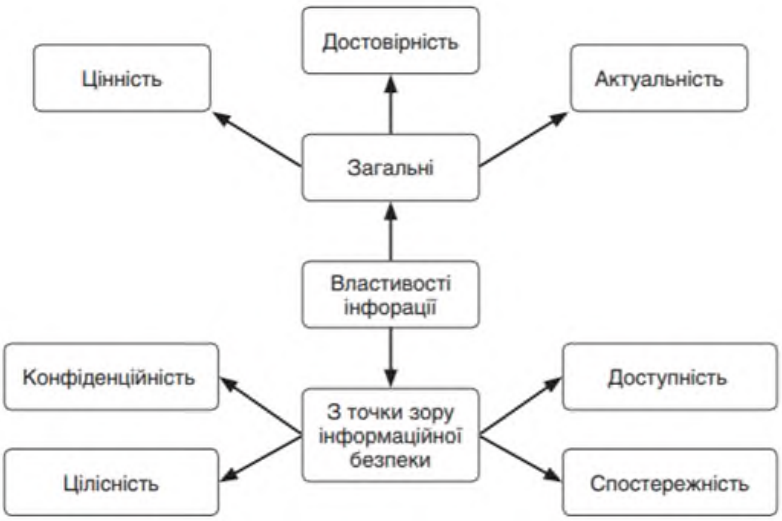

Рис. 61 Властивості інформації

Інформаційною безпекою (у контексті безпосередньої діяльності із захисту інформації) може вважатись комплекс заходів, що спрямовані на забезпечення захищеності інформації від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки, запису чи знищення даних.

Інформаційну безпеку за сферою застосування можна розглядати у контексті безпеки держави, організації та особистості.

Термін **«захист інформації»** (або англ. Data protection) визначає сукупність методів і засобів, що забезпечують цілісність, конфіденційність і доступність інформації за умов впливу на неї загроз природного або штучного характеру, реалізація яких може призвести до завдання шкоди власникам і користувачам інформації3 .

До основних завдань у сфері захисту інформації (ЗІ) в інформаційно-телекомунікаційних системах у цілому належать:

- керування доступом користувачів до інформаційних ресурсів систем з метою захисту від неправомірного випадкового або навмисного втручання у роботу і несанкціонованого (із перевищенням наданих повноважень) доступу до програмних і апаратних ресурсів як персоналу, так і сторонніх осіб;
- захист даних, що передаються каналами зв'язку;

- захист інформації з обмеженим доступом від витоку;
- захист інформації від спеціальних впливів;
- реєстрація, збереження і надання даних про події, що відбувалися у системі і стосувалися інформаційної безпеки (ІБ);
- контроль роботи користувачів системи адміністраторами та обов'язкове повідомлення адміністратора безпеки про будь-які спроби несанкціонованого доступу до ресурсів системи;
- контроль і підтримка цілісності критичних ресурсів системи захисту і середовища виконання прикладних програм;
- забезпечення функціонування програмно-технічних комплексів з метою захисту інформації від впровадження у роботу потенційно небезпечних програм і засобів подолання системи захисту;
- керування та моніторинг засобів захисту інформації.

Дані – інформація, подана у формалізованому вигляді, придатному для передачі, інтерпретації чи обробки за участю людини або автоматичними засобами.

Організація даних – зображення і керування даними у відповідності з визначеними відношеннями.

Керування даними – процес, що забезпечує подання, накопичення, зберігання, використовування даних, а також маніпулювання ними.

Подання даних – сукупність правил кодування даних та створення конструкцій даних у системі обробки даних.

База даних – сукупність взаємопов'язаних даних, організованих у відповідності зі схемою БД таким чином, щоб з ними міг працювати користувач.

СУБД (СКБД) – сукупність програмних та мовних засобів, що забезпечують керування базою даних. Головна задача СУБД полягає в забезпеченні користувача інструментарієм, що дозволяє оперувати даними в абстрактних термінах, не пов'язаних зі способом збереження даних в комп'ютері.

Таблиця 1. Ролі користувачів у сучасних СКБД

Роль	Можливості	Загрози
Власник	Усі дії по налаштуванню та обслуговуванню БД та видалення	Втрата даних у зв'язку з некомпетентністю чи халатністю,
Адміністратор	Адміністрування бази даних, надання привілеїв.	Цілісність даних, ненавмисне надання прав іншим користувачам.
Редактор	Редагування та видалення даних у таблицях	Цілісність та конфіденційність даних
Читач	Зчитування даних	Конфіденційність даних
Користувач без прав на доступ	Не може виконувати дії з БД	-

Методи захисту інформації в базах даних

1. **Підтримка цілісності.**

Засоби підтримки цілісності даних також вносять певний внесок до загальної захищеності бази даних, оскільки вони попереджують перехід даних в неузгоджений стан, а відповідно, і запобігають загрозі отримання помилкових або некоректних результатів розрахунків.

2. **Шифрування.**

Шифрування – це кодування даних з використанням спеціального алгоритму, внаслідок чого дані стають недоступними для читання будь-якою програмою, що не має ключа дешифрування. Якщо в системі разом з БД міститься важлива конфіденційна інформація, то має сенс закодувати її з метою попередження можливостей несанкціонованого доступу із зовні (по відношенню до СУБД). Тому деякі СУБД містять засоби шифрування, призначені для таких цілей, а відповідні підпрограми забезпечують санкціонований доступ до даних (після їх декодування). Шифрування також може використовуватися для захисту даних при їх передачі по лініях зв'язку.

Для організації захисту передачі даних по незахищених мережах повинні використовуватися системи шифрування, що включають наступні компоненти:

- ключ шифрування, призначений для шифрування початкових даних (звичайного тексту);
- алгоритм шифрування, який описує, як за допомогою ключа шифрування перетворити звичайний текст в шифротекст;
- ключ дешифрування, призначений для дешифрування шифротексту;
- алгоритм дешифрування, який описує, як за допомогою ключа дешифрування перетворити шифротекст в початковий звичайний текст.

Одна з поширених систем шифрування називається DES (Data Encryption Standard) — в ній використовується стандартний алгоритм шифрування, розроблений фірмою IBM. У цій схемі для шифрування і дешифрування використовується один і той же ключ, який повинен зберігатися в секреті, хоча сам алгоритм шифрування не є секретним. Цей алгоритм передбачає перетворення кожного 64-бітового блоку звичайного тексту з використанням 56-бітового ключа шифрування.

3. Допоміжні процедури

Хоча вище вже були описані різні механізми, які можуть використовуватись для захисту даних в середовищі СУБД, самі по собі вони не гарантують необхідного рівня захищеності і можуть виявитися неефективними у разі неправильного застосування або управління. Тому існують різні допоміжні

процедури, які повинні використовуватися спільно з описаними вище механізмами захисту. Такими процедурами, зокрема, є:

3.1. Авторизація і аутентифікація

Механізм паролів, є одним із найпоширеніших методом підтвердження особи користувачів. З погляду забезпечення необхідного рівня захисту дуже важливо, щоб всі використовувані паролі трималися користувачами в секреті і регулярно оновлювалися через деякий встановлений інтервал часу. В ході процедури реєстрації в системі пароль не повинен відображатися на екрані, а списки ідентифікаторів користувачів і їх паролі повинні зберігатися в системі в зашифрованому вигляді.

Ідентифікація - це пред'явлення користувачем якогось унікального, властивого тільки йому ідентифікатора (ознаки). На сьогодні існує декілька способів ідентифікації користувачів, у кожного з яких свої переваги і недоліки. **Аутентифікація** - це процедура, яка перевіряє, чи має користувач з пред'явленим ідентифікатором право на доступ до ресурсу. Методи аутентифікації можна розділити на 4 великі групи, які наведені у таблиці.

Таблиця 2. Методи аутентифікації та їх характеристика

№	Метод аутентифікації	Характеристика методу
1	Методи, засновані на знанні секретної інформації	Класичним прикладом таких методів є парольний захист, коли в якості засобу ауткентифікації користувачу пропонується ввести пароль - деяку послідовність символів. Такі методи аутентифікації є найпоширенішими.
2	Методи, засновані на використанні унікального предмета	В якості такого предмета можуь бути використані: смерт-карта, токен, електронний ключ тощо.
3	Методи, засновані на використанні біометричних характеристик людини	На практиці частіше використовуються одна або деякі з наступних бірметричних характеристик: відбитки пальців (найбільш розповсюджено); малюнок сітківки або райдужної оболонки ока; термографія долоні; геометрія і термограма обличчя; почерк (підпис); голос.
4	Методи, засновані на інформації, асоційованій з користувачем	Прикладом такої інформації можуть бути координати користувача, визначені за допомогою GPS. Цей підхід навряд чи може бути використаний як єлиний механізм аутентифікації , проте цілком допустимо його використання як додаткового елементу захисту.

Поширена практика сумісного використання декількох з перерахованих вище механізмів – у таких випадках кажуть про **багатофакторну аутентифікацію**.

Розглянемо перераховані підходи докладніше.

Парольні системи захисту. Головна перевага парольної ідентифікації - простота і звичність. Паролі давно вбудовані в операційні системи та інші сервіси. При правильному використанні паролі можуть забезпечити прийнятний для багатьох організацій рівень безпеки. Проте за сукупністю характеристик їх слід визнати найслабкішим засобом перевірки достовірності. Саме слабкий рівень парольного захисту є однією з основних причин уразливості комп'ютерних систем до спроб несанкціонованого доступу (НСД).

Хешування (використання незворотної хешфункції до будь-якої інформації перетворює її на унікальний код) не забезпечує захист від підбору паролів по словнику у разі отримання бази даних зловмисником. При виборі алгоритму хешування, який буде використаний для розрахунку згорток паролів, необхідно гарантувати неспівпадання значень згорток, отриманих на основі різних паролів користувачів. Крім того, слід передбачити механізм, що забезпечує унікальність згорток у випадку, якщо два користувачі вибирають однакові паролі.

При шифруванні паролів особливе значення має спосіб генерації і зберігання ключа шифрування бази даних облікових записів.

Перерахуємо деякі можливі варіанти:

- ключ генерується програмно і зберігається в системі, забезпечуючи можливість її автоматичного перезавантаження;
- ключ генерується програмно і зберігається на зовнішньому носієві, з якого прочитується при кожному запуску;
- ключ генерується на основі вибраного адміністратором пароля, який вводиться в систему при кожному запуску.

Найбезпечніше зберігання паролів забезпечується при їх хешуванні і подальшому шифруванні отриманих згорток, тобто при їх комбінації. Враховуючи, що користувачі нерідко вибирають недостатньо стійкі паролі, можна зробити висновок, що отримання бази даних облікових записів або перехоплення переданого по мережі значення згортки пароля представляють серйозну загрозу безпеці парольної системи.

У захищеній системі передачу можна застосовувати тільки у поєднанні із засобами захисту мережевого трафіку.

Ідентифікація з використанням унікального предмета. Кожен апаратний (електронний) ідентифікатор є фізичним пристроєм (eToken), який зазвичай невеликих розмірів (його можна носити із собою), зручний та недорогий. Основне призначення:

- двофакторна аутентифікація користувачів при доступі до захищених ресурсів (комп'ютерів, мереж, додатків);
- безпечне зберігання закритих ключів цифрових сертифікатів, криптографічних ключів, профілів користувачів, налаштувань додатків тощо в незалежній пам'яті ключа;
- апаратне виконання криптографічних операцій в довіреному середовищі (генерація ключів шифрування, симетричне і асиметричне шифрування, розрахунок хеш-функції, формування електронного цифрового підпису - ЕЦП).

Біометрична ідентифікація

Біометрична ідентифікація - це спосіб ідентифікації особи за окремими специфічними біометричними ознаками.

Сучасний рівень розвитку комп'ютерних технологій дав змогу використовувати подібні ознаки як основу для ідентифікації людини і ухвалення рішення про доступ до ресурсів. Біометричні механізми ідентифікації наведені у табл. 3.

Таблиця 3. Біометричні механізми ідентифікації

Вид ознаки	Характеристика механізмів ідентифікації
Динамічні ознаки - поведінкові характеристики, які побудовані на особливостях підсвідомих рухів у процесі відтворення будь-якої дії	*Ідентифікація за голосом* - враховуються унікальні частотні характеристики голосу людини
	Ідентифікація за почерком - досліджується почерк людини. Перевіряються такі динамічні характеристики: графічні параметри, сила натиску на поверхню, швидкість написання. На основі цих характеристиках і будується цифровий код
	Ідентифікація за клавіатурним почерком - метод аналогічний ідентифікації за почерком. Замість того, щоб ставити автограф, людині необхідно надрукувати кодове слово. Цифровий код будується по динаміці набору певного слова або фрази
Статичні ознаки - ознаки, які практично не змінюються з часом, починаючи з народження людини (фізіологічні характеристики)	*Ідентифікація за відбитком пальця* побудована таким чином: за допомогою сканера одержують зображення відбитку, потім це зображення за складним алгоритмом перетворюється на спеціальний цифровий код, який далі порівнюється з еталонними кодами, що зберігаються в базі даних
	Ідентифікація за розташуванням вен на долоні. Прилад, який зчитує інформацію в цьому випадку, є

	інфрачервона камера. У результаті на вході програми при формуванні цифрового коду з'являється малюнок вен на руці людини. Не потребує контакту людини з пристроєм для сканування. Має високі показники надійності і достовірності
	Ідентифікація за сітківкою ока. В цьому випадку сканується малюнок кровоносних судин очного дна, який має нерухому структуру, незмінну в часі. За допомогою програмного забезпечення із зображення виділяється малюнок потрібної райдужної оболонки. Цей метод є одним з найбільш точних серед біометричних методів
	Ідентифікація за райдужною оболонкою ока. Малюнок райдужної оболонки ока - унікальний для кожної людини. За допомогою програмного забезпечення із зображення виділяється малюнок потрібної райдужної оболонки. Цей метод є одним з найбільш точних серед біометричних методів
	Ідентифікація за формою кисті руки грунтується на розпізнаванні геометричних особливостей кисті руки. Спеціальний сканер формує тривимірний малюнок кисті. При аналізі цього малюнка виконуються вимірювання, за допомогою яких формується відповідний цифровий код
	Ідентифікація за формою обличчя. Двовимірне розпізнавання обличчя на сьогодні - один із самих неефективних методів біометрії, тому має обмежене коло застосування або використовується тільки в сукупності з іншими методами

Комплексна (або багатофакторна) ідентифікація

Впровадження комбінованих систем збільшує кількість ідентифікаційних ознак і тим самим підвищує безпеку.

Нині існують комбіновані системи наступних типів:

- системи на базі безконтактних смарт-карт і USB-ключів;
- системи на базі гібридних смарт-карт;
- біоелектронні системи.

Безконтактні смарт-карти і USB-ключі.

У корпус брелока USB-ключа вбудовується антена і мікросхема для створення безконтактного інтерфейсу. Це дасть змогу організувати управління доступом у приміщення і до комп’ютера, використовуючи один ідентифікатор. Ця схема використовування ідентифікатора може виключити ситуацію, коли

співробітник, покидаючи робоче місце, залишає USB-ключ у роз’ємі комп’ютера, що дасть змогу працювати під його ідентифікатором.

Гібридні смарт-карти. Один чип підтримує контактний інтерфейс, інший - безконтактний. Як і гібридні USB-ключі, гібридні смарт-карти розв’язують дві задачі: доступ у приміщення і доступ до комп'ютера.

Додатково на карту можна нанести логотип компанії, фотографію співробітника або магнітну смугу, що робить можливим повністю замінити звичайні перепустки і перейти до єдиної “електронної перепустки”.

Біоелектронні системи. Як правило, для захисту комп’ютерних систем від несанкціонованого доступу застосовується комбінація з двох систем - біометричної і контактної на базі смарт-карт або USB-ключів. Досягти підвищення надійності та точності автоматизованих систем ідентифікації користувачів можна за рахунок об’єднання використання біометричних характеристик разом із класичними способами ідентифікації користувачів [11].

3.2. Копіювання

Процедури, що регламентують процеси створення резервних копій, визначаються типом і розмірами експлуатованої бази даних, а також тим набором відповідних інструментів, який надається використовуваній СУБД. Ці процедури повинні включати необхідні етапи, на яких безпосередньо виконуватиметься створення резервної копії як усієї БД із визначеною частотою, так і обов'язкове інкрементне копіювання, що виконується з вищою частотою.

У процедурах копіювання також може вказуватися, які ще частини системи (наприклад, прикладні програми), крім самих даних, повинні підлягати копіюванню.

3.3. Відновлення

Як і процедури копіювання, процедури відновлення також мають бути ретельно продумані і опрацьовані. Те, які саме процедури відновлення повинні виконуватися, визначаються типом відмови, яка мала місце (руйнування носія, відмова програмного забезпечення або устаткування системи), та особливостями методів відновлення, прийнятих у використовуваній СУБД.

3.4. Аудит

Одним з призначень процедури аудиту є перевірка того, чи всі передбачені засоби управління задіяні і чи відповідає рівень захищеності встановленим вимогам. В ході виконання інспекції аудитори можуть ознайомитися з використовуваними ручними процедурами, обстежувати комп'ютерні системи і перевірити стан всієї наявної документації на дану систему.

Зокрема, аудиторська перевірка передбачає контроль наступних використовуваних процедур і механізмів управління:

- ❑ підтримка точності даних, що вводяться;
- ❑ підтримка точності процедур обробки даних;
- ❑ запобігання появі і своєчасне виявлення помилок в процесі виконання програм; коректне тестування, документування і супровід розроблених програмних засобів;
- ❑ попередження несанкціонованої зміни програм:
- ❑ надання прав доступу і контроль за їх використанням;
- ❑ підтримка документації в актуальному стані.

Контрольні питання

1. Що таке захист інформації? Які основні завдання у сфері захисту інформації?
2. Назвіть ролі користувачів у сучасних СКБД.
3. Які існують методи захисту інформації в базах даних?
4. Які існують методи аутентифікації? Охарактеризуйте їх.
5. Що таке біометрична ідентифікація? Які існують біометричні механізми ідентифікації?
6. Що таке комплексна (або багатофакторна) ідентифікація? Які існують комбіновані системи захисту інформації?

ТЕМА 8. КІБЕРЗЛОЧИННІСТЬ ТА КІБЕРТЕРОРИЗМ

Віртуальний простір переймає від реального все підряд, у тому числі й злочинність у її нових формах і проявах.

Особливості кіберпростору, які злочинець використовує з метою досягнення злочинного результату:

1) віддаленість (дистанційність) доступу до предмета посягання з використанням кіберпростору, що забезпечує транскордонну складову такої злочинної діяльності, яка викликає необхідність вирішення слідчих питань територіальної юрисдикції;
2) оперативність створення, поширення, модифікації або знищення інформації в кіберпросторі, що є предметом злочинного посягання або слідом злочину – це сприяє значному прискоренню та якісному приховуванню злочинної діяльності;
3) віртуальність, що забезпечує відносну конфіденційність інформації про особу злочинця та можливість упливати на свідомість певної категорії осіб;
4) комунікативність, яка уможливлює створення злочинних груп та ефективну діяльність уже наявної організованої злочинності;
5) недосконаліть забезпечення інформаційної безпеки та правової охорони відносин у кіберпросторі, що надає злочинцю можливість уникати кримінальної відповідальності за вчинений злочин [12].

Кіберзлочинність – незаконні дії, які здійснюються людьми, що використовують інформаційні технології для злочинних цілей.

Кіберзлочинність включає в себе різні види злочинів, що здійснюються за допомогою комп'ютера і в мережі Інтернет. Об'єктом кіберзлочинів є персональні дані, банківські рахунки, паролі та інша особиста інформація як фізичних осіб, так і бізнесу та державного сектору. Кіберзлочинність є загрозою не тільки на національному, а й на глобальному рівні.

Кіберзлочин – це протиправне винне діяння (дія або бездіяльність), яке передбачає втручання в дані персональних комп'ютерів, комп'ютерних програм і комп'ютерних мереж, або діяння, вчинене за допомогою комп'ютерів та інших сучасних технологій, за яке передбачається кримінальна відповідальність та яке може створити особисту небезпеку для громадян, загрозу національній безпеці держави та світовій безпеці. Важливим кроком на шляху до визначення на національному рівні понять "кіберзлочин" та "кіберзлочинність" стало прийняття 5 жовтня 2017 року Закону України "Про основні засади забезпечення кібербезпеки України", де у п. 8 ч. 1 ст. 1 зазначається, що: **кіберзлочин**

(комп’ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України.

Мотиви вчинення кіберзлочинів:

1) злочини, вчинені з корисливих мотивів, що пов’язані з фінансово-економічною сферою відносин у кіберпросторі;
2) злочини, вчинені з соціально-економічних мотивів, що пов’язані з соціальною сферою відносин суб’єктів у кіберпросторі;
3) злочини, вчинені з антидержавно-політичних мотивів, пов’язані з державно-політичною сферою відносин суб’єктів у кіберпросторі;
4) злочини, вчинені з ідейних мотивів, пов’язані зі світоглядною сферою життя суб’єктів відносин у кіберпросторі.

Класифікація кіберзлочинів:

1) правопорушення проти конфіденційності, цілісності і доступності комп'ютерних даних і систем, зокрема:

- незаконний доступ, наприклад, шляхом злому, обману та іншими засобами;
- нелегальне перехоплення комп'ютерних даних;
- втручання у дані, включаючи навмисне пошкодження, знищення, погіршення, зміну або приховування комп'ютерної інформації без права на це;
- втручання у систему, включаючи умисне створення серйозних перешкод функціонуванню комп'ютерної системи, наприклад, шляхом розподілених атак на ключову інформаційну інфраструктуру;
- зловживання пристроями, тобто виготовлення, продаж, придбання для використання, розповсюдження пристроїв, комп'ютерних програм, комп'ютерних паролів або кодів доступу метою здійснення кіберзлочинів;
- 2) правопорушення, пов'язані з комп'ютерами, включаючи підробку і шахрайство, вчинені з використанням комп'ютерів;
- 3) правопорушення, пов'язані зі змістом інформації, зокрема, дитяча порнографія, расизм і ксенофобія;
- 4) правопорушення, пов'язані з порушенням авторських та суміжних прав, наприклад незаконне відтворення і використання комп'ютерних програм, аудіо/відео та інших видів цифрової продукції, а також баз даних і книг.

Найпоширеніші види кіберзлочинів

- ***Кардинг*** – шахрайські операції з кредитними картками (реквізитами кредитних карток), які не погоджені власником картки. Це може бути крадіжка чи незаконне отримання кредитної картки, викопіювання даних картки для подальшого її підроблення, викопіювання реквізитів картки для здійснення покупок через Інтернет без участі власника картки. У будь-якому разі основною метою злочинців є отримання доступу до чужих грошових коштів. Для досягнення цієї мети зловмисники вигадують різноманітні способи отримання потрібної інформації в неуважних і легковірних громадян. Одним із таких способів є фішинг.

- ***Фішинг*** – шахрайські дії, спрямовані на виманювання реквізитів картки у її власника. Зазвичай власник кредитної картки сам добровільно повідомляє шахраям потрібну інформацію.

Фішинг буває кількох видів:

• **СМС-фішинг**, коли потенційна жертва шахраїв отримує повідомлення про те, що її кредитну картку заблокував банк, а для розблокування необхідно надати реквізити, або ж про те, що власник картки отримав виграш, але потрібно заплатити за його доставку. Варіацій СМС-повідомлень безліч, тому потрібно бути особливо уважними й обачними, якщо ви отримуєте повідомлення.

• **Інтернет-фішинг**, коли шахраї створюють фішингові (підроблені) сторінки, які імітують офіційні сторінки банків, платіжних сервісів, інтернет-магазинів тощо. На жаль, не всі уважно перевіряють назву сайта, уводячи дані кредитної картки, що на руку кібершахраям.

•***Вішинг*** – це майже той самий фішинг, однак виманювання реквізитів картки зловмисники здійснюють за допомогою телефонних дзвінків (шахраї часто представляються працівниками банку й намагаються вивідати у власника картки ПІН-код чи примусити здійснити якісь дії зі своїм рахунком).

•***Скімінг*** – копіювання даних платіжної картки за допомогою спеціального пристрою (скімера). Зазвичай відбувається під час здійснення карткових операцій із банкоматами. Для отримання даних злочинці використовують міні-камери або змінні клавіатури.

•***Шимінг*** – модернізований різновид скімінгу. У цьому разі шахраї використовують майже непомітний прилад, який розміщують усередині картридера. Таким чином дані кредитки копіюються непомітно.

•***Онлайн-шахрайство*** – фальшиві інтернет-аукціони, інтернет-магазини, сайти й телекомунікаційні засоби зв'язку.

•***Піратство*** – протиправне розповсюдження об'єктів інтелектуальної власності в Інтернеті.

•**Malware (малварь, *мальваре)*** – створення та поширення вірусів і шкідливого програмного забезпечення.

•***Протиправний контент*** – контент, який пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості й насильства.

•***Рефайлінг*** – незаконна підміна телефонного трафіку [13].

Кримінально-правова охорона суспільних відносин у кіберпросторі в України. Конвенція Ради Європи про кіберзлочинність/

Сучасний стан правового регулювання боротьби зі злочинами, вчиненими у кіберпросторі, характеризується: відносною цілісністю системи актів у цьому напрямку на національнальному рівні; дезорганізованості системи нормативноправових актів на міжнародному рівні регулювання. Центральне місце на національному рівні в механізмі правового регулювання боротьби з такими злочинами займають норми: **Конвенції Ради Європи про кіберзлочинність від 23 листопаду 2001 року, Конвенції Організації Об'єднаних Націй проти транснаціональної організованої злочинності від 15 листопада 2000 року, загальні та спеціальні норми КК України, які передбачають численні конвенційні та альтернативні Конвенціям склади кримінальних правопорушень, що вчиняються в обстановці кіберпростору.** Складовими національної системи правового регулювання боротьби з такими злочинами виступають також норми галузевого законодавства, зокрема у сфері забезпечення національної, економічної та кібернетичної безпеки, захисту суспільства, дітей, інформації, авторських та суміжних прав.

10 найвідоміших українських хакерів

1. 20 травня 2003 року в тайському місті Бангкок на прохання американської влади був заарештований житель Тернополя **Максим Височанський** (справжнє прізвище Ковальчук) за звинуваченням у хакерстві. США обвинувачували українського хакера в порушення авторських прав виробників, незаконне поширення програмного забезпечення, відмивання грошей і незаконне проникнення до комп`ютерної мережі, що завдало компаніям-виробникам збитків у розмірі 3 млн доларів. Сам Височанський входив в десятку найбільш небезпечних кіберзлочинців, розшукуваних ФБР.

2. Улітку 2007 року в Туреччині був заарештований харків'янин **Максим Ястремський**, він же хакер Максик, який через Інтернет зламував кредитні картки і перекидав гроші на свої рахунки в 13 країнах світу. У такий спосіб він вкрав 11 млн. доларів США.

3.У травні 2008 року за американським ордером під час відпустки в Греції був затриманий українець **Єгор Шевельов**. Українця вважали учасником хакерської групи, яка займалася крадіжками платіжних карт і завдала матеріальних збитків на 4 млн доларів. За версією слідства, перебуваючи в Києві з листопада 2001 по серпень 2007 року, він продав 95 тисяч крадених карт, заробивши більше 600 тис. доларів США.

4. У червні 2014 року в Італії за американським ордером був затриманий українець **Сергій Вовненко**. За твердженням прокурорів, Вовненко під ніками Томас Рімкіс, Flycracker, Flyck, Fly (Муха), Centurion, MUXACC1, Strainer і Darklife з вересня 2010 по серпень 2012 року проникав зі спільниками в комп'ютери приватних осіб і компаній в США та інших країнах і викрадав дані, в тому числі імена користувачів і паролі, які давали хакерам доступ до чужих банківських рахунків, а також номери пластикових карт і особисті дані їх власників.

5.У листопаді 2014 року в США був затриманий киянин **Вадим Єрмолович**, якого звинуватили в тому, що він і його спільники викрали понад 150 тис. ще не опублікованих корпоративних прес-релізів, в яких були відомості про злиття і поглинання, а також звіти про фінансовий стан великих компаній. Ця інформація допомагала успішно грати на біржі: заробіток склав близько 100 млн. доларів США.

6.У липні 2016 року в Польщі був заарештований харків'янин **Артем Ваулін**, якого звинуватили в управлінні найбільшим торрентом в мережі KickassTorrents (KAT).

7. У лютому 2018 року в місті Бельсько-Бяла працівники Центрального слідчого бюро Польщі при співпраці з ФБР затримали 44-річного громадянина України, якого підозрюють у поширені шкідливого програмного забезпечення. Його підозрюють в участі в організованій злочинній групі, яка поширює шкідливе програмне забезпечення і причетна до хакерських атак. Як зазначили у поліції, втрати через злочинну діяльність угрупування, до якого належав українець, оцінюються в кілька сотень мільйонів доларів.

8. 25 лютого 2018 року в Києві кіберполіція затримала організатора міжнародної злочинної платформи «Avalanche» **Геннадія Капканова**, якого розшукували в 30 країнах світу. Мережа «Avalanche» функціонувала 7 років та щодня інфікувала по всьому світу до півмільйона комп'ютерів. Грошові втрати, пов'язані з кібератаками «Avalanche», за попередніми підрахунками, склали сотні мільйонів євро по всьому світу.

9. 6 березня 2018 року в місті Аліканте в Іспанії заарештували 34- річного українця **Дениса К**. (прізвище не розголошується), який з 2014 року проживає в Аліканте. За даними слідства, жертвами хакера стали понад 100 банків з 40 країн. Однак основні крадіжки ним були здійснені в банках Росії. За попередніми даними, сума викраденого перевищує 1 мільярд євро, хоча мова може йти і про значно більшу суму - аж до 10 мільярдів.

10. 13 березня 2018 року співробітники кіберполіції Чернівецької області спільно з німецькими колегами викрили двох хакерів з Чернівців - 28-річну жінку та 22-річного чоловіка (в інтересах слідства прізвища не розголошуються). За даними правоохоронців українські хакери входили до групи, яка з 2013 по 2016 рік злочинним шляхом діставала цифрові пакетні марки (DHL lables), які потім збувала із суттєвими знижками. Збитки клієнтів світового сервісу логістики DHL з головним офісом у Німеччині склали півтора мільйона євро.

Загалом правоохоронці задокументували понад 200 випадків незаконного продажу поштових пакетних марок. Отримані злочинним шляхом кошти негайно переводилися в готівку через валютні рахунки, відкриті в банках Кіпру та Іспанії [14].

11. Жовтень 2021. Кіберполіція викрила українського хакера у здійсненні вірусних атак на понад 100 іноземних компаній. Серед потерпілих – відомі світові енергетична та туристична компанії, а також розробники техніки. За відновлення доступу до закриптованих даних 25-річний хакер вимагав викуп. Збитки, завдані потерпілим, сягають 150 млн доларів США, повідомляє пресцентр Міністерства внутрішніх справ.

Ідентифікувати хакера вдалося в ході міжнародної поліцейської операції із залученням Інтерполу та Європолу, правоохоронців Франції та США. На криптогаманцях зловмисника заблоковано 1,3 млн доларів. За даними правоохоронців, вірусне програмне забезпечення потрапляло на техніку корпорацій шляхом зламу програми для віддаленої роботи користувача із комп'ютером (сервером), а також через спам-розсилки на корпоративні електронні поштові скриньки листів зі шкідливим вмістом.

Способи захисту від кіберзлочинів

Звісно, викладений вище перелік шахрайських дій не є виключним, але, дотримуючись кількох простих правил, можливо суттєво полегшити своє життя, зберігши і нерви, і гроші.

1. Зберігати ПІН-код кредитки, паролі, дані для входу в інтернет-банкінг у надійному місці, найкраще – у власній пам'яті.
2. У жодному разі не повідомляти третім особам паролі й реквізити картки.

3. Бути дуже обережними, здійснюючи інтернет-покупки. Користуватися лише офіційними й перевіреними сайтами.
4. Користуватися банкоматами, розміщеними у відділеннях банків або в місцях із відеонаглядом.
5. Не використовувати неліцензійне програмне забезпечення та не завантажувати його безкоштовно з підозрілих сайтів.
6. Не відкривати підозрілі листа та не переходити за незрозумілими посиланнями.
7. Обов'язково встановити антивірусні програми.
8. Здійснювати резервне копіювання важливих файлів і не надавати доступу стороннім особам до свого комп'ютера та/або телефону.

Кібертероризм

Термін **«кібертероризм»** був запропонований у 1980-х р. старшим науковим співробітником американського Інституту безпеки і розвідки (анг. – Institute for Security and Intelligence) Баррі Колліном, який використав його в контексті тенденції до переходу тероризму від фізичного до віртуального, породжуючого перетин та злиття цих світів.

Кібертероризм є рідновидом тероризму, однак поряд із такими його формами, як ядерний, біологічний, хімічний, екологічний, комп’ютерний (кібернетичний), з огляду на масову інформатизацію суспільства, несе одну із найбільших і найсерйозніших загроз людству.

Під кібертероризмом розуміють навмисну мотивовану атаку на інформацію, що обробляється комп’ютером, комп’ютерну систему або мережу, яка пов’язана з небезпекою для життя і здоров’я людей або настанням інших тяжких наслідків, якщо такі дії вчинені з метою порушення громадської безпеки, залякування населення, провокування військового конфлікту.

Таким чимом, можна визначити кібертероризм як похідний тероризму, об’єктом посягання якого є інформаційна безпека. Він є найбільш небезпечним, оскільки межі його визначені віртуальним середовищем, і знайти порушника дуже важко.

ЗАКОН УКРАЇНИ Про основні засади забезпечення кібербезпеки України Із змінами і доповненнями, внесеними Законами України від 21 червня 2018 року N 2469-VIII, від 17 червня 2020 року N 720-IX

Стаття 1. Визначення термінів

Стаття 2. Принципи застосування Закону

Стаття 3. Правові основи забезпечення кібербезпеки України

Стаття 4. Об'єкти кібербезпеки та кіберзахисту

Стаття 5. Суб'єкти забезпечення кібербезпеки
Стаття 6. Об'єкти критичної інфраструктури
Стаття 7. Принципи забезпечення кібербезпеки
Стаття 8. Національна система кібербезпеки

Служба безпеки України здійснює запобігання, виявлення, припинення та розкриття кримінальних правопорушень проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснює контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом та кібершпигунством, негласно перевіряє готовність об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; протидіє кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави; розслідує кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечує реагування на кіберінциденти у сфері державної безпеки;

Портрет кіберзлочинця

Характеризуючи особу комп'ютерного злочинця, необхідно відмітити основне, а саме: в електронну злочинність втягнуто широке коло осіб — від висококваліфікованих фахівців до дилетантів. Правопорушники мають різний соціальний статус та різний рівень освіти (навчання та виховання).

Слід зазначити, що типовий комп'ютерний злочинець знайомиться з комп'ютером у дитинстві, обожнює його. Для нього комп'ютерна система — це таємниця, яку необхідно дослідити та ефективно використовувати в реальному житті. Уже в школі, а потім у вищих навчальних закладах, студенти вивчають основи комп'ютерної науки (кібернетики, інформатики, нейробіоніки, нейрокібернетики). У більшості випадків комп'ютерні злочинці набувають знань, навиків і вмінь в ліцеї, коледжі або в університеті. Самостійне вивчення ЕОМ, інформаційних технологій, систем і мереж зв'язку (дарпанет, фідонет, інтернет тощо) також може бути надійним фундаментом майбутньої злочинної діяльності.

Аналіз вітчизняної і зарубіжної судової практики та вивчення літературних наукових джерел свідчать, що типовий вік комп'ютерних правопорушників коливається в досить широких межах (у середньому 15 — 45 років). Згідно матеріалів досліджень вік 33 % комп'ютерних злочинців на момент скоєння злочину не перевищував 20 років, 13% були старші за 40 років і 54% мали вік від 20 до 40 років.

Отже, сучасні хакери і кракери — це не завжди безтурботні, слухняні хлопчики, як вважали раніше. Для прикладу наведемо віковий розподіл комп'ютерних злочинців, які були заарештовані в США за комп'ютерні злочини. Близько 83% осіб цієї категорії — це чоловіки, але слід зауважити, що частка жінок сьогодні швидко зростає через професійну орієнтацію деяких спеціальностей та посад, які обіймають в основному жінки (секретар, бухгалтер, економіст, менеджер, касир, контролер, діловод тощо). За даними соціологів США, приблизно третину комп'ютерних злочинців становлять жінки.

Більшість комп'ютерних правопорушників у віці від 14 до 21 року навчаються в коледжі або університеті. Про це свідчить той факт, що найбільше комп'ютерних вірусів виникає в період літніх або зимових канікул. Ці комп'ютерні правопорушники добре встигають з одних навчальних дисциплін, але можуть відставати з інших. Цікаво, що значна частка програмістів, наприклад, погано пише документацію або має слабкі мовні навики.

Ці особи мають IQ вищий від середнього, оскільки для написання компактної програми необхідний високий рівень інтелекту. Цікаво, що 77% комп'ютерних злочинців, які вчинили кібератаку чи інший комп'ютерний злочин, мали середній рівень інтелектуального розвитку, 21% вищий від середнього і лише 2% нижчий від середнього. При цьому 20% комп'ютерних злочинців мали середню освіту, 20% — середню спеціальну і 40% — вищу.

Основними характеристиками особи комп'ютерного злочинця є активна життєва позиція, оригінальність (нестандартність) мислення і поведінки, обережність, уважність. Такі особи зосереджують увагу на розумінні, передбаченні й управлінні процесами. Це є основою їх компетенції та професійної майстерності. До того ж, вони відзначаються уважністю і пильністю, їхні дії витончені, хитрі, супроводжуються відмінним маскуванням.

В аспекті психофізіологічної характеристики — це, як правило, яскраво мисляча й творча особа, професіонал у своїй справі, здатний іти на технічний виклик, бажаний працівник. Водночас — це людина, яка боїться втратити свій авторитет або професійний чи соціальний статус у рамках соціальної групи, або ж вона побоюється на роботі глузувань колег. Поведінка рідко відхиляється від загальноприйнятих у суспільстві соціальних норм. Крім того, практика свідчить, що комп'ютерні злочинці у своїй більшості не мають взагалі кримінального минулого.

Важливо зазначити те, що значна частина комп'ютерних злочинів здійснюється індивідуально. Але останнім часом спостерігається тенденція до співучасті в групових кібернетичних посяганнях [15].

Боротьба із кібертероризмом має включати усі дієві шляхи та методи захисту і попередження вчинення таких злочинів:

– належне законодавче врегулювання поняття «кіберзлочинності», «кіберзлочину», його видів, основних характеристик, відповідальності за його вчинення, порядку притягнення особи до відповідальності;

– створення відповідних державних органів, із безумовним залученням спеціалістів у сфері комп'ютерних технологій, для захисту та боротьби з кібертероризмом;

– розроблення стійкого системного захисту інформації, інформаційних технологій, захисту ЕОМ;

– належне фінансування такого роду діяльності із привенції та захисту інформаційної безпеки;

– міжнародне співробітництво як у теоретичних розробках, так і у практичній діяльності.

Внаслідок вчинення кібертерористичних актів може бути викрадена інформація, яка є складовою державної таємниці, порушена система життєзабезпечення держави, що є загрозою для безпеки країни і за своєю суттю є порушенням загальноприйнятих принципів міжнародного права.

Отже, акти кібертероризму постають як реальна загроза не тільки для окремих комп'ютерних мереж будь-яких корпорацій чи приватних осіб, але і для інформаційних та комунікаційних систем цілої держави, а тому їх необхідно кваліфікувати як сучасні, навіть надсучасні, форми вчинення акту агресії, оскільки наслідки таких атак сміливо можна порівнювати з наслідками озброєного нападу [16].

Контрольні питання:

1. Що таке кіберзлочин? Яка класифікація кіберзлочинів?
2. Що таке кібертероризм? В чому полянає особливіть кібертероризму?
3. Назвіть найвідоміших українських хакерів та їх злочини.
4. Охарактеризуйте портрет кіберзлочинця.
5. Назвіть методи захисту і попередження вчинення кіберзлочинів.

ТЕМА 9. КРИТИЧНА ІНФРАСТРУКТУРА ТА ЇЇ ЗАХИСТ

Визначення основних термінів

1) акт несанкціонованого втручання - діяння, що створило загрозу безпечному функціонуванню об'єкта критичної інфраструктури та призвело до одного або декількох з таких наслідків: порушило його безперервність і стійкість; створило реальні чи потенційні загрози національній безпеці;

2) безпека критичної інфраструктури - стан захищеності критичної інфраструктури, за якого забезпечується функціональність, безперервність роботи, цілісність і стійкість критичної інфраструктури;

3) державна система захисту критичної інфраструктури - система суб'єктів із забезпечення формування та реалізації державної політики у сфері захисту критичної інфраструктури;

4) життєво важливі послуги - послуги, надання яких забезпечується державними установами, підприємствами та організаціями будь-якої форми власності і збої та переривання у наданні яких призводять до швидких негативних наслідків для національної безпеки;

5) життєво важливі функції - функції, що виконуються органами державної влади, державними установами, підприємствами та організаціями будь-якої форми власності, порушення яких призводить до швидких негативних наслідків для національної безпеки;

6) захист критичної інфраструктури - всі види діяльності, спрямовані на своєчасне виявлення, запобігання і нейтралізацію загроз безпеці об'єктів критичної інфраструктури, а також мінімізацію та ліквідацію наслідків у разі їх реалізації [17].

Об'єкти критичної інфраструктури

До об'єктів критичної інфраструктури відносяться підприємства, установи, організації незалежно від форми власності, які:

1) провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, оборонно-промислового комплексу, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторах;

2) надають послуги у сферах життєзабезпечення населення, зокрема у сферах централізованого водопостачання, централізованого водовідведення, постачання теплової енергії, гарячої води, електричної енергії і газу, виробництва харчових продуктів, охорони здоров'я;

3) включені до переліку підприємств, що мають стратегічне значення для економіки і безпеки держави;

4) підлягають охороні та обороні в умовах надзвичайного стану і особливого періоду;

5) є об'єктами підвищеної небезпеки;

6) є об'єктами, які мають загальнодержавне значення, розгалужені зв'язки та значний вплив на іншу інфраструктуру;

7) є об'єктами, порушення функціонування яких призведе до кризової ситуації регіонального значення [18].

Пріоритетами забезпечення безпеки критичної інфраструктури визначено:

– комплексне вдосконалення правової основи захисту критичної інфраструктури, створення системи державного управління її безпекою;

– посилення охорони об’єктів критичної інфраструктури, зокрема енергетичної і транспортної;

– налагодження співробітництва між суб’єктами захисту критичної інфраструктури, розвиток державно-приватного партнерства у сфері запобігання надзвичайним ситуаціям та реагування на них;

– розробка та запровадження механізмів обміну інформацією між державними органами, приватним сектором і населенням стосовно загроз критичній інфраструктурі та захисту чутливої інформації у цій сфері;

– профілактика техногенних аварій та оперативне і адекватне реагування на них, локалізація і мінімізація їх наслідків;

– розвиток міжнародного співробітництва у цій сфері [19].

Рис. 62 Порядок формування переліку об'єктів критичної інфраструктури

Рис. 63 Захист інформації в критичних системах інформаційної інфраструктури

Захист інформації в критичних системах інформаційної інфраструктури розглядається в контексті критично важливих секторів; захист критичної інформаційної інфраструктури передбачає забезпечення гарантії того, що подібні системи та мережі стійкі відносно ризиків інформаційної безпеки, мережевої безпеки, безпеки Інтернет, так само як і ризиків кібербезпеки.

Інформаційні системи об’єктів критичної інфраструктури зазвичай являються об’єктом захисту, як цілісні утворення. В той же час, їх складові елементи: обслуговуючий персонал, математичне, програмне, технічне, інформаційне забезпечення тощо можливо розглядати, як окремі об’єкти захисту від кіберзагроз.

Кіберзагрози для інформаційних систем об’єктів критичної інфраструктури можуть виходити з різних джерел: навмисних, ненавмисних, природних. Основними з них є: зловмисники, оператори ботнету, злочинні групи, іноземні спецслужби, інсайдери, фішери, сніфери, спамери, автори шпигунського і шкідливого програмного забезпечення, терористи, промислові шпигуни тощо.

На наступному малюнку приведена модель взаємодії елементів інформаційної системи об’єкту критичної інфраструктури. На ньому зображено, яким чином впливає кожна із складових систем (організаційна, технічна, персонал) на забезпечення кібербезпеки інформаційних систем об’єктів критичної інфраструктури.

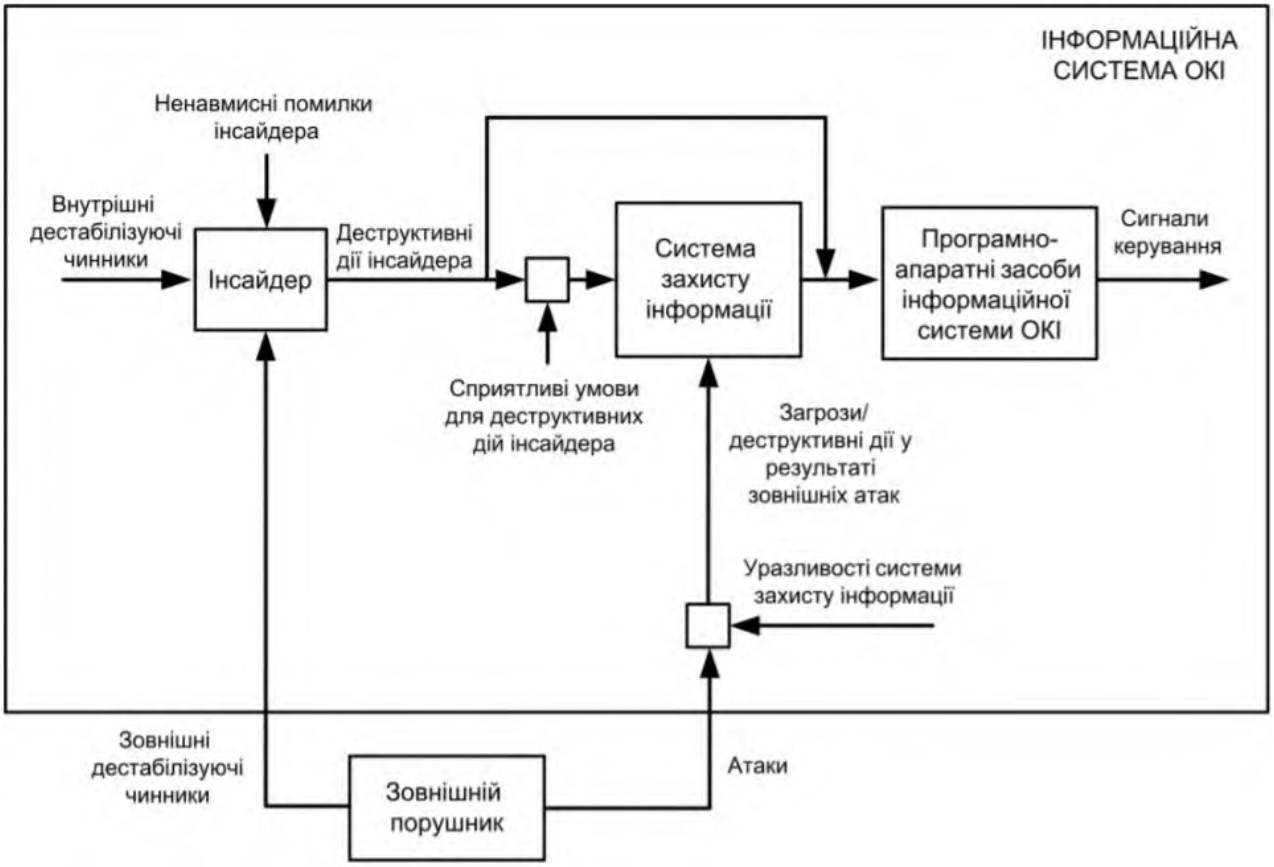

Рис. 64 Модель взаємодії елементів інформаційної системи об’єкту критичної інфраструктури

Суспільні, державні інтереси та відносини, яким може бути завдано шкоди, окреслюють так:

1) функціонування суспільства, соціально-економічного розвитку держави та забезпечення національної безпеки;
2) життєво важливі національні інтереси України;
3) інтереси економіки і безпеки держави, суспільства, населення;
4) національна безпека й оборона, природне середовище;
5) економічна, соціально-політична, військова, екологічна безпека;
6) соціальна й економічна сфери держави;
7) рівень обороноздатності та національної безпеки;
8) життєдіяльність суспільства, соціально-економічного розвитку країни та забезпечення національної безпеки.

Джерела кіберзагроз для інформаційних систем об’єктів критичної інфраструктури можуть знаходитись як ззовні (зовнішній порушник) так і зсередини (інсайдер).

При цьому, кібератакам зовнішнього порушника протистоїть система захисту інформації інформаційної системи об'єктів критичної інфраструктури, до функцій якої обов'язково повинні входити:

- ✓ захист периметра мережі;
- ✓ забезпечення безпеки міжмережевих взаємодій;
- ✓ моніторинг і аудит безпеки;
- ✓ виявлення і запобігання діям атак;
- ✓ резервне копіювання і відновлення даних;
- ✓ аналіз захищеності і керування політикою безпеки;
- ✓ контроль цілісності даних;
- ✓ захист від шкідливого програмного забезпечення;
- ✓ фільтрація контенту і запобігання витоку конфіденційної інформації;
- ✓ установка оновлень програмного забезпечення;
- ✓ адміністрування безпеки.

Захист таких систем повинен розглядатися по наступних напрямках:

- ➢ захист інформаційних і фізичних компонентів інформаційної системи об’єктів критичної інфраструктури;
- ➢ технічний захист інформації інформаційних систем об'єктів критичної інфраструктури;
- ➢ захист процесів, процедур і програм обробки інформації інформаційних систем об’єктів критичної інфраструктури;
- ➢ захист каналів зв'язку інформаційних систем об’єктів критичної інфраструктури; придушення побічних електромагнітних випромінювань;
- ➢ керування та контроль системою захисту.

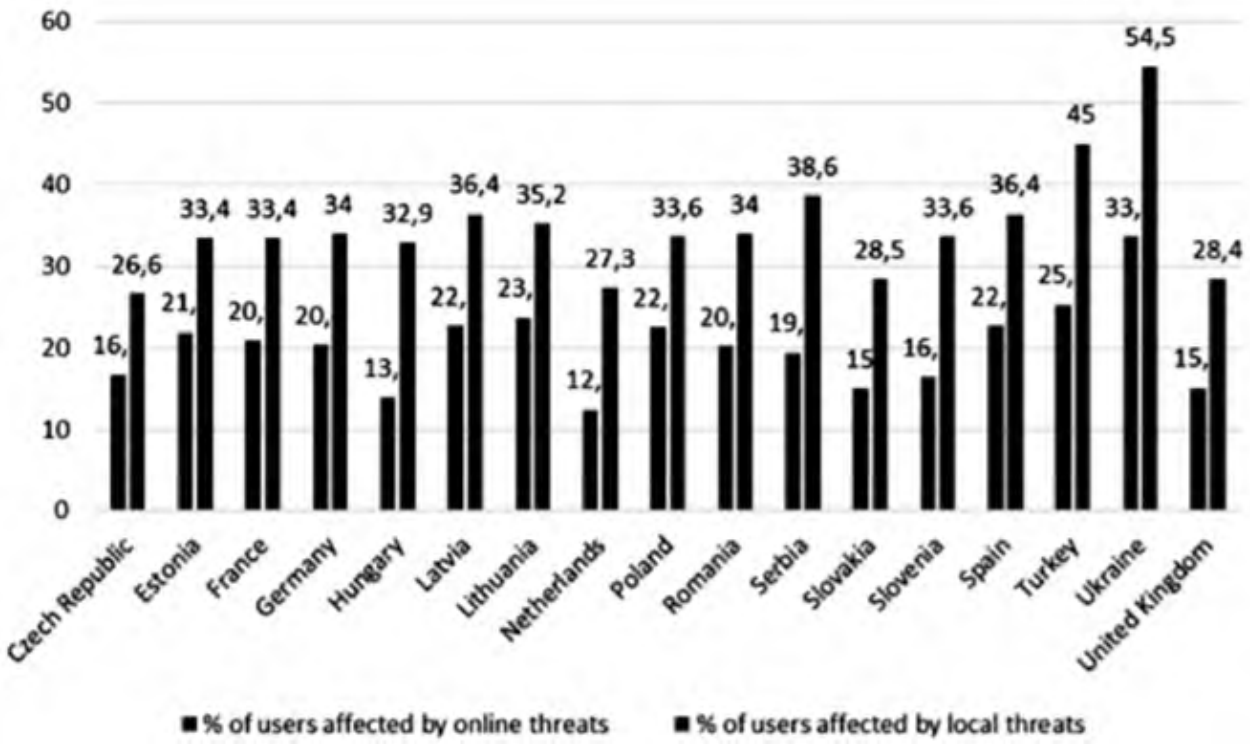

Рис. 65 Статистика кіберзагроз

Таким чином, із урахуванням викладеного можна зазначити, що на стан забезпечення кібербезпеки інформаційної системи об’єкта критичної інфраструктури впливають такі фактори:

– наявність необхідної та достатньої нормативно-правової бази з питань забезпечення кібербезпеки інформаційних систем об’єктів критичної інфраструктури;

– наявність джерел кіберзагроз, їх можливості, тип, вид, мета, мотиви, зацікавленість у здійсненні кібератак;

– наявність уразливостей у системах кіберзахисту, які можуть використовуватися при здійсненні кібератак;

– наявність чи відсутність сприятливих умов для реалізації кіберзагроз;

– привабливість активів, на які власне і спрямовуються кібератаки;

– наслідки від можливої реалізації кіберзагроз;

– рівень фахової підготовки співробітників, відповідальних за кібербезпеку на всіх рівнях: організація, підприємство, галузь, відомство тощо.

Також, одним із таких показників, на нашу думку може бути кількість кібератак за певний інтервал часу – рік, півріччя, квартал, місяць.

Крім того, одним із суттєвих показників може бути спрямованість кібератак – органи державної влади, енергетика, банківська сфера, силові відомства, дипломатичні установи тощо.

Корисним для оцінки та аналізу стану кібербезпеки може бути поєднання кількості кібератак за певний інтервал часу з урахуванням їх спрямованості. Це дасть змогу визначити вектор зацікавленості зловмисника та їх мету – кібердиверсія, кіберрозвідка, кібершпигунство тощо по відношенню до кожного напрямку [20].

Кібернетичні системи відеоспостереження

Кібернетичні системи відеоспостереження - це впорядкована сукупність об'єктів (елементів системи), що взаємодіють і взаємопов'язаних між собою, які здатні сприймати, запам'ятовувати і переробляти відеоінформацію, а також обмінюватися нею.

Кібернетична система відеоспостереження є відкритою. Має як вхідні, так і вихідні канали, по яких вона обмінюється сигналами із зовнішнім середовищем. Відомо, що відкрита кібернетична система може розглядатися як перетворювач вхідних сигналів у вихідні, тобто як перетворювач інформації. Тому вважаємо, що кібернетична система відеоспостереження складається з рецепторів у вигляді датчиків або детекторів, мережі телекомунікації (каналів прямого і зворотного зв'язку) та аналізаторів сигналів.

Перелік функцій, якими повинні володіти кібернетичні системи відеоспостереження для забезпечення безпеки об'єктів підприємства критичної інфраструктури:

1) Організувати автоматизований контроль доступу автомобілів на територію об'єкта, що спостерігається;
2) Організувати автоматизований контроль доступу людей в приміщення об'єкта, що спостерігається;
3) Забезпечувати безперервну відеотрансляцію і запис незважаючи на форс-мажорні ситуації;
4) Покрити більшу зону спостереження об'єкта меншою кількістю камер;
5) Скоротити вартість системи відеоспостереження об'єкта;
6) Отримувати негайні повідомлення на монітор, смартфон або електронну пошту: про відсутність співробітника на своєму робочому місці; про перетин будь-ким контрольної лінії або периметра; про появу людини в забороненому місці; про фіксацію відсутності спеціального одягу, наприклад. каски на голові працівника; про виявлення диму або вогню на території об'єкта; про будь-яких аномально гучних звуках в зоні відеоспостереження на території об'єкта; про виявлення несправності камер відеоспостереження об'єкта;
7) Виконувати автоматично відео аналітику щодо: розпізнавання автономерів, розпізнавання осіб; резервування каналу з відображенням; управління PTZ-камерами; розгортки fisheye камер: контролю активності персоналу; трекінгу; виявлення осіб; відсутності заданих засобів захисту на особі; появи диму і вогню; появи гучного звуку та ознак саботажу

Розпізнавання автономерів. Застосовується для автоматизації контролю пропуску автомобільного транспорту на територію об'єкта. Ця функція дозволяє додавати в базу даних «білі» і «чорні» номери автомобілів; зберігати час і дату розпізнавання, номерний знак а також відео фрагмент проїзду автомобіля, номер якого зафіксований камерою; вивантажувати списки номерів в формати XLS і CSV.

За допомогою системи «Розпізнавання автономерів» можливо: запобігати несанкціоноване проникнення транспортних засобів на територію об'єкта; організувати автоматичне відкривання шлагбаума при в'їзді / виїзді автомобілів з території об'єкта. Таким чином, створюється можливість забезпечити безпеку об'єкта, а також знизити витрати на забезпечення безпеки.

Рис. 66 Розпізнавання автономерів

Розпізнавання осіб. Застосовується для автоматизації та контролю доступу людей на територію об'єкта. Ця функція дозволяє: інтегрувати модуль з системою контролю і управління доступом (СКУД) до об'єкта; створювати базу фото осіб зі статусами «довірена» і «чорний список»; отримувати автоматичні повідомлення на монітор, телефон, e-mail про спроби проникнення осіб, які не мають прав доступу; шукати фрагменти з виявленим особою в відео-архіву, шукати людей в відео-архіву по фотографіях.

За допомогою системи «Розпізнавання осіб» можна контролювати допуск персонал в усі приміщення об'єкта, а саме: забезпечити автоматичний допуск на територію та до приміщень об'єкта працівників, які мають дозвіл на це і контролювати час їх перебування там; запобігати проникненню на територію і в приміщення об'єкта осіб, які не мають на це дозволу. Таким чином, створюється можливість забезпечити високий рівень безпеки працівників та інфраструктури на основі біометричних методів контролю.

Рис. 67 Розпізнавання осіб

Резервування каналу з відображенням. Дозволяє забезпечувати відео потік і запис відео незалежно від форс-мажорних ситуацій. Ця функція дозволяє встановлювати спеціальний модуль на кожній камері, запис з якої критично важлива. Якщо сервер разом з камерами, на яких встановлено модуль, вийде з ладу, ці камери будуть переведені на резервний сервер автоматично. Це забезпечить постійну передачу відеопотоку і запобіжить втрату архіву, поки сервер знаходиться у відключеному стані.

Завдяки «Резервуванню каналу з відображенням» видсютня втрата жодної хвилини відео потоку. Є можливість отримувати все оповіщення на смартфон або на електронну пошту, не дивлячись на проблеми з сервером. Таким чином, створюється можливість забезпечити безперервне отримання інформації для організації безпеки працівників і не допускати збитків майну, інфраструктурі об'єкта.

Рис. 68 Резервуванню каналу з відображенням

Трекінг. Визначення місця розташування рухомих об'єктів в часі за допомогою камери застосовується для мінімізації збитку майна, викликаного діями третіх осіб, а також для зниження ймовірності терористичних актів на території об'єкта. Ця функція дозволяє налаштувати: мінімальний розмір об'єктів, рух яких необхідно відстежувати; максимальний зсув об'єкта від кадру до кадру - не більше 1/5 кадру.

Завдяки функції «Трекінг» можна отримувати повідомлення на монітор, смартфон або електронну пошту кожен раз коли: об'єкт перетинає контрольну лінію (вторгнення на територію та інші); об'єкт переміщується по території; об'єкт знаходиться на території тривалий час. Також можна здійснювати пошук по архіву фрагментів відео, на яких об'єкт перетинає контрольну лінію або знаходиться в контрольній зоні. Крім того, можна заощадити ємність сервера, налаштувавши програму так, щоб запис починалася тільки в разі виникнення контрольного події. Таким чином, не обов'язково сидіти перед моніторами для відеоспостереження 24 години на добу. Завдяки трекінгу можна відправити службу безпеки в небезпечну зону для нейтралізації правопорушника і таким чином: забезпечити безпеку працівників; запобігти можливій терористичну атаку; захистити майно та інфраструктуру

Рис. 69 Визначення місця розташування рухомих об’єктів в часі за допомогою камери

Детектор саботажу. Детектор саботажу TRASSIR Sabotage Detector контролює якість відеосигналу. У великих системах забезпечення безпеки встежити за станом безлічі камер дуже складно. Детектори саботажу покликані інформувати служби та операторів про нештатні ситуації із зображенням. Модуль здійснює автоматичне виявлення випадків расфокусування камери, зміни поля зору, закриття об'єктиву або його засвічення, розпізнавання обриву зв'язку і втрати сигналу. Детектор має можливість настройки реакції на інцидент, наприклад, залучення уваги оператора звуковим сигналом і / або повідомленням, включення сирени, управління сухими контактами і ін.

Завдяки «Детектор саботажу» можна отримувати інформацію про непрацездатність системи відеоспостереження та оперативне її відновлювати. Коли виникає будь-яка з вказаних подій, відправляється негайне повідомлення на монітор, смартфон або на електронну пошту.

Таким чином, ви можете безперервно забезпечувати безпеку працівників, а також майна, інфраструктури.

Рис. 70 Детектор саботажу

Кібернетичні системи відеоспостереження повинні виконувати наступний перелік функцій:

1) Організувати автоматизований контроль доступу автомобілів на територію об'єкта, що спостерігається;

2) Організувати автоматизований контроль доступу людей в приміщення об'єкта, що спостерігається;

3) Забезпечувати безперервну відео трансляцію і запис незважаючи на форс-мажорні ситуації;

4) Створювати покрити більшу зону спостереження об'єкта меншою кількістю камер;

5) Скоротити вартість системи відеоспостереження об'єкта;

6) Отримувати негайні повідомлення на монітор, смартфон або електронну пошту;

7) Виконувати автоматично відео аналітику щодо: розпізнавання автономерів, розпізнавання осіб; резервування каналу з відображенням; управління PTZкамерами; розгортці fisheye-камер: контролю активності персоналу; трекінгу; виявлення осіб; відсутності заданих засобів захисту на особі; появи диму і вогню; появи гучного звуку та ознак саботажу [21].

Контрольні питання:

1. Що відноситься до об'єктів критичної інфраструктури?
2. Що є пріоритетами забезпечення безпеки критичної інфраструктури?
3. Опишіть модель взаємодії елементів інформаційної системи об’єкту критичної інфраструктури.
4. Які фактори впливають на стан забезпечення кібербезпеки інформаційної системи об’єкта критичної інфраструктури?
5. Що таке кібернетичні системи відеоспостереження? Де вони можуть бути застосовані?
6. Назвіть функції, якими повинні володіти кібернетичні системи відеоспостереження для забезпечення безпеки об'єктів підприємства критичної інфраструктури.

ТЕМА 10. МУЛЬТИМЕДІЙНІ ВИДАННЯ

Поява систем мультимедіа спричинила революцію в таких галузях, як освіта, комп'ютерний тренінг, бізнес, і в багатьох інших сферах професійної діяльності. Інформаційні технології на базі мультимедіа забезпечують сьогоденну динаміку зростання процесу інформатизації суспільства. Усе це диктує певні вимоги для видавничополіграфічної галузі, які пов'язані з необхідністю подальшого впровадження сучасних технологій мультимедіа в процес видавництва.

Мультимедіа-технології засновані на комплексному представленні даних будь-якого типу. Такі технології забезпечують сумісну обробку символів, тексту, таблиць, графіків, зображень, документів, звуку, мови, що створює мультисередовище.

У даний час мультимедіа-технології є областю інформаційних технологій, що бурхливо розвивається. У цьому напрямі активно працює значна кількість крупних і дрібних фірм, технічних університетів і студій. Як результат їх діяльності, випущено і продовжують розроблятися численні інструментальні засоби для проектування і виготовлення всіляких мультимедійних продуктів. Для ефективного використовування подібних інструментів розробник мультимедійних видань повинен чітко розуміти особливості представлення мультимедійної інформації і її місце в поліграфії. У зв'язку з цим виникає об'єктивна необхідність аналізу поняття "мультимедіа" і вивчення сучасних форматів її уявлення.

Визначення мультимедійної інформації

Термін "інформація" має багато тлумачень і визначень. Енциклопедія кібернетики трактує інформацію (лат. informatio – роз'яснення, виклад, обізнаність) як одну із найзагальніших понять науки.

У вузькому значенні термін "інформація" – це будь-які дані, що є об'єктом зберігання, передачі і перетворення. Як і безліч понять, що прийшли з англійської мови, "мультимедіа" не має однозначного тлумачення. Розрізняють два терміни – "multimedia" і "multiple media" (мультимедіа і множинні середовища передачі інформації). У даний час існує більше десятка визначень терміна мультимедіа. У табл. 1 наведено декілька прикладів подібних визначень. З наведених прикладів можна зробити висновок, що на сьогодні склалося три різні розуміння поняття "мультимедіа.

Мультимедіа як ідея – новий підхід до зберігання інформації різного типу.

Мультимедіа як ідеологія – це прагнення збільшити ефективність спілкування людини і комп'ютера за рахунок застосування нових каналів передачі інформації.

Мультимедіа як технологія – сукупність організаційних технічних і програмних засобів, а також службовців для розробки мультимедіа.

Місце мультимедійних видань в поліграфії

Перше офіційне визначення електронного видання було подано в міжнародному стандарті ISO 9707: 1991 "Information and documentation – Statistics on the production and distribution of books, newspapers, periodicals and electronic publications", де електронне видання (electronic publication) розуміється як документ, який публікується у машиночитаній формі та доступний для публіки, включає файли даних та програмне забезпечення (прикладні програми); може бути записаним на папері, магнітному, оптичному та інших медіа, призначених для обробки комп'ютером або периферійними пристроями.

Дослідниками у галузі інформаційної діяльності електронне видання трактується як самостійний (тобто може використовуватися незалежно від його виробника, зокрема, й через телекомунікаційні мережі), закінчений (тобто не змінюється з плином часу) продукт, який містить інформацію, представлену в електронній формі, і призначений для довготривалого зберігання, всі копії якого відповідають оригіналу.

Відповідно до ГОСТ 73.83-2001 електронне видання – це електронний документ, або група електронних документів, які пройшли редакційно-видавниче опрацювання, мають вихідні відомості і призначені для розповсюдження у незмінному вигляді.

Це визначення вміщує такі типи електронних видань: текстове (символьне), зображувальне, звукове, програмний продукт та мультимедіа або їх комбінації, тобто відповідає визначенням електронних ресурсів, наданим в стандартах ISBD(ER), UNIMARC, AACR2.

Серед великого різноманіття продуктів поліграфії електронні видання займають особливе місце (рис. Х). Поява електронних книг ініціювала дискусію про майбутнє поліграфії і зокрема паперової книги: чи потрібна вона взагалі, які її перспективи і яке місце видавця в нових умовах. У електронних видань багато загального з іншими видами видавничої продукції (книгами, журналами, образотворчою продукцією та ін.), але їх унікальні можливості не входять в рамки традиційного уявлення про видавничий процес у цілому. Електронне видання повною мірою відповідає своєму призначенню тоді, коли в ньому реалізовані функції інформаційно-пошукової і інформаційно-довідкової систем,

воно не дублює книгу, а містить те уявлення про інформацію, яке поліграфічне видання дати не може.

Рис. 71 Місце мультимедійних видань в поліграфії

Класифікація електронних видань

Класифікувати об’єкти такої багатогранної системи як електронні видання надзвичайно складно: безліч сторін проблеми породжує безліч критеріїв класифікації. На рис. 1 наведено один з можливих варіантів класифікаційних критеріїв електронних видань, причому на ньому приведено далеко не всі з них. Для деяких виділених класів можна привести подальшу типізацію. Розглянемо ці критерії більш детально.

Рис. 72 Класифікація електроних видань

За природою уявлення основної інформації електронні видання (ЕВ) можуть бути розділені на такі основні групи:

- текстове (символьне) електронне видання – ЕВ, що містить переважно текстову інформацію, представлену у формі, що допускає посимвольну обробку;
- образотворче електронне видання – ЕВ, що містить переважно електронні зразки об’єктів, що допускають перегляд і друкарське відтворення, але не допускають посимвольну обробку;

- звукове електронне видання – цифрове представлення звукової інформації, у формі, яка допускає її прослуховування, але не призначена для друкарського відтворення;
- програмний продукт – самостійний, відчужуваний твір, що є публікацією тексту програми або програм на мові програмування або у вигляді виконуваного коду;
- мультимедійне електронне видання – ЕВ, в якому присутня інформація різних типів.

За технологією розповсюдження визначають такі види електронних видань:

- локальні електронні видання – призначені для локального використання, видаються у вигляді певної кількості ідентичних екземплярів (тиражу) на носіях, що переносяться (окремих фізичних носіях);
- мережеві електронні документи, які доступні потенційно необмеженій кількості користувачів через телекомунікаційні мережі;
- електронні ресурси (документи або видання) комбінованого розповсюдження, які можуть використовуватися як локально, так і через мережі.

За характером взаємодії з користувачем відрізняють:

- детерміновані електронні видання, параметри, зміст і спосіб взаємодії з якими визначені виробником і не можуть змінюватися користувачем;
- не детерміновані (інтерактивні) ресурси, параметри, зміст і спосіб взаємодії з якими прямо або побічно встановлює користувач відповідно до його мети, інтересів, рівня підготовки, тощо на основі інформації та алгоритмів, визначених виробником.

За періодичністю визначають:

- неперіодичне електронне видання – ЕВ, які виходять одноразово;
- серіальне – ЕВ, яке виходить за невстановленою тривалістю;
- періодичне – ЕВ, яке виходить через певні інтервали часу;
- ЕВ, випуск яких продовжується у міру накопичення матеріалу;
- ЕВ, що оновлюється (кожний наступний випуск містить актуальну інформацію попереднього випуску).

За структурою електронні видання можуть бути розділені на однорідні та гіпертекстові.

Складовими частинами будь-якого електронного видання є деякі інформаційні об’єкти, що мають зв’язки один з одним. Якщо такі зв’язки лінійні, то можна говорити про однорідні видання. Такий вид видань практично цілком співпадає з презентаційними виданнями.

За наявності складної організації міжоб'єктних зв'язків (деревовидна або мережна структура), слід говорити про гіпертекстові або, у разі мультимедійного видання – гипермедійні електронні видання. Таким чином, поняття гіпермедіа означає об'єднання двох понять: мультимедіа і гіпертекст.

Наведені структури видань підрозділяються на однотомні, багатотомні та електронні серії, що вміщують сукупність однотипних томів.

Однотомне електронне видання розміщується на одному носії. Багатотомне електронне видання складається з двох і більше пронумерованих частин, кожна з яких представлена на окремому носії і є єдиним цілим за змістом і оформленням. Електронна серія включає сукупність томів, об'єднаних спільністю задуму, тематики, цільовим призначенням, що виходять в однотипному оформленні.

Область застосування електронного видання також можна використовувати як критерій класифікації. Це можуть бути інформаційно-пошукові системи, презентаційні, програмні або імітаційні видання. Найбільш поширені перші, що використовуються для пошуку необхідної інформації серед відносно великого масиву даних. Презентаційні електронні видання надають інформацію в строго безумовному порядку, заданому при їх створенні. Окремо слід виділити імітаційні видання, що надають користувачу уявлення віртуальної реальності. Поширюване сьогодні програмне забезпечення також потрапляє під визначення електронного видання, що приводить до програмного типу видань.

Окрім подібної типології електронні видання можна класифікувати по соціальних групах, в яких вони застосовуються. При цьому видання можуть бути художніми (для розваги і дозвілля), науковими (для підтримки наукового процесу), технічними (для використовування в інженерній діяльності), документальними (для підтримки документообігу) і т. д.

У технічних і наукових публікацій є цілий ряд обов'язкових особливостей: якість представлення інформації не нижче, ніж у поліграфічних видань; висока швидкість створення і низька вартість; читабельність на всіх типах сучасних комп'ютерів; можливість містити будь-яку інформацію; сумісність з будь-якими засобами доставки.

За поліграфічним критерієм класифікації визначають оригінал-макет видання – оригінал, призначений для безпосередньої репродукції. У сучасній практиці він зазвичай виконується в електронній формі і виводиться на папір або плівку за допомогою принтерів. До цього ж типу можна віднести редакційні електронні версії видань, які використовуються і в редакторському процесі, і для аналітичної роботи, і для випереджального доступу до видання читачами.

Електронні копії поліграфічних видань також займають в сучасному світі значне місце. Вони, на відміну від оригінал-макетів, будуються вже після випуску поліграфічної продукції на її основі і можуть містити значно більший об’єм даних з розвинутими засобами доступу і пошуку інформації. І, нарешті, власне електронні видання, які ніякого відношення до поліграфії не мають. Такі видання розробляються "з нуля" і у зв’язку з цим представляють найбільший інтерес для вивчення.

Мультимедійні видання також можна розглядати як один з видів мультимедійних проектів. Основні типи мультимедіа-проектів (рис. 2) не є промисловими стандартами – це лише вельми узагальнені групи, в які вписується розробка, що виконана за допомогою засобів мультимедіа (наприклад, Flash, Director та ін.).

Лінійна презентація є будь-яким фільмом, який відтворюється від початку і до кінця.

На сходинці вище лінійних презентацій знаходяться інтерактивні презентації. Вони забезпечують користувачу можливості щодо управління інформаційним потоком або загальним мультимедійним вмістом.

Керовані даними презентації. До цієї категорії розробки відносяться будь-які фільми, які завантажують зовнішні (динамічні або статичні) дані, що управляють вмістом.

Керовані даними додатки. Додатки даного типу дають користувачу можливість виконати певну задачу або дозволити транзакцію між фільмом і віддаленим зовнішнім джерелом даних. Так, наприклад, працюючий в оперативному режимі Flash-банкомат може дозволити клієнту банку реєструватися на захищеному сервері банку і перекласти гроші на інший рахунок або сплатити рахунок. Для виконання всіх цих задач необхідна транзакція між Flash-фільмом і банківським сервером.

Рис. 73 Основні типи мультимедійних проектів

Представлення мультимедійної інформації

Людина сприймає інформацію про оточуючу його дійсність за допомогою шести органів чуття. Проте на практиці сучасні комп'ютерні технології дозволяють моделювати, як правило, тільки два типи сприйняття: зорове і слухове.

Зорове і слухове сприйняття мультимедіа У мультимедійних проектах (виданнях) річ йде лише про аудіовізуальне сприйняття, під яким розуміється здібність людини до виявлення смислових, образних взаємозв'язків між одиницями аудіовізуального оповідання (подіями, сценами, епізодами, кадрами, елементами внутрішньо кадрової композиції) Таким чином, багатокомпонентне мультимедіа - середовище розділяється на два ряди: візуальний і звуковий.

Звуковий ряд (аудіоряд) може включати мову, музику, ефекти (звуки типу шуму, грому, скрипу і т. д., об'єднувані позначенням WAVE (хвиля). Головною проблемою при використанні цієї групи мультисередовища є інформаційна місткість. Для запису однієї хвилини WAVE - звуку вищої якості необхідна пам'ять приблизно 10 Мбайт. Іншим напрямом є використовування звуків MIDI (Musical Instrument Digitale Interface) – одноголосна і багатоголоса музика, звукові ефекти. У даному випадку звуки музичних інструментів, звукові ефекти та ремарки синте-зуються електронними синтезаторами. Корекція і цифрова запис MIDI-звуків здійснюється за допомогою музичних редакторів. Головною перевагою MIDI є малий об'єм необхідної пам'яті – 1 хвилина MIDI-звуку займає в середньому 10 Кбайт.

Візуальний ряд в порівнянні зі звуковим рядом характеризується великим числом елементів. Виділяють статичні реалістичні зображення (фото), текстові

документи, динамічні реалістичні зображення (відео), а також синтезовані зображення, які можуть бути статичними (графіка) або динамічними (анімація).

Формати документів

Формати для представлення електронних книг:

DjVu – (фонетичне скорочення від "Digital View"– "Цифровий вигляд" або "Цифрова фотографія") – технологія стиснення зображень з втратами, розроблена спеціально для зберігання сканувальних документів – книг, журналів, рукописів та ін., де велика кількість формул, схем, малюнків і рукописних символів робить надзвичайно трудомістким їх повноцінне розпізнавання.

Цей формат також є ефективним рішенням, якщо необхідно передати всі нюанси оформлення, наприклад, історичних документів де важливе значення має не тільки зміст, а й колір і фактура паперу; дефекти пергаменту: тріщини, сліди від складання; виправлення, плями, відбитки пальців; сліди, залишені іншими предметами.

- FictionBook (повністю відкритий формат).
- Mobipocket (для кишенькових комп'ютерів).
- PDF (часто книги "друкують" в PDF після верстки).
- RB (формат Rocket eBook).

Формати для обробки текстів

- Текстовий файл (.txt).
- Rich Text Format (.rtf) (прийнятий Microsoft формат для зберігання форматованого тексту).
- Texinfo (.info);
- WordPerfect (.wpd);
- Microsoft Word (.doc, .docx, .docm) (захищений Microsoft-формат, часто змінюється).

Формати для опису сторінок

- PDF.
- DjVu.
- PostScript (.ps, .ps. gz) – це фактично не просто мова опису сторінок (тобто набір якихось кодів схожий на алфавіт), а ціла мова програмування з типовими командами (цикли, оператори, структури даних), за допомогою якої можна писати справжні програми. PostScript (PS) з моменту своєї появи залишається майже абсолютним стандартом у сфері професійного друку і до друкарської підготовки. Але, не дивлячись на те, що PS надає широкі можливості максимально якісному кольоровому друку, він не зовсім підходить для

"рутинного друку" простих текстових документів зважаючи на свою невисоку швидкість і деякі інші недоліки.

- XML Paper Specification (XPS).
- Формати анімації і цифрового відео Форматів відео сьогодні дуже багато. Найпопулярніші – MPEG, AVI, MOV, WMV і ін. Вони відрізняються різними алгоритмами стиснення відео і компаніями-розробниками. Окремо слід зазначити формат FLV – Macromedia Flash-відео, який використовується при включенні відео в Flash-презентації і Flash-фільми, а також формат MPEG.

Графічні формати

Традиційно прийнято розділяти растрову (фотографії, малюнки, картини і ін.) і векторну графіку (схеми, креслення, 3D-моделі та ін.).

Растровий формат характеризується тим, що все зображення по вертикалі і горизонталі розбивається на достатньо дрібні прямокутники – так звані елементи зображення, або пікселі (від англійського pixel – picture element). У файлі зберігається інформація про колір кожного пікселя даного зображення. Чим менше прямокутники, на які розбивається зображення, тим більше роздільна здатність, тобто, тим більше дрібні деталі можна закодувати в такому графічному файлі.

При векторному форматі малюнок представляється у вигляді комбінації простих геометричних фігур (графічних примітивів) – крапок, відрізків прямих і кривих, кіл, прямокутників і т. п. При цьому для повного опису малюнка необхідно знати вигляд і базові координати кожної фігури, наприклад, координати двох кінців відрізка, координати центру і діаметр кола і т. д. Цей спосіб кодування ідеально підходить для малюнків, які легко представити у вигляді комбінації найпростіших фігур, наприклад, для технічних креслень[22].

Список використаних джерел

1. М.О.Антонченко Інформаційна культура як складова загальнолюдської культури. [Електронний ресурс] – Режим доступу: https://fi.npu.edu.ua/files/Zbirnik_KOSN/2/25.pdf
2. Буйницька О. П. Інформаційні технології та технічні засоби навчання. Навч. посіб. – К.: Центр учбової літератури, 2012. – 240 с.
3. Коваленко Ю.О. Інформаційна культура в системі регіонального інформаційного менеджменту. Математичні методи, моделі та інформаційні технології в економіці [Електронний ресурс] – Режим доступу: http://www.bses.in.ua/journals/2016/8-2016/56.pdf
4. Ковалюк Т.В. Основи програмування / Т.В. Ковалюк. – К.: Видав. група BHV, 2005.– 384 с.: іл.
5. Буйницька О. П. Інформаційні технології та технічні засоби навчання. Навч. посіб. – К.: Центр учбової літератури, 2012. – 240 с.
6. Цуканова О.В. Інформаційні війни: вплив на суспільство [Електронний ресурс] / О.В. Цуканова. – Режим доступу: http://www.sworld.com.ua/konfer34/800.pdf.
7. Міжнародний альянс інтелектуальної власності оцінив охорону авторського права в Україні у 2021 році [Електронний ресурс] – Режим доступу: https://musicbusiness.in.ua/news/mizhnarodnyy-alians-intelektualnoi-vlasnosti-otsinyv-okhoronu-avtorskoho-prava-v-ukraini-u-2021-rotsi/
8. Аксютіна А.В., Нестерцова-Собакарь О.В., Тропін В.В. та ін. А 41 Інтелектуальна власність: навч. посібник [для студ. вищ. навч. закл.] / За заг ред канд. юрид. наук, доц. НестерцовоїСобакарь О.В. – Дніпро: Дніпроп. держ. ун-т внутр. справ, 2017. – 140 с.
9. Суб'єкти права інтелектуальної власності [Електронний ресурс] – Режим доступу: https://buklib.net/books/30281/
10. Семків В. О., Шандра Р. С. Інтелектуальна власність : підручник для студентів неюридичних факультетів / В. О. Семків, Р. С. Шандра. – Львів: Галицький друкар, 2015. – 280 с.
11. Кошева Н. А. Ідентифікація користувачів інформаційно-комп’ютерних систем: аналіз і прогнозування підходів / Н. А. Кошева, Н. І. Мазниченко // Системи обробки інформації. - 2013. - Вип. 6. - С. 215-223. - Режим доступу: http://nbuv.gov.ua/UJRN/soi_2013_6_44
12. Самойленко О. А. Виявлення та розслідування кіберзлочинів [Текст] : навчально-методичний посібник / О. А. Самойленко. Одеса : , 2020. 112 с.

13. Кіберзлочинність у всіх її проявах: види, наслідки та способи боротьби. [Електронний ресурс] – Режим доступу: https://gurt.org.ua/articles/34602/
14. 10 найвідоміших українських хакерів [Електронний ресурс] – Режим доступу: https://www.ukrinform.ua/rubric-society/2430232-10-najvidomisih-ukrainskih-hakeriv.html
15. Комп'ютерна злочинність. Навчальний посібник. – Київ: "Атіка", 2002. – 240 с.
16. Марків, С. Історико-правовий аспект кібертероризму [Текст] / Сергій Марків // Актуальні проблеми правознавства. - 2017. - Вип. 2. - С. 103-106.
17. ЗАКОН УКРАЇНИ Про критичну інфраструктуру (Із змінами, внесеними згідно із Законом № 2684-IX від 18.10.2022) [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/1882-20#Text
18. ПЕРЕЛІК підприємств, які мають стратегічне значення для економіки і безпеки держави. ЗАТВЕРДЖЕНО постановою Кабінету Міністрів України від 23 грудня 2004 р. № 1734 [Електронний ресурс] – Режим доступу: https://www.kmu.gov.ua/npas/10493361
19. УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №287/2015 Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України" [Електронний ресурс] – Режим доступу: https://www.president.gov.ua/documents/2872015-19070
20. С.Гончар, Г.Леоненко Аналіз факторів впливу на стан кібербезпеки інформаційної системи об'єкту критичної інфраструктури Cybersecurity and critical infrastructure protection. Information technology and security. july-december 2016. vol. 4. iss. 2 (7)
21. Катков Ю.І., Сєрих С.О., Шашлов А.В., Вергун Д.С. Кібернетичні системи відеоспостереження для забезпечення безпеки об'єктів підприємства критичної інфраструктури. К.: Науково-практичний журнал «Наукові записки УНДІЗ». 2019. №3(55). С.63-73.
22. О.В. Дуболазов, І.В. Солтис МУЛЬТИМЕДІЙНІ ТЕХНОЛОГІЇ В МЕТОДИЧНОМУ ЗАБЕЗПЕЧЕННІ НАВЧАЛЬНОГО ПРОЦЕСУ У ВИЩІЙ ШКОЛІ. КОНСПЕКТ ЛЕКЦІЙ. Чернівці 2022 [Електронний ресурс] – Режим доступу: https://archer.chnu.edu.ua/xmlui/bitstream/handle/123456789/4725/КОНСПЕКТ%20ЛЕКЦІЙ.pdf?sequence=1&isAllowed=y

ДЛЯ НОТАТОК

Навчальне видання

ШАБАЛА Євгенія Євгенівна,
КЛЮЄВА Вікторія Василівна

ІНФОРМАЦІЙНА КУЛЬТУРА

Конспект лекцій

Редагування та коректура *Є.Є. Шабала*
Комп'ютерне верстання *М.М. Власенко*

Підписано до друку 02.02.2023 Формат 60 х 84 1/ 16
Ум. друк. арк. 5,81 Обл.-вид. арк. 4,61
Електронний документ. Вид. № 10/І-16 Зам. 40/1-16

Видавець і виготовлювач
Київський національний університет будівництва і архітектури

Повітрофлотський проспект, 31, Київ, Україна, 03680

Свідоцтво про внесення до Державного реєстру суб'єктів
видавничої справи ДК № 808 від 13.02.2002 р.