**МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ**
**ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ**
**ФАКУЛЬТЕТ ПІДГОТОВКИ ФАХІВЦІВ ДЛЯ ПІДРОЗДІЛІВ КРИМІНАЛЬНОЇ ПОЛІЦІЇ**
**КАФЕДРА КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ**

**ТЕМА:**

# ЕКСПЕРТНІ СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ЩОДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

студентка 2 курсу навчання
освітнього ступеню «магістр»
ННІЗДН факультету № 2
Шевченко Олена Ігорівна

**Науковий керівник**:
кандидат юридичних наук, доцент
Форос Ганна Володимирівна

**Рецензент:** кандидат юридичних наук,
Мельнікова Олена Олександрівна

***Кваліфікаційна робота допущена до захисту***
_____ 2022 р., протокол № ___
В.о. завідувача кафедри кібербезпеки та інформаційного забезпечення,
доктор юридичних наук, доцент
_____А.М. Бабенко
(підпис)

Одеса – 2022

**ПЛАН:**

# ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АІПС – автоматизована інформаційно-пошукова система

АС – автоматизована система

ЗМІ – засоби масової інформації

ЗУ – Закон України

ЕС –експертна система

ІБ – інформаційна безпека

ІК – інформаційна картка

ІТ – інформаційні технології

ІТС – інформаційно-телекомунікаційна система

ІС – інформаційна система

КБ – кібернетична безпека

КЗ – криптографічний захист

СІТ- сучасні інформаційні технології

СППР - система підтримки прийняття рішень

СУБД – системи управління базами данних

# ВСТУП

**Актуальність теми**. Поширення інформаційних технологій стимулювало дуже велика кількість нових ідей, адже комп'ютерний світ - це нове, поки що мало вивчене і освоєне творче про простір. Однак найчастіше виявляється, що для втілення всіх творчих ідей не вистачає обчислювальної потужності комп'ютера, і її доводиться збільшувати, впроваджувати нові технології, що прискорюють швидкість роботи. Чим вище швидкість роботи комп'ютера, тим ширше творчий простір, що дозволяє людині реалізовувати свої фантазії в електронному вигляді. Однак людська психологія така, що його потреби безмежні, чим більше буде посилюватися міць комп'ютерів, тим більше він буде від них вимагати.

Забезпечення інформаційної безпеки є важливим завданням для будь-якої організації, оскільки від збереження конфіденційності, цілісності та доступності інформаційних ресурсів багато в чому залежать якість та оперативність прийняття управлінських рішень, ефективність їх реалізації. Держава, регламентуючи відносини в інформаційній сфері, не здатна впоратися у повному обсязі із завданнями забезпечення безпеки всіх суб'єктів інформаційних відносин, однозначно відповідаючи лише за захист відомостей, що становлять державну таємницю. Тому в умовах різних форм власності ці завдання у повному обсязі мають вирішуватись керівниками організацій. При цьому виникає проблема забезпечення захисту інформації та інформаційних технологій, відповідного регулюванням суспільних відносин в інформаційній сфері. Особливу занепокоєність викликає можливість розробки, застосування та розповсюдження інформаційної зброї, виникнення у зв’язку з цим загрози інформаційних війн та інформаційного тероризму, чиї негативні наслідки можна порівняти з наслідками застосування зброї масового знищення.

Потреба в тому, щоб явно подавати людські знання, є центральним питанням за розроблення експертних систем. Основані на знаннях (інтелектуальні) інформаційні системи або експертні комп’ютерні системи

мають здатність показати вражаючу, а інколи приголомшуючу продуктивність щодо розв’язання проблем у порівнянні з людиною, що не є експертом. Вони роблять це за допомогою використання обширних баз знань, поєднаних зі спеціалізованим евристичним доведенням. Проте в даний час актуальними є вже не стільки питання захисту інтелектуальної власності та інформації, що становить особисту, комерційну або службову таємницю, скільки таке конструювання структур та функцій організацій, яке б забезпечувало безпеку інформаційних систем, що супроводжують, а часто й забезпечують нормальне функціонування виробничих (інтелектуальних), інноваційних, випереджаючих тощо) технологій. Така проблема може бути вирішена на базі експертних систем підтримки прийняття рішень, які реалізують спеціальні методики обстеження організацій та видачі рекомендацій щодо забезпечення їх інформаційної безпеки.

Вказанні аспекти зумовлюють потребу в дослідженні проблем стану і розвитку системи забезпечення інформаційної безпеки організацій, встановлення місця та ролі експертних систем підтримки прийняття рішень щодо забезпечення цієї самої безпеки.

Науково-теоретичну основу дослідження складає значна кількість наукових праць, присвячених аналізу проблем забезпечення інформаційної безпеки. Серед сучасних робіт вітчизняних та зарубіжних дослідників цих проблем, в роботі було використано праці: В.А. Авраменко, О. В. Андрійчук , І.В. Арістової, П.Д. Бєлякова, М.С., В.К. Гаєвського, В. В.Ковтунець , Б.А. Кормич, В.А. Ліпкана, В.В. Лунєєва, А.І. Марущака, Н. О Миронова, В.С. Цимбалюка, В.І. Шакуна, С.О. Прокопова, Е.В. Рижкова та інших.

**Метою** дослідження є дослідження особливостей застосування експертних систем підтримки прийняття рішень щодо забезпечення інформаційної безпеки організацій.

Для досягнення вказаної мети в процесі дослідження ставились і вирішувались такі **завдання**:

- дослідити експертну систему підтримки прийняття рішень щодо

забезпечення інформаційної безпеки організації, яка формує рекомендації щодо підвищення ефективності забезпечення її інформаційної безпеки;

- встановити та дослідити класифікацію експертних систем підтримки прийняття рішень;
- дослідити основні підходи до розуміння поняття і змісту інформаційної безпеки організації;
- узагальнити організаційно-теоретичні напрямки забезпечення інформаційної безпеки України.

*Об'єктом дослідження є* суспільні правовідносини, що виникають в сфері застосування експертних систем підтримки прийняття рішень щодо забезпечення інформаційної безпеки організації.

*Предметом дослідження* є теоретичні та методологічні засади використання експертних систем підтримки прийняття рішень щодо забезпечення інформаційної безпеки організації.

Методологічною основою дослідження є діалектико-матеріалістичний метод пізнання соціальних явищ і процесів, а також концептуальні положення Конституції України, інформаційного законодавства України, теорії кібернетики та системного аналізу.

В дослідженні використовувались загальнонаукові і спеціальні методи. *Порівняльно-правовий* – при аналізі норм чинного законодавства України та поглядів учених щодо унормування і розуміння окремих інститутів забезпечення інформаційної безпеки. *Догматичний* – при визначенні поняття і структури інформаційної безпеки, а також аналізі та класифікації експертних систем підтримки прийняття рішень, обґрунтуванні висновків і пропозицій за темою дослідження.

Теоретичне підґрунтя магістерської роботи становлять наукові праці вчених управлінців, фахівців з теорії інформації, а також, залежно від змісту розглядуваних питань конституційного та інформаційного права, інформатики, теорії інформації та кібернетики

*Апробація результатів магістерської роботи*. Основні положення роботи були відображенні в матеріалах науково-практичної конференції «Кібербезпека в Україні: правові та організаційні питання»(Одеса, 19 листопада 2021 р.).

*Структура роботи* обумовлена предметом, методологією дослідження та завданнями викладення матеріалу. Дипломна робота складається із вступу, двох розділів, чотирьох підрозділів, висновків та списку використаних джерел. Загальний обсяг роботи становить 67 сторінок, із них список використаних джерел становить 43 найменування і розташований на 4 сторінках.

# РОЗДІЛ 1. ХАРАКТЕРИСТИКА ЕКСПЕРТНИХ СИСТЕМ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ

## *1.1.Експертна система як найпоширеніша орієнтована на знання система підтримки прийняття рішень*

До інформаційних систем нового покоління належать системи підтримки прийняття рішень (СППР) та інформаційні системи, побудовані на штучному інтелекті (інтелектуальні автоматизовані системи).

Проведений аналіз, дозволив дійти висновку, що підґрунтям для розроблення та функціонування орієнтованих на знання СППР є технологія експертних систем та засоби добування знань. Відомо, що основна концепція експертних систем (ЕС) базується на припущенні, що знання експерта можуть бути записані в комп'ютерній пам'яті і потім застосовані іншими, коли з'являється в цьому потреба. Оскільки з проблематики побудови та використання експертних систем є достатня кількість літературних джерел, то є резон розглянути цей тип інформаційних систем у контексті створення орієнтованих на знання систем підтримки прийняття рішень.

Потреба в тому, щоб явно подавати людські знання, є центральним питанням розроблення експертних систем. Основані на знаннях (інтелектуальні) інформаційні системи або експертні комп'ютерні системи мають здатність показати вражаючу, а інколи приголомшуючу продуктивність щодо розв'язання проблем у порівнянні з людиною, що не є експертом. Вони роблять це за допомогою використання значних баз знань, поєднаних зі спеціалізованим евристичним доведенням. Цей підхід привів до розроблення систем, що мають низку переваг, зокрема:

- у деяких типах проблем, як наприклад, у діагностиці дефектів, терапії, селекції, вони можуть розв'язати низку проблем інколи краще, ніж людина;

- вони можуть надати організаціям можливість краще управляти важливими ресурсами менеджменту, професійних знань і досвідом, забезпечуючи їх нагромадження та зберігання, централізовану підтримку і зручний розподіл;
- вони можуть відповідати на прості запитання і пояснювати, те, як вони розв’язують проблеми. Дуже часто пояснення того, як був досягнутий розв’язок, набагато важливіше, ніж сам розв’язок.

Так, на думку Р.Г. Савенко та М.В. Лисенко, система підтримки прийняття рішень – це інтерактивна комп'ютерна система, яка призначена для підтримки різних видів діяльності при прийнятті рішень із слабоструктурованих або неструктурованих проблем. Інтерес до СППР, як перспективної галузі використання обчислювальної техніки та інструментарію підвищення ефективності праці в сфері управління економікою, постійно зростає. У багатьох країнах розробка та реалізація СППР перетворилася на дільницю бізнесу, що швидко розвивається. [ 32, 24]

Так, під час розв'язання поставлених завдань основну роль відіграють евристичні і наближені методи, що, на відміну від алгоритмічних, не завжди гарантують успіх. Евристика, в принципі, є правилом впливу, що в машинному вигляді відображає деяке знання, набуті людиною разом із накопичуванням практичного досвіду розв'язання аналогічних проблем. Такі методи є наближеними в тому сенсі, що, по-перше, вони не потребують вичерпної вихідної інформації, а, по-друге, існує певний ступінь впевненості (або невпевненості) в тому, що запропонований розв'язок є правильним.

Експертні системи відрізняються і від інших видів програм із галузі штучного інтелекту. Саме експертні системи застосовуються для предметів реального світу, операції з якими зазвичай вимагають великого досвіду, накопиченого людиною. Експертні системи мають яскраво виражену практичну направленість для застосування в науковій або комерційній сфері.

У сучасному розумінні термін «штучний інтелект» можна трактувати як науковий напрям (дисципліну), в рамках якого ставляться та розв’язуються

завдання апаратного й програмного моделювання тих видів людської діяльності, які традиційно вважаються інтелектуальними, тобто потребують певних розумових зусиль. У Державному Стандарті України ДСТУ 2938-94 вказувалось, що штучний інтелект визначається як «здатність систем обробки даних виконувати функції, що асоціюються з інтелектом людини, такі як логічне мислення, навчання та самовдосконалення».

Штучний інтелект – це штучні системи, створені людиною на базі ЕОМ, що імітують розв'язування людиною складаних творчих завдань. Створенню інтелектуальних інформаційних систем сприяла розробка в теорії штучного інтелекту логіко-лінгвістичних моделей. Ці моделі дають змогу формалізувати конкретні змістовні знання про об'єкти управління та процеси, що відбуваються в них, тобто ввести в ЕОМ логіко-лінгвістичні моделі поряд з математичними. Логіко лінгвістичні моделі – це семантичні мережі, фрейми, продукувальні системи – іноді об'єднуються терміном «програмно-апаратні засоби в системах штучного інтелекту». [18]

Розрізняють три види інтелектуальних автоматизованих систем:

1. інтелектуальні інформаційно-пошукові системи (системи типу «запитання – відповідь»), що в процесі діалогу забезпечують взаємодію кінцевих користувачів – непрограмістів з базами даних та знань професійними мовами користувачів, близьких до природних;

2. розрахунково-логічні системи, що надають змогу кінцевим користувачам, що не є програмістами та спеціалістами в галузі прикладної математики, розв'язувати в режимі діалогу з ЕОМ свої задачі з використанням складаних методів і відповідних прикладних програм;

3. експертні системи, що дають змогу провадити ефективну комп'ютеризацію галузей, у яких знання можуть бути подані в експертній описовій формі, але використання математичних моделей утруднене або неможливе.

Адже повернимося до експертних систем, експертна система - це методологія адаптації алгоритму успішних рішень одної сфери науково-

практичної діяльності в іншу. З поширенням комп’ютерних технологій це тотожна (подібна, заснована на оптимізуючому алгоритмі) інтелектуальна комп’ютерна програма, що містить знання та аналітичні здібності одного або кількох експертів щодо деякої галузі застосування і здатна робити логічні висновки на основі цих знань, тим самим забезпечуючи вирішення специфічних завдань (консультування, навчання, діагностика, тестування, проектування тощо) без присутності експерта (спеціаліста в конкретній проблемній галузі).

Також визначається як система, яка використовує базу знань для вирішення завдань (видачі рекомендацій) у деякій предметній галузі. Цей клас програмного забезпечення спочатку розроблявся дослідниками штучного інтелекту шістдесяті роки минулого століття здобув комерційне застосування, починаючи з 1980-их. Часто термін система, заснована на знаннях використовується в якості синоніма експертної системи, однак можливості експертних систем ширші за можливості систем, заснованих на детермінованих (обмежених, реалізованих на поточний час) знаннях. [ 27]

Однак узгодженого визначення експертних систем не існує. Натомість автори дають визначення залежно від застосування, структури таких систем. Ранні визначення експертних систем припускали застосування виведення нових знань на основі правил.

Так однією з основних характеристик експертної системи є її швидкодія, тобто швидкість отримання результату та його достовірність (надійність). Дослідницькі програми штучного інтелекту можуть бути і не дуже швидкими, натомість, експертна система повинна за прийнятний час знайти розв'язок, що був би не гіршим за розв'язок, що може запропонувати фахівець в цій предметній області.

Експертна система повинна мати можливість пояснити, чому запропоновано саме цей розв'язок і довести його обґрунтованість. Користувач повинен отримати всю інформацію, необхідну йому для того, аби переконатись в обґрунтованості запропонованого розв'язку.

Експертна система - це програма, що поводиться подібно експерту в деякій, звичайно вузькій прикладній області. Типові застосування експертних систем містять у собі такі задачі, як медична діагностика, локалізація несправностей в устаткуванні й інтерпретація результатів вимірів.

Експертні системи повинні вирішувати задачі, що вимагають для свого рішення експертних знань у деякій конкретній області. У тій чи іншій формі експертні системи повинні мати ці знання. Тому їх також називають системами, заснованими на знаннях. Однак не всяку систему, засновану на знаннях, можна розглядати як експертну.

Експертна система повинна також уміти певним чином пояснювати свою поведінку і свої рішення користувачу, так само, як це робить експерт-людина. Це особливо необхідно в галузях, для яких характерна невизначеність, неточність інформації (наприклад, у медичній діагностиці). У цих випадках здатність до пояснення потрібна для того, щоб підвищити ступінь довіри користувача до рад системи, а також для того, щоб дати можливість користувачу знайти можливий дефект у міркуваннях системи. У зв'язку з цим в експертних системах варто передбачати дружня взаємодія з користувачем, що робить для користувача процес міркування системи "прозорим".[ 18; 27; 32]

Як в будь якій інформаційній або комп’ютерній системи ключовим поняття є визначення інформації. Саме  інформація виступає основним предметом безпеки експертних систем підтримки та прийняття рішень.

З формуванням інформаційного суспільства категорія "інформація" стала ключовою: вона виступає одним із найважливіших факторів системи суспільних відносин. У зв'язку з цим у сучасній філософії, теоретичних і прикладних науках, не можуть підібрати однозначного трактування категорії "інформація".

В науковій та спеціальній літературі існує чимало визначень інформації залежно від галузі науки, сфери людської діяльності, де цій термін використовується. Питанням дослідження різних видів інформації,

визначення її ролі в системі управління, теорії аналізу та обробки соціальної інформації, методології й методики створення різних інформаційних систем у певних сферах людської діяльності присвячено багато праць [9; 23;28].

Як свідчать дослідження, сьогодні це визначення залежить від різних чинників (критеріїв). Зазначимо деякі з них: конкретна галузь знань чи суспільного життя, у якій ведеться дослідження (предметна галузь суспільних відносин, організація управління соціальною системою тощо); характер завдань, для яких вводиться це поняття; інші критерії.

У загальному розумінні інформація - це певні відомості, сукупність певних даних, знань. У філософський науці прийнято виділяти два аспекти існування інформації як субстанції – атрибутивний та функціональний.

Прихильники першого розглядають інформацію як об’єктивну властивість усіх матеріальних об’єктів (інформація – атрибут матерії); прихильники другого стверджують, що інформація є умовою і результатом спрямованої активності й тому вона виникає тільки на соціально-свідомомурівні. Не викликає сумніву, що інформація, якою обмінюються члени суспільства, обов’язково пов’язана з відбиттям реальності. Ще Н. Вінер розумів під інформацією позначення змісту, який надходить із зовнішнього світу у процесі пристосування до нього людини. При цьому слід підкреслити різницю у ставленні до пошуку та обробки інформації людини та машини.

У вузькому значенні теорія інформації – це математична теорія передачі повідомлень у системах зв’язку. Виникла вона внаслідок досліджень американського вченого К. Шеннона. Основні її постулати такі. Повідомлення (точніше, їх коди) надходять з джерела інформації через канал зв’язку до приймача інформації. Ці повідомлення змінюють систему знань (тезаурус) приймача, зменшують рівень його розмаїття, невизначеності, який вимірюється ентропією. Ентропія системи повідомлень визначається їх вірогідностями як середнє значення логарифмів величин, які є зворотними до цих вірогідностей. Виміряти середню кількість інформації можна по зменшенню ентропії сприймача у результаті зміни його уявлень. До речі,

звідси й приходить одиниця виміру інформації. Вона визначається кількістю інформації про те, яка з двох однаково вірогідних подій реалізувалася і називається «біт» (початок і кінець англійського словосполучення binarydigit (бінарний розряд). Теорія інформації знайшла розвиток у кібернетиці. Саме за допомогою теорії інформації вдалося науково довести загальновідомий принцип кібернетики про те, що розмаїття системи управління має бути не нижче розмаїття об'єкта, який керується цією системою.[32, 214]

Одні з прихильників теорії інформаційної революції – американці Р. Кохане та Дж. Най класифікують всю інформацію, що обертається в сучасному Світі, за трьома типами: вільна інформація, комерційна інформація та стратегічна інформація [28, 85].

До вільної інформації можна віднести таку, що розповсюджується безкоштовно. До такої вільної інформації відносяться програми громадського телебачення, радіомовлення, політична реклама, різного роду інформаційні акції, вільна інформація, розміщена в мережі Інтернет тощо. Стрімке, практично в геометричній прогресії зростання потоків та обсягів вільної інформації, яке носить характер інформаційного вибуху, вбачається одним з результатів інформаційної революції.

Інший різновид інформації – комерційна, тобто та інформація, яка виробляється з метою отримання прибутку у вигляді компенсації за її використання іншими, набуває в наші дні все більшого поширення. Взагалі, однією з ознак формування інформаційного суспільства є те, що інформація сама по собі стала товаром, при чому товаром, що має стратегічне значення для держави і суспільства. Поступово навіть рівень економічної могутності держави починає вимірюватись не лише обсягами та рівнем матеріального виробництва, а саме обсягами виробництва та поширення інформації.

Як зазначають фахівці в галузі економіки: "З економічної точки зору інформація представляє собою неречовий продукт інтелектуальної діяльності людини і суспільства" [28, 36].

При цьому виробництво та розповсюдження інформації на сьогоднішній день є одним з найприбутковіших видів бізнесу, що підтверджується результатами роботи тієї ж корпорації Microsoft, лідера на ринку інформаційних технологій.

Однією з найхарактерніших ознак інформаційної революції в цій сфері стало народження електронної комерції, яка розвивається у відповідності до всіх законів ринку та вільної конкуренції. В сфері електронної комерції найбільш яскраво проявляється та модель ринкових відносин, яка чекає наше суспільство в майбутньому і ця модель ставить перед законодавцем непрості проблеми щодо правового регулювання таких відносин.

Отже, з точки зору теорії інформації, інформація – це зміст повідомлення про сукупність явищ і подій, що представляють інтерес для зацікавлених осіб та організацій, підлягають реєстрації та обробці. При цьому за інформацію вважаються лише ті дані та зведення, які несуть дещо нове, раніше невідоме для споживача (суб'єкта управління).

Згідно Закону України “Про інформацію”, інформація - це будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [2, ст. 1].

Відсутність однозначного визначення поняття "інформація" можна вважати природним явищем. Навряд чи є потреба шукати загальне (абстрактне) його визначення, що охоплює всю багатогранність, багатоаспектність його буття. Воно неминуче буде або дуже загальним, або надто заплутаним.

Основна функція інформації полягає в повідомленні суб'єкту про стан середовища, в якому проходить його життєдіяльність, у зниженні ступеня невизначеності тієї чи іншої ситуації.

Для задоволення своїх інформаційних потреб суб'єкти інформаційної діяльності використовують певні джерела інформації. А оскільки поняття "джерело інформації" вживається надзвичайно широко, то, щоб уникнути

ускладнень у роботі, аналітику треба добре розуміти, яке змістове навантаження несе цей термін у кожному конкретному випадку.

У загальному розумінні під джерелами інформації розуміють документи та інші носії інформації, які являють собою матеріальні об'єкти, що зберігають інформацію, а також повідомлення засобів масової інформації, публічні виступи.

З поняттями "джерело інформації" та "документ" пов'язаний термін "носій інформації (даних)", який в науковій літературі визначається як матеріальний об'єкт, призначений для зберігання даних.

Поняття інформаційної технології базується на двох основних поняттях – «інформація» і «технологія». Як ми вже вказували вище, під інформацією розуміють повідомлення, що інформують про стан справ, про стан чого-небудь. Технологія як строго наукове поняття означає певний комплекс наукових і інженерних знань, втілений у способах, прийомах праці, наборах виробничо-речових чинників виробництва.

Сучасні інформаційні технології (СІТ) - сукупність методів і засобів одержання і використання інформації на базі обчислювальної та інформаційної техніки, з широким застосуванням інформаційних методів.

У сучасних інформаційних технологіях виділяють 3 складові: апаратне забезпечення (засоби обчислювальної техніки та оргтехніки - hardware); програмне забезпечення (прикладне та системне програмне забезпечення, методичне та інформаційне забезпечення - software); організаційне забезпечення (включаючи людину в системи інформаційних технологій, взаємодія людини з цими системами, системне використання технічних і програмних засобів - orgware). [19;32]

Можна виділити основні особливості інформаційних технологій, які відрізняють їх від технологій матеріального виробництва:

- метою інформаційної технології є отримання нової інформації для її аналізу людиною і прийняття на цій основі рішення щодо виконання певної дії;

- засоби, якими здійснюється технологічний процес, - це в сучасних інформаційних технологіях різноманітні програмні, апаратні, програмно апаратні обчислювальні комплекси;
- критеріями оптимальності технологічного процесу є надійність обробки інформації, достовірність і повнота цієї інформації, своєчасність передачі інформації користувачам.

Створення та функціонування інформаційних систем в управлінні тісно пов'язані з розвитком інформаційної технології - головною складовою частини автоматизованої інформаційної системи. Інформаційна система за своїм складом нагадує підприємство з перероблення даних і виробництва вихідної інформації.

Як і в будь-якому процесі, в інформаційній системі наявна технологія перетворення даних у результативну інформацію.

Сучасна інформаційна технологія орієнтована на застосування найширшого спектру технічних засобів електронно-обчислювальних машин і засобів комунікацій. На її основі створено та створюються обчислювальні системи й мережі різних конфігурацій не тільки для нагромадження, зберігання, перероблення інформації, але й максимального зближення термінальних улаштувань до робочого місця спеціаліста та для підтримки прийняття рішення керівника.

Принципова відміна нової інформаційної технології полягає не тільки в автоматизації процесів зміни форми й розміщення інформації, а й у зміні її змісту. І сьогодні можна говорити про забезпечувальні інформаційні технології і функціональні інформаційні технології.

Забезпечувальні інформаційні технології - технології оброблення інформації, які використовуються як інструмент у різних предметних сферах для розв'язання різних задач.

Функціональні інформаційні технології - це модифікація забезпечувальних інформаційні технології, за якої реалізується, будь-яка з предметних технологій. Наприклад, в арсеналі облікового процесу можуть

перебувати як забезпечувальні технології (наприклад, текстові й табличні процесори), так і спеціальні функціональні технології (табличні процесори, СУБД, експертні системи, реалізуючі предметні технології).

Інформаційні технології можна класифікувати за рядом ознак: за способом реалізації в АІС; за ступенем охоплення задач управління; за класом реалізуючих технологічних операцій; за типом користувацького інтерфейсу; за способом побудови мережі; за обслуговуючими предметними сферами.

Як вже говорилося, інформаційні технології застосовуються практично всюди. Технології планування та управління, наукових досліджень і розробок, експериментів, проектування, грошово-касових операцій, криміналістики, медицини, освіти тощо - сьогодні не обходяться без участі комп'ютерів.

Як виробничі, так і інформаційні технології виникають не спонтанно, а в результаті технологізації того або іншого соціального процесу, тобто цілеспрямованого активного впливу людини на ту чи іншу область виробництва і перетворення її на базі машинної техніки. Чим ширше використання ЕОМ, тим вище їх інтелектуальний рівень, тим більше виникає видів інформаційних технологій, до яких відносяться:

- технології планування та управління;
- наукових досліджень і розробок;
- експериментів;
- проектування;
- грошово-касових операцій;
- криміналістики;
- медицини;
- освіти та інші. [12;35]

Інформаційній технології властиві:

- високий ступінь розчленованості процесу на стадії, що відкриває нові можливості для його раціоналізації і перекладу на виконання за допомогою машин. Це - найважливіша характеристика машинізованого технологічного процесу;

• системна повнота (цілісність) процесу, який повинен включати весь набір елементів, що забезпечують необхідну завершеність дій людини при досягненні поставленої мети;

• регулярність процесу й однозначність його фаз, що дозволяють застосовувати середні величини при їхній характеристиці, і, отже, допускають їх стандартизацію та уніфікацію. В результаті з'являється можливість обліку, планування, диспетчеризації інформаційних процесів.

У такій розвинутій формі, що має всі ознаки відмічені, інформаційно-комунікативні процеси присутні в машинізоване кібернетичних системах.

Основна мета використання інформаційних технологій - автоматизація виробничої або адміністративної роботи. В якості основного засобу автоматизації інформаційно-управлінської діяльності і виступають персональні ЕОМ. Свою роботу в конторі службовець здійснює через реалізацію різних інформаційних процесів, тобто процесів отримання, реєстрації, накопичення, перетворення, генерації, відображення і передачі інформації.

Повертаючись до експертних систем, то доволі часто до них висувають додаткову вимогу - здатність мати справу з невизначеністю і неповнотою. Інформація про поставлену задачу може бути неповною чи ненадійною; відносини між об'єктами предметної області можуть бути наближеними. Наприклад, може не бути повної впевненості в наявності в пацієнта деякого симптому чи в тому, що дані, отримані при вимірі, вірні; ліки може стати причиною ускладнення, хоча звичайно цього не відбувається. В усіх цих випадках необхідні міркування з використанням ймовірнісного підходу.

У самому загальному випадку для того, щоб побудувати експертну систему, ми повинні розробити механізми виконання наступних функцій системи:

- рішення задач з використанням знань про конкретну предметну область можливо, при цьому виникне необхідності мати справу з невизначеністю;

- взаємодія з користувачем, включаючи пояснення намірів і рішень системи під час і після закінчення процесу рішення задачі.

Кожна з цих функцій може виявитися дуже складною і залежить від прикладної області, а також від різних практичних вимог. У процесі розробки і реалізації можуть виникати різноманітні важкі проблеми.

При розробці експертної системи прийнято поділяти її на три основних

- модулі:
- база знань;
- машина логічного висновку;
- інтерфейс із користувачем. [35, 83]

База знань містить знання, що відносяться до конкретної прикладної області, у тому числі окремі факти, правила, що описують чи відносини що описують чи відносини явища, а також, можливо, методи, евристики і різні ідеї, що відносяться до рішення задач у цій прикладній області.

Машина логічного висновку вміє активно використовувати інформацію, що міститься в базі знань.

Інтерфейс із користувачем відповідає за безперебійний обмін інформацією між користувачем і системою; він також дає користувачу можливість спостерігати за процесом рішення задач, що протікають у машині логічного висновку.

Прийнято розглядати машину висновку й інтерфейс як один великий модуль, звичайно називаний оболонкою експертної системи, чи, для стислості, просто оболонкою.

### *1.2. Класифікація експертних систем підтримки прийняття рішень*

Системи підтримки прийняття рішень набули широкого застосування в економіках різних країн, причому їх кількість постійно зростає. Орієнтовані на операційне управління СППР застосовуються в маркетингу (для прогнозування й аналізу збуту, дослідження ринку і цін), для виконання науково-дослідних і конструкторських робіт, в управлінні кадрами, виробництвом тощо. Найбільша частка комп'ютерної підтримки різних функцій припадає на стратегічне планування, управління і розвиток підприємств, операційне управління й розподіл ресурсів.

Системами підтримки прийняття рішень називають інтелектуальні системи, за допомогою яких особи, що приймають рішення (ОПР), мають змогу аналізувати ситуації, формулювати задачі, виробляти, контролювати й оцінювати варіанти рішень, які забезпечують досягнення поставленої мети. Згідно з таким узагальненим визначенням можна тлумачити СППР як одну з категорій управлінських інформаційних систем. Проте останні найчастіше визначаються як системи підготовки управлінських звітів – періодичних структурованих документів. На противагу цьому СППР має бути дієвою інтерактивною системою, що реагує як на заплановані, так і на непередбачувані інформаційні запити, зорієнтована на специфічний тип рішень або на множину взаємозв'язаних рішень і застосовується там, де неможливо або небажано мати повністю автоматичну систему. [ 32; 35]

Сфера використання таких систем практично необмежена. Вони мають не лише суто економічне застосування, а й призначаються для правоохоронних органів, судового виробництва, органів виконання покарань, національної безпеки, служби охорони, військової розвідки, митниці, міграційної служби та багатьох інших. Правоохоронна діяльність вирізняється в цьому списку, оскільки створення СППР у цій галузі можливе тільки в разі взаємодії математиків, юристів, практиків та фахівців з інформаційних технологій, причому готові системи мають працювати в умовах розподілених

організаційних структур, що використовують різноманітні засоби автоматизації і не завжди забезпечені якісними каналами зв'язку.

Понад 25 років практичного використання систем підтримки прийняття рішень показали, що прийняття рішень можна підтримувати по-різному. Різні типи систем підтримки прийняття рішень надають різну допомогу ОПР – пропонуються можливості використовувати і маніпулювати великими базами даних або застосовувати правила і контрольні перевірки чи користуватися великими математичними моделями. Для позначення певних типів СППР (іноді із суто маркетинговою метою) вживають багато специфічних термінів. Основні категорії систем підтримки прийняття рішень розглядають залежно від того, який із головних компонентів системи взято за домінуючий. Проте зазначимо, що ІС можна віднести до класу систем підтримки прийняття рішень тільки за наявності в неї родової структури – підсистем керування базою даних, керування базою моделей та інтерфейсу користувача.

Системи підтримки прийняття рішень, зорієнтовані на дані, – це тип СППР, який зосереджується передусім на доступі й маніпуляції великими базами структурованих даних.

До цієї категорії відносять:

• системи підготовки управлінських звітів;

• сховища даних - це особлива форма організації бази даних, призначена для зберігання в погодженому вигляді агрегованої інформації, одержуваної з баз даних різних OLTP-систем та зовнішніх джерел. Одна з найважливіших цілей створення сховищ даних – швидка реакція на інтерактивні запити. Сховища містять великі обсяги даних і мають такі характеристики, як предметна орієнтація, інтегрованість, підтримання хронології, незмінність, мінімальна надмірність, захищеність;

•системи аналізу даних (ALOP) – це системи швидкого аналізу розподіленої багатовимірної інформації. Термін «OLAP» невіддільний від терміна «сховище даних». OLAP-системи забезпечують різні точки зору на дані та різні форми їх подання. Програмний продукт можна віднести до класу

OLAP, якщо він має три головні особливості: багатовимірність даних, складні обчислення, швидка обробка;

• виконавчі інформаційні системи (інформаційна система керівника) – автоматизовані системи, призначені для забезпечення необхідною актуальною інформацією менеджерів вищої ланки управління у процесі прийняття стратегічних рішень. Акцент робиться на графічні дисплеї та легкий у використанні інтерфейс, за допомогою яких подається інформація з корпоративної бази даних;

• географічні ІС (геоінформаційні системи або просторові СППР - системи підтримки прийняття рішень, що дають змогу поєднувати модельне зображення території (електронне відображення карт, схем, космо-, аерозображень земної поверхні) з інформацією табличного типу (різноманітні статистичні дані, списки, економічні показники тощо). [35;86]

Другу велику категорію становлять СППР, зорієнтовані на доступ та маніпуляцію моделями – статистичними, фінансовими, оптимізаційними і/або імітаційними. Здебільшого такі системи використовують дані й параметри, що їх надають ОПР, але, як правило, не потребують великих обсягів даних. Приклади таких СППР:

засоби аналізу рішень, які допомагають ОПР розбити проблему на складові й структурувати її. Мета цих інструментальних засобів полягає в тому, щоб допомогти користувачеві застосувати такі моделі, як дерева рішень, моделі багатоатрибутної корисності, моделі Баєса, моделі аналізу ієрархій тощо;

засоби лінійного програмування – засоби використання відповідних математичних моделей для пошуку оптимального розв'язку задач розподілу ресурсів і т. ін.;

імітаційні засоби – засоби проведення певної кількості експериментів для перевірки результатів, що випливають з кількісної моделі системи.

Деякі OLAP-системи, що дають змогу виконувати складний аналіз даних, можуть бути класифіковані як гібридні СППР, що забезпечують і

моделювання, і пошук та підсумковий аналіз даних. Гібридним підходом до СППР вважаються також технології здобування даних. Синонімами терміна «здобування даних» є «виявлення знань у базах даних» та «інтелектуальний аналіз даних». Мета здобування даних полягає у виявленні прихованих правил і закономірностей у наборах даних.

Засоби здобування даних та експертні системи становлять ще одну категорію СППР - рекомендаційні СППР. Експертні системи (ЕС) як системи штучного інтелекту часто розглядають як окремий клас ІС, але останнім часом спостерігається тенденція реалізації їхніх модулів у складі СППР і виконавчих ІС. [18]

Системи підтримки прийняття рішень, зорієнтовані на документи розробляються для управління неструктурованими документами і Web-сторінками. Такі СППР інтегрують різноманітні технології зберігання та оброблення гіпертекстових документів, зображень, звуків, відео тощо.

Групові системи підтримки прийняття рішень (комунікаційні СППР) – це інтерактивні автоматизовані системи, призначені для підтримки розв'язування неструктурованих і напівструктурованих проблем кількома ОПР, що працюють як група. Групові системи підтримки прийняття рішень є гібридними системами – вони підтримують електронні, візуальні та звукові комунікації, складання розкладів, спільне використання даних і моделей, колективне генерування альтернатив, консолідацію ідей та інтерпретацію результатів. Крім цього, групові СППР мають можливості, які вже були розглянуті стосовно інших класів систем підтримки прийняття рішень СППР.

Нині більшість використовуваних систем підтримки прийняття рішень є внутрішньо організаційними – їх розроблено для індивідуального або групового використання в межах окремої організації. На відміну від них інтерорганізаційні СППР, що належать до порівняно нової категорії систем, можуть мати серед своїх користувачів і зовнішніх щодо фірми осіб (акціонерів, споживачів, постачальників і т. ін.). Створити такі системи вдалося насамперед завдяки розширенню доступу до мережі Інтернет, яка

забезпечує комунікаційні зв'язки різних типів, зокрема й необхідні для систем підтримки прийняття рішень. На базі Web-технологій створюються та використовуються системи, які дістали назву Web-зорієнтованих. [32]

Усі зазначені типи систем підтримки прийняття рішень можна класифікувати залежно від ступеня їх спеціалізації. Функціонально зорієнтовані системи розробляються для підтримання специфічних бізнес-функцій або типів ділової діяльності. Такі системи можна назвати галузевими. Вони можуть бути зорієнтовані на маркетинг або фінанси, складання розкладів або встановлення діагнозів. Зазначені СППР можна придбати в «коробковому» варіанті або створити в результаті пристосування загальноорієнтованих систем, які в цілому підтримують ширші завдання, такі як управління проектами, аналіз рішень, бізнес-планування.

Систематику систем підтримки прийняття рішень можна побудувати за функціональними галузями (маркетинг, планування, інвестиції та ін.), в яких підтримується прийняття рішень, за рівнями інформаційного забезпечення (тактичний, операційний, стратегічний, рівень середньої ланки управління) тощо.

Розглянемо дві найвідоміші таксономії систем підтримки прийняття рішень.

Класифікація систем підтримки прийняття рішень Альтера, розроблена на основі емпіричних досліджень 56 різних СППР, виділяє два типи систем.

1. Системи, орієнтовані на дані (вибирають інформацію):

- накопичування файлів (File draver systems);
- аналізу даних (Data analysis systems);
- аналізу інформації (Analysis information systems).

2. Системи, орієнтовані на моделі (дають змогу підтримувати прийняття рішень):

- розрахункові або облікові та фінансові моделі;
- репрезентативні або образні;
- оптимізаційні;

- рекомендаційні. [35, 89]

Класифікація СППР Пауера передбачає виділення п'яти категорій СППР (орієнтовані на дані СППР (Data-driven DSS), орієнтовані на моделі СППР (Model-driven DSS), на знання СППР (Knowledge-driven DSS), на документи СППР (Document-driven DSS), на комунікації та групові СППР і три групи, які ґрунтуються на вторинних ознаках (ін-терорганізаційні та інтраорганізаційні СППР, функціонально-специфічні СППР і СППР загального призначення, СППР на базі Web).

Різноманіття нових інструментів (методи штучного інтелекту, системи інтелектуального аналізу даних, оперативна аналітична обробка - OLAP і технології (World Wide Web, Інтернет, інтернет-мережі) здатне розширити можливості СППР і змінити форми розвитку.

Системи підтримки прийняття рішень набули широкого застосування в економіках різних країн, причому їх кількість постійно зростає. Орієнтовані на операційне управління СППР застосовуються в маркетингу (для прогнозування й аналізу збуту, дослідження ринку і цін), для виконання науково-дослідних і конструкторських робіт, в управлінні кадрами, виробництвом тощо. Найбільша частка комп'ютерної підтримки різних функцій припадає на стратегічне планування, управління і розвиток підприємств, операційне управління й розподіл ресурсів.

Розглянемо окремі системи підтримки прийняття рішень, що використовуються в економіці. Так, система підтримки прийняття рішень «Combi-PC» передбачає в ролі об'єктів аналізу різні види продукції, варіанти планів, заходів, виконавців, підприємств. База даних системи будується як набір таблиць. Порівняльна оцінка об'єктів у процедурах вибору підтримується множиною алгоритмів і процедур багатокритеріального впорядкування (методи порогів порівнянності, парних порівнянь, ітеративна спортивна модель, процедури експертної та одновимірної класифікацій). Користувач може конструювати метод розв'язання своєї задачі як ланцюжок етапів або підбирати готовий метод із бібліотеки. Ця система підтримки

прийняття рішень дає змогу розв'язувати задачі оцінювання адаптаційних можливостей галузей економіки, аналізу системи показників якості продукції, тематичного планування науково-дослідних і конструкторських робіт, порівняльного аналізу діяльності підприємств.

Система підтримки прийняття рішень DSS-UTES призначена для пошуку оптимальних рішень у складних проблемних моделях. її побудовано як відкриту систему, що дає змогу підключати для виконання окремих етапів розв'язання задачі автономні проблемні блоки і моделі користувача. До складу DSS-UTES входять: диспетчер системи; підсистема побудови багатовимірної функції корисності; підсистема оцінювання результатів роботи моделі; підсистема оптимізації керівних параметрів програми користувача.

Система підтримки прийняття рішень ISDS може бути використана інноваційними та фінансовими менеджерами у формуванні програм розробки нових виробів і технологій у великих корпораціях. Система підтримує такі функції: попередній відбір пропозицій для інноваційних проектів; порівняльний аналіз нових пропозицій і проектів, які вже розробляються; формування інвестиційних груп із проектів, що пропонуються для розробки.

Система підтримки прийняття рішень Marketing Expert забезпечує підтримку прийняття рішень на всіх етапах розробки стратегічного і тактичного планів маркетингу та контролю за їх реалізацією. Система виконує два основні завдання: аудит маркетингу; планування маркетингу з використанням відомих аналітичних методик (GAP-аналізу, сегментного аналізу, SWOT-аналізу, Portfolio-аналізу та ін.).

Система підтримки прийняття рішень Decisiyn Grid - програмна оболонка для автоматизації процесу зіставлення дискретних альтернатив за багатьма критеріями. Інформація для прийняття рішень уводиться в порівняльну таблицю, стовпці якої відповідають альтернативам, а рядки - критеріям їх оцінювання. На перетині рядків і стовпців розміщується оцінка альтернативи за певним критерієм. Система має багато функціональних можливостей, які створюють зручні умови для кращого оцінювання і

порівняння альтернатив і, отже, підвищують якість процесу прийняття рішень. Є можливість побудови сценарію дій, графічного перегляду результатів, використання шаблонів.

Система підтримки прийняття рішень Visual IFPS/Plus (Interactive Financial Planning System) - інтерактивна система планування фінансів. Система дає змогу розв'язувати досить широкий спектр задач: добір балансових підсумків, розподіл прибутку за статтями доходів, передбачення змін валютних курсів, прогнозування, аналіз ризиків, розробки стратегії збуту продукції, відбір науково-дослідних проектів, стратегічне планування, планування прибутку і бюджету, вибір між стратегіями закупівлі та виготовлення продукції власними силами тощо. СППР Visual IFPS/Plus має широке застосування у фінансах, статистиці й управлінні виробництвом.

В галузі права можна визначити такі напрями застосування інтелектуальних систем і технологій:

- інтелектуалізація автоматизованих інформаційно-пошукових систем із законодавства;
- створення автоматизованих систем аналізу нормативних правових текстів;
- побудова консультативних систем із правотворення;
- створення експертних систем у сфері правозастосовної діяльності;
- розробка алгоритмів і програм ідентифікації за допомогою ЕОМ об'єктів при розслідуванні та розгляді судових справ (сфера криміналістики й судової експертизи). [12; 19]

Зарубіжні комерційні правові експертні системи використовуються переважно в галузі управління фінансами. Наведемо кілька прикладів.

Експертна система «DSCAS» допомагає аналізувати юридичні аспекти позовів щодо відшкодування додаткових витрат, пов'язаних з відмінностями фізичних умов на місці передбачуваного будівництва від зазначених у контракті. Такі позови ґрунтуються на даних, які містяться в конкретних

договорах. ЕС забезпечує посадову особу правовими знаннями для прийняття рішення щодо позову.

Експертна система «LEGAL ANALYSIS SYSTEM» допомагає адвокатам аналізувати справи про навмисну образу дією з погляду права і практики його застосування.

Експертна система «ТАХМАМ» допомагає дослідити логіку міркувань та аргументацію на прикладі законодавства про оподаткування корпорацій.

Експертна система «SAL» підтримує юристів при встановленні розмірів позовів, пов'язаних із професійними захворюваннями робітників, які працюють з азбестом.

Окремого розгляду потребують пакети програм для аналізу рішень. Комп'ютеризовані інструментальні засоби аналізу рішень допомагають прийняти рішення щодо проведення декомпозиції та структурування проблеми, застосовуючи подібні до дерев рішень моделі, моделі багатоатрибутної корисності, аналітичний ієрархічний процес (Analytical Hierarchy Process - AHP). Приклади пакетів програм для аналізу рішень: AliahThink, BestChoice3, Criterium Decision Plus, DecideRight, DecisionMaker, Demos, DPL, Expert Choice, Strad.

AHP - це потужний і гнучкий процес підтримки прийняття рішень, що допомагає менеджерам визначати пріоритети і приймати найкращі рішення за умов урахування їх кількісного та якісного аспектів.

Система підтримки прийняття рішень Analytica 2.0 - програмне забезпечення кількісного моделювання. її можливості включають аналіз сценаріїв, діаграми впливу, багатовимірне моделювання й аналіз ризику. Система забезпечує прозорість і потужність бізнес-моделювання, це інструментальний засіб створення й аналізу кількісних бізнес-моделей Analytica 2.0 широко використовується для створення й дослідження моделей у різних галузях: бізнес і фінанси; аеропростір; консалтинг; електронна комерція; охорона здоров'я; енергетика й навколишнє середовище; захист;

науково-технічні дослідження; виробництво; телекомунікації; вища освіта і т. д.

Система підтримки прийняття рішень Expert Choice орієнтована на застосування діаграм впливу. Expert Choice базується на одному з відомих методів прийняття рішень AHP - багатокритеріальному ієрархічному підході до підтримки прийняття рішень. Ця СППР забезпечує такі можливості: полегшує визначення й описання мети (цілей); полегшує ідентифікацію всього рангу альтернативних розв'язків; оцінює ключові співвідношення (компроміси) між цілями й альтернативами; дає змогу отримати рішення, яке повністю зрозуміле та підтримується групою розробників проблеми.

Expert Choice об'єднує і синтезує думки будь-якої кількості осіб, котрі приймають рішення, щоб забезпечити повний спектр різного сприйняття проблеми. Система має п'ять діаграм чутливості ("що..., якщо...?"), які динамічно тестують сценарії, для з'ясування того, як зміна ваги одного з критеріїв впливає на результат вибору. Expert Choice здійснює попарні порівняння, щоб визначити пріоритети для цілей і альтернатив. Групові оцінки можуть бути введені з використанням радіохвиль або через Інтернет. Якщо в процесі попарних оцінювань беруть участь кілька осіб, то середнє геометричне значення результатів оцінювань у подальшому враховується як загальна оцінка групи експертів. [35]

Таким чином, можемо констатувати, що системами підтримки прийняття рішень називають інтелектуальні системи, за допомогою яких особи, що приймають рішення (ОПР), мають змогу аналізувати ситуації, формулювати задачі, виробляти, контролювати й оцінювати варіанти рішень, які забезпечують досягнення поставленої мети. СППР має бути дієвою інтерактивною системою, що реагує як на заплановані, так і на непередбачувані інформаційні запити, зорієнтована на специфічний тип рішень або на множину взаємозв'язаних рішень і застосовується там, де неможливо або небажано мати повністю автоматичну систему.

Сфера використання таких систем практично необмежена. Вони мають не лише суто економічне застосування, а й призначаються для правоохоронних органів, судового виробництва, органів виконання покарань, національної безпеки, військової розвідки, митниці, податкової поліції, міграційної служби та багатьох інших.

## Висновки до першого розділу

1. Система підтримки прийняття рішень – це інтерактивна комп'ютерна система, яка призначена для підтримки різних видів діяльності при прийнятті рішень із слабоструктурованих або неструктурованих проблем. Інтерес до СППР, як перспективної галузі використання обчислювальної техніки та інструментарію підвищення ефективності праці в сфері управління економікою, постійно зростає.

Експертна система повинна мати можливість пояснити, чому запропоновано саме цей розв'язок і довести його обґрунтованість. Користувач повинен отримати всю інформацію, необхідну йому для того, аби переконатись в обґрунтованості запропонованого розв'язку. Експертна система - це програма, що поводиться подібно експерту в деякій, звичайно вузькій прикладній області. Типові застосування експертних систем містять у собі такі задачі, як медична діагностика, локалізація несправностей в устаткуванні й інтерпретація результатів вимірів.

При розробці експертної системи прийнято поділяти її на три основних модулі: база знань; машина логічного висновку; інтерфейс із користувачем. База знань містить знання, що відносяться до конкретної прикладної області, у тому числі окремі факти, правила, що описують чи відносини що описують чи відносини явища, а також, можливо, методи, евристики і різні ідеї, що відносяться до рішення задач у цій прикладній області. Машина логічного висновку вміє активно використовувати інформацію, що міститься в базі знань. Інтерфейс із користувачем відповідає за безперебійний обмін

інформацією між користувачем і системою; він також дає користувачу можливість спостерігати за процесом рішення задач, що протікають у машині логічного висновку.

2. Системами підтримки прийняття рішень називають інтелектуальні системи, за допомогою яких особи, що приймають рішення (ОПР), мають змогу аналізувати ситуації, формулювати задачі, виробляти, контролювати й оцінювати варіанти рішень, які забезпечують досягнення поставленої мети. Згідно з таким узагальненим визначенням можна тлумачити СППР як одну з категорій управлінських інформаційних систем.

Основні категорії систем підтримки прийняття рішень розглядають залежно від того, який із головних компонентів системи взято за домінуючий.

Системи підтримки прийняття рішень, зорієнтовані на дані, – це тип СППР, який зосереджується передусім на доступі й маніпуляції великими базами структурованих даних. До цієї категорії відносять: системи підготовки управлінських звітів; сховища даних; системи аналізу даних (ALOP); виконавчі інформаційні системи (інформаційна система керівника); географічні ІС;

Другу велику категорію становлять СППР, зорієнтовані на доступ та маніпуляцію моделями – статистичними, фінансовими, оптимізаційними і/або імітаційними. Здебільшого такі системи використовують дані й параметри, що їх надають ОПР, але, як правило, не потребують великих обсягів даних. Приклади таких СППР: засоби аналізу рішень, які допомагають ОПР розбити проблему на складові й структурувати її; засоби лінійного програмування; імітаційні засоби.

# РОЗДІЛ 2. ОРГАНІЗАЦІЙНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЙ

## *2.1. Теоретичні засади забезпечення інформаційної безпеки організацій*

Проблема безпеки як соціального явища виділяється як одна із глобальних проблем сучасності. В самому широкому плані категорія “безпека” характеризує такий стан людського суспільства, при якому забезпечується нормальне його існування (виживання) та розвиток [24, с.15]. Безпека розуміється як критерій, обставина збереження об’єкта і надійності його функціонування.

Якщо розглядати рівні безпеки по аналогії із структурою самої соціальної системи, то можна виділити:

- безпеку суспільства в цілому;
- безпеку компонентів соціальної системи ( підсистем і елементів);
- безпеку середовища, в якому функціонує суспільство.

Конституція України, що стала гарантом побудови демократичної правової держави, не могла не врахувати загальносвітових тенденцій інформатизації суспільства. Тому ряд її статей визначають забезпечення інформаційної безпеки як одну з найважливіших функцій держави і мають стати запорукою розвитку національного інформаційного законодавства. Згідно, Закону України “Про Національну програму інформатизації”, інформаційна безпека - невід’ємна частина політичної, економічної, оборонної та інших складових національної безпеки [3].

Досить тривалий час поняття «кібербезпека» та «інформаційна безпека» в науковій та спеціальній літературі, ототожнювали або розглядали кібербезпеку як складову інформаційної безпеки. Але у «Стратегії національної безпеки України» надається розмежування понять кібербезпека

та інформаційна безпека, шляхом визначення загроз інформаційній безпеці та загроз кібербезпеці і безпеці інформаційних ресурсів [6].

Так, до загроз інформаційній безпеці віднесено ведення інформаційної війни проти України; відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства. Загрози кібербезпеці і безпеці інформаційних ресурсів 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.

Не спиняючись на визначені загроз, було встановлено Пріоритети забезпечення інформаційної безпеки до яких віднесено забезпечення наступальності заходів політики інформаційної безпеки на основі асиметричних дій проти всіх форм і проявів інформаційної агресії; створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них; протидія інформаційним операціям проти України, маніпуляціям суспільною свідомістю і поширенню спотвореної інформації, захист національних цінностей та зміцнення єдності українського суспільства; розробка і реалізація скоординованої інформаційної політики органів державної влади; виявлення суб'єктів українського інформаційного простору, що створені та/або використовуються Росією для ведення інформаційної війни проти України, та унеможливлення їхньої підривної діяльності; створення і розвиток інститутів, що відповідають за інформаційно-психологічну безпеку, з урахуванням практики держав - членів НАТО; удосконалення професійної підготовки у сфері інформаційної безпеки, упровадження загальнонаціональних освітніх програм з медіакультури із залученням громадянського суспільства та бізнесу[6].

На думку вчених, інформаційна безпека – це стан захищеності інформаційного простору, що забезпечує формування та розвиток цього простору в інтересах особистості, суспільства та держави[13; 23]. В межах даного напряму існує визначення інформаційної безпеки як стану, тенденції

розвитку, умови життєдіяльності соціуму, його структур, інститутів та установ, за яких забезпечується збереження якісної, з об’єктивно обумовленими інноваціями в ній, вільної, відповідно власній природіфункціонування інформації. Ряд представників цього напряму розглядають інформаційну безпеку як стан, що характеризується відсутністю небезпеки, тобто чинників та умов, які загрожують безпосередньо індивіду, спільноті, державі з боку інформаційно-комунікаційного середовища.

Отже, інформаційна безпека являє собою одне з найважливіших понять в науці і в різних сферах людської діяльності. Сутність і комплексність цього поняття обумовлюється характером сучасного інформаційного суспільства. Аналіз різних підходів до визначення змісту поняття „інформаційна безпека” дає змогу зауважити про недоцільність жорсткого обрання тієї чи іншої позиції. Наведені вище підходи до визначення поняття інформаційної безпеки дають змогу розглядати дану проблему комплексно та системно. Інформаційна безпека є і властивістю, і атрибутом інформаційного суспільства, і діяльністю, і результатом діяльності людини, спрямованої на забезпечення певного рівня безпеки в інформаційній сфері.

Зміст поняття „інформаційна безпека” розкривається у практичній діяльності, наукових дослідженнях, а також нормативно-правових документах. Варто зазначити, що у науковій літературі поки відсутній єдиний консолідований підхід до змісту поняття „інформаційна безпека”. Для одних воно відображає стан, для інших процес, діяльність, здатність, систему гарантій, властивість, функцію. З метою упорядкування різних поглядів ми вирішили їх класифікувати за критерієм ознаки, що визначає зміст даного поняття.

Так, Гаєвський В.К., Авраменко В.А. визначають інформаційну безпеку як стан захищеності життєво важливих інтересів особи, суспільства та держави, який виключає можливість заподіяння їм шкоди через неповноту, невчасність і недостовірність інформації, через негативні наслідки функціонування інформаційних технологій або внаслідок поширення

законодавчо забороненої чи обмеженої для поширення інформації, тоді як Додонов О.Г. визначає інформаційну безпеку як стан захищеності інформаційного простору, що забезпечує формування та розвиток цього простору в інтересах особистості, суспільства та держави [13; 23-24].

Так, науковці вказують, що безпека це - стан захищеності особи, суспільства та держави від зовнішніх та внутрішніх небезпек та загроз, який базується на діяльності людей, суспільства, держави, світового співтовариства по виявленню (вивченню), попередженню, послабленню, ліквідації та відбиттю небезпек і загроз, здатних знищити їх, позбавити фундаментальних матеріальних і духовних цінностей, завдати неприйнятну шкоду, закрити шлях для прогресивного розвитку [13; 38].

Цікаве судження з цього приводу відомого українського дослідника проблем інформаційної безпеки Калюжного Р.А. Він вважає, що інформаційна безпека - вид суспільних інформаційних правовідносин щодо створення, підтримки, охорони та захисту бажаних для людини, суспільства і держави безпечних умов життєдіяльності; суспільних правовідносин пов’язаних із створенням, поширенням, зберіганням та використанням інформації[12, с. 17-21].

Провідними елементами системи кібернетичної та інформаційної безпеки, у тому числі щодо захисту інформації в інформаційно-телекомунікаційних системах, є такі найважливіші чинники:

- провідний предмет суспільних правовідносин – інформація в інформаційно-телекомунікаційних системах;

- суб’єкти – окремі люди, їх спільноти, різного роду організації, суспільство, держава, інші держави, їх союзи, світове співтовариство.

- об’єкт – правовідносини між суб’єктами (суспільні відносини), які визначаються за певними об’єктивно існуючими критеріями.

Однією із складових інформаційної безпеки є інформаційна безпека підприємств та організацій.

Безпека підприємства - це стан стійкої життєдіяльності, за якого забезпечується реалізація основних інтересів і пріоритетних цілей підприємства, захист від зовнішніх і внутрішніх дестабілізуючих факторів незалежно від умов функціонування [21,6]

Зважаючи на надане визначення поняття «безпека підприємства», можна зробити висновок, що основною метою забезпечення безпеки підприємств та організацій є нейтралізація та ліквідація загроз належному здійсненню підприємницької діяльності в Україні, у результаті настання яких можуть бути нанесені підприємствам або організаціям усіх форм власності збитки або упущено отримання вигоди.

До числа найбільш поширених визначень поняття «інформаційна безпека підприємництва» відносяться такі:

- це суспільні відносини щодо створення та підтримання на належному (бажаному, можливому) рівні життєдіяльності відповідної інформаційної системи, у тому числі підприємництва[38, 89];
- це суспільні відносини щодо створення і підтримання на належному рівні життєдіяльності інформаційної системи суб’єкта господарської діяльності [33, 34];
- -це відношення рівня інформаційного захисту до рівня інформаційних загроз; сукупність засобів та дій уповноважених осіб, спрямованих на захист інформаційних ресурсів та інформаційної інфраструктури даного підприємства в процесі обміну, обробки та зберігання інформації на всіх рівнях інформаційної системи підприємства [22,55].

Ефективне функціонування інформаційної безпеки організацій неможливе без забезпечення її стабільності, що досягається у результаті діяльності органів державної влади шляхом прийняття необхідних нормативно-правових актів та діяльності відповідних суб’єктів, на яких покладено безпосередній обов’язок щодо вироблення та реалізації

нормативних, організаційних та технічних заходів, спрямованих на забезпечення інформаційної безпеки в організації.

Метою забезпечення інформаційної безпеки підприємництва в Україні є створення умов для безперешкодного здійснення підприємницької діяльності (підприємництва) в Україні шляхом забезпечення ефективного функціонування інформаційної системи суб'єктів господарської діяльності.

Одним із кроків у напрямку забезпечення інформаційної безпеки організацій та підприємств є інформаційно-аналітичне забезпечення безпеки організацій та підприємств . На думку Є.В. Позднишева, інформаційно-аналітичне забезпечення безпеки підприємництва - це вид інформаційно-аналітичного забезпечення підприємницької діяльності, який здійснюється оцінці обстановки і прийнятті рішення на відповідному стратегічному, оперативному та тактичному рівнях в інтересах розвитку підприємства шляхом добування, обробки і надання керівництву необхідної інформації [21,7].

Слід зазначити, що для кожного суб'єкта господарської діяльності проблема забезпечення інформаційної безпеки є індивідуальною справою, оскільки має відображати особливості забезпечення інформаційної безпеки на даному підприємстві з урахуванням специфіки його діяльності та пріоритетних у даному випадку напрямків захисту інформації. Але, у той самий час на державному рівні у відповідних нормативно-правових актах має бути визначено та закріплено базову модель забезпечення інформаційної безпеки підприємництва в державі в цілому. Враховуючи основні положення базової моделі, на окремих підприємствах вже мають вироблятися та впроваджуватися різноманітні заходи, спрямовані на належне забезпечення інформаційної безпеки підприємства.

Отже інформаційна безпека являє собою одне з найважливіших понять у науці, а також в різних сферах людської життєдіяльності. Сутність і комплексність цього поняття визначені характером сучасного інформаційного суспільства. Аналіз різних підходів до визначення змісту поняття

„інформаційна безпека” дає змогу зауважити про недоцільність жорсткого обрання тієї чи іншої позиції. Наведені вище підходи до визначення поняття інформаційної безпеки дають змогу розглядати дану проблему комплексно та системно, додати знань про цей багатогранний феномен.

Такий підхід дав нам можливість зробити висновок, що інформаційна безпека не може розглядатися лише в якості окремого стану. Безперечно, вона є і властивістю, і атрибутом інформаційного суспільства, і діяльністю, і результатом діяльності людини, спрямованої на забезпечення певного рівня безпеки в інформаційній сфері. Інформаційна безпека має враховувати майбутнє, отже вона є не станом, а процесом. Таким чином, інформаційну безпеку слід розглядати крізь органічну єдність ознак, таких як стан, властивість, а також управління загрозами і небезпеками, за якого забезпечується обрання оптимального шляху їх усунення та мінімізації впливу негативних наслідків.

При дослідженні сутності інформаційної безпеки має враховуватися той факт, що сутність є внутрішнім змістом предмету, який знаходить відображення у сталій єдності усіх багатоманітних і суперечливих форм буття. Базовою характеристикою інформаційної безпеки слід вважати імовірність підвищеного ризику реалізації загрози або небезпеки для діяльності органів влади в цілому і для кожного її структурного елементу зокрема. Критерієм ефективності забезпечення інформаційної безпеки є високий рівень безпеки при мінімумі відповідних затрат. Отже можна говорити про структуру поняття інформаційної безпеки. Основним її елементом є життєво важливі інтереси соціальної системи, які співвідносяться із зовнішніми чинниками у вигляді інтересів наднаціональних або інших національно-державних структур в рамках міжнародного співтовариства. Зсередини національно-державного утворення його життєво важливі інтереси взаємодіють з інтересами його складових елементів. В якості останніх виступають соціальні групи, еліта, організації, партії, релігійні та етнічні утворення, рухи тощо. Сукупність

внутрішніх і зовнішніх інформаційних загроз створює передумови для порушення безпечного функціонування системи органів влади.

Метою будь-якого виду інформаційної безпеки є забезпечення цінності системи, захист і гарантування точності і цілісності інформації, і мінімізування руйнування, що можуть мати місце, якщо інформація буде модифікована чи зруйнована.

В науковій та спеціальній літературі до об’єктів інформаційної безпеки відносять інформаційні ресурси, канали інформаційного обміну і телекомунікації, механізм забезпечення функціонування телекомунікаційних систем і мереж та інші елементи інформаційної інфраструктури країни.

Загрози інформаційної безпеки в організації поділені за трьома ознаками:

- джерело загрози;
- об'єкт загрози;
- методи та засоби реалізації загрози. [13;42]

Кожна з виділених ознак містить свої характеристики, що відображають його особливості та впливають на характер загрози. Джерело загрози має дві важливі характеристики – тип та розташування; об'єкт загрози характеризується типом та метою загрози; методи та засоби реалізації загрози обумовлені особливостями джерела та об'єкта загрози.

Безліч джерел небезпеки представлено у вигляді матриці розмірністю 3x2:

$$I = \begin{pmatrix} I_A^{in} & I_A^{out} \\ I_T^{in} & I_T^{out} \\ I_C^{in} & I_C^{out} \end{pmatrix},$$

або I=$\{ I_j^k \}$,де j - індекс типу джерела загрози, j = {A, T, C}, IA - безліч антропогенних джерел загрози; IT – безліч техногенних джерел загрози; IC – безліч стихійних джерел небезпеки; k – індекс розташування джерела загрози, k={in,out}, Iin – безліч внутрішніх джерел загрози, Iout – безліч зовнішніх

джерел загрози.

Вважаючи, що будь-яке джерело загрози спрямоване на будь-який ресурс організації з метою порушення будь-якого аспекту ІБ, задається бінарне ставлення $\rho_1 = (I_j^k, O_i^m)$ реальних пар «джерело загрози – об'єкт загрози», де

$\rho_1 \in I \times O = \{(I_j^k, O_i^m) \mid I_j^k \in I, O_i^m \in O\}$.

Будь-яке джерело загрози, спрямований на конкретний об'єкт і має певну мету порушення аспекту ІБ, використовує для реалізації методи та пов'язані з ними засоби, що описується бінарним ставленням $\rho_2 = (z_e, l_q)$, $z_e \in Z$, $l_q \in L$, де Z - безліч методів реалізації загрози; L – безліч засобів реалізації небезпеки.

Таким чином, можна записати, що якщо на множині IxO задано бінарне відношення $\rho_1 = (I_j^k, O_i^m)$ і на безлічі ZxL поставлено бінарне відношення $\rho_2 = (z_e, l_q)$, то можливе відображення f, що задає відповідність $(I_j^k, O_i^m) \xrightarrow{f} (z_e, l_q)$ і має такі особливості: значення функції залежать від змінних $I_j^k$ і $O_i^m$; умови бієкції виконуються, т.к. не виконуються умови ін'єкції (область визначення визначається парами $(I_j^k, O_i^m)$ на множині IxO, а значення функції з множини ZxL для різних елементів можуть збігатися). Відображення f є сюр'єктивним, а завдання множини пар (ze,lq) виконується експертними процедурами.

Таким чином, формалізований опис загроз ІБ організації набуде вигляду:

$U = (I_j^k, O_i^m, z_e, L_n)$,

де $I_j^k$ -ідентифікатор джерела загрози, що характеризується типом та розташуванням; $O_i^m$ -ідентифікатор об'єкта загрози, що характеризується типом ресурсу організації та метою порушення аспекту ІБ; $z_e$ -ідентифікатор е-го способу реалізації небезпеки; $L_n$ -ідентифікатор n-го підмножини засобів реалізації небезпеки.

Багато ресурсів організації представляється R={RH, RF, RS}, де RH – безліч людських ресурсів, RF – безліч фізичних ресурсів, RS – безліч інформаційних ресурсів. У свою чергу, кожен із типів ресурсу є безліччю, що

містить елементи: Rj={rji}, де j – ідентифікатор типу ресурсу, і – номер j – го типу ресурсу. Вважаючи, що багато загроз ІБ спрямовані попри всі ресурси організації, тобто. $\exists \tau_1 \in R \times U = \{(r_{ji}; u_i)\}$ і має місце (1), то бінарне відношення $\tau 1$ визначається однозначно щодо об'єкту загрози, тобто. $r_{ji} \equiv O_i^m$.

Для безлічі загроз ІБ організації існує безліч заходів щодо їх нейтралізації: V = {vi}. Бінарне відношення реальних пар «загроза – методи нейтралізації» має вигляд: $\tau 2 \in UxV = \{(ui; vi)\}$. З іншого боку, ЗІБ організації передбачає захист всіх ресурсів, тобто. з кожним ресурсом організації пов'язано безліч заходів щодо ЗІБ, що відбивається бінарним ставленням $\tau 3 \in RxW = \{(rji; wi)\}$, де R - безліч ресурсів організації; W – безліч заходів щодо ОІБ, спрямованих на захист ресурсів.

Вибір заходів з ЗІБ визначається нечіткою відповідністю множин U і W: Г={U,W,F}, де F – функція приналежності UxW, яка задається у вигляді графа з безліччю вершин $U \cup W$, кожна дуга якого позначає функцію приладдя $\mu_F(u_i, w_j)$ або за допомогою матриці інциденцій RГ, рядки якої позначені елементами wj, а стовпці – ui, на перетині рядків та стовпців розташований елемент $k_h = \mu_F(u_i, w_j)$, де $\mu_F$ -функція власності елементів нечіткого графіку.

Для генерації варіантів заходів забезпечення інформації безпеки завдання оптимізації (залежно від вимог користувача) формулюється у двох варіантах.

*Перший варіант*. Відомі вартості ресурсів організації, загроз, методів та засобів захисту ресурсів від загроз: $c(r_{ji}), c(u_i), c(w_i)$. Слід визначити за заданих значень ризиків з урахуванням проведеної селекції мінімальні витрати на ВІБ. У цьому запроваджено обмеження: вартість ресурсу більше чи дорівнює вартості загрози, спрямованої нього, інакше, кошти, витрачені реалізацію загрози, економічно не виправдані. З тієї ж причини вартість ресурсу більша або дорівнює вартості заходів щодо його захисту.

Другий варіант. Відомі вартості ресурсів організації, загроз, методів та засобів захисту ресурсів від загроз: $c(r_{ji}), c(u_i), c(w_i)$. Необхідно визначити

мінімальне значення ризиків за заданого значення витрат на забезпечення інформаційної безпеки.

За тих же обмежень маємо треті варіант.

$$\begin{cases} C_{опБ} = \sum_{i=1}^{n} c(w_i) \to \min \\ C_{риск} = \sum_{i=1}^{m} f(r_{ji}, u_i) \le C_{зад} \\ c(u_i) \le c(w_i) \le c(r_{ji}) \\ c(u_i); c(r_{ji}); c(w_i); j = \overline{1,m} \end{cases} \qquad \begin{cases} C_{риск} = \sum_{i=1}^{m} f(r_{ji}, u_i) \to \min \\ C_{опБ} = \sum_{i=1}^{n} c(w_i) \le C_{зад} \\ c(u_i) \le c(w_i) \le c(r_{ji}) \\ c(u_i); c(r_{ji}); c(w_i); j = \overline{1,m} \end{cases}$$

Вибір оптимального варіанту зі згенерованої множини ідентичний типової задачі прийняття рішення групою експертів з використанням теорії нечітких множин.

Розроблена методика забезпечення інформаційної безпеки організації включає кілька етапів. Перший етап – створення моделі об'єкта забезпечення інформаційної безпеки, яка формується шляхом внесення до системи повної інформації про всі ресурси організації, що входять до інформаційної системи організації. Другий етап оцінки важливості ресурсів з погляду інформаційної безпеки, визначення відповідності між існуючим та необхідним рівнями інформаційної безпеки в організації. Третій етап – виявлення вразливостей та оцінка ризиків. Виконання дій за даними етапами формує на виході повну модель об'єкта інформаційної безпеки з урахуванням реального виконання вимог. Побудована модель аналізується та генерується звіт, який містить значення ризику для кожного ресурсу. Користувач задає критерії оптимізації, за якими генеруються оптимальні варіанти заходів щодо інформаційної безпеки. [21]

Ризик характеризує збитки, які можуть настати в результаті реалізації загроз, і залежить від показників цінності ресурсів, ймовірності реалізації загроз та вразливостей в забезпеченні інформаційної безпеки. Процедура оцінки ризиків полягає в використанні якісних величин оцінок загроз, ресурсів, і вразливостей. Вразливість ресурсу диференційована на низьку (Н), середню (С) та високу (В), а величина ризику у показниках та шкалах даної методики належить інтервалу від 0 до 9.

Таким чином, в науковій та спеціальній літературі інформаційна безпека розглядається як елемент або підсистема національної безпеки. На нашу думку, інформаційна безпека – це рівень захищеності життєвоважливих інтересів людини, суспільства і держави в інформаційній сфері від зовнішніх та внутрішніх загроз

Провідними елементами системи інформаційної безпеки, у тому числі щодо захисту інформації в інформаційно-телекомунікаційних системах, є такі найважливіші чинники:

- провідний предмет суспільних правовідносин – інформація в інформаційно-телекомунікаційних системах;

- суб'єкти – окремі люди, їх спільноти, різного роду організації, суспільство, держава, інші держави, їх союзи, світове співтовариство.

- об'єкт – правовідносини між суб'єктами (суспільні відносини), які визначаються за певними об'єктивно існуючими критеріями.

Найбільшу загрозу інформаційним ресурсам, що можуть спричинити небажаний вплив на інформаційну систему, а також на інформацію, яка зберігається в ній, представляють: розкриття інформаційних ресурсів; порушення їх цілісності; збій у роботі самого обладнання.

## *2.2. Методи та засоби забезпечення інформаційної безпеки організацій*

Визначальним у проблематиці теорії організації інформаційної безпеки є з’ясування її напрямків на засадах комплексного підходу щодо методів захисту. Аналіз наукових досліджень, що присвячені визначенню напрямків та методів захисту інформації, дозволяє умовно визначити такі напрямки захисту: правові, організаційні (управлінські), програмні, технічні та криптографічні.

Так, безпекою інформаційних систем (інформаційна безпека), що часто скорочується до infosec, називається практика, політика й принципи захисту цифрових даних та інших видів інформації. Вона стосується процесів та методологій, пов'язаних із збереженням конфіденційної інформації, доступності та забезпеченням її цілісності. [42]

Це також стосується:

- контроль доступу, який запобігає входу або доступу до системи несанкціонованого персоналу;
- захист інформації незалежно від того, де ця інформація знаходиться, тобто в дорозі (наприклад, в електронній пошті) або в зоні зберігання;
- виявлення та усунення порушень безпеки, а також документування цих подій.

До сфери infosec входить створення набору бізнес-процесів, які захищатимуть інформаційні активи, незалежно від того, як ця інформація відформатована, чи передається вона, обробляється або перебуває у сховищі.

Як правило, організація застосовує інформаційну безпеку для захисту своїх цифрових даних як частину загальної програми забезпечення кібербезпеки. Три основні принципи infosec, які називають тріадою ЦРУ, - це конфіденційність, цілісність і доступність.

Тож, якщо коротко, інформаційна безпека - це гарантія того, що ваші співробітники зможуть переглядати та редагувати потрібні їм дані, при цьому не дозволяючи нікому більше отримати доступ до них. Інформаційна безпека також пов'язана із системами управління ризиками та правовими нормами. Варто поглибитися в те, чим саме є комп'ютерна безпека в сфері IT, які бувають IT-технології, системи, рішення для захисту даних і забезпечення інформаційної цілісності. [42]

Політика інформаційної безпеки реалізується як системою інститутів публічної влади, так і інститутами громадянського суспільства, до компетенції яких стосується вирішення питань щодо створення безпечних умов функціонування і розвитку інформаційної сфери. Проблема забезпечення безпеки в інформаційній сфері поки перебуває на стадії розробки. Дана обставина обумовлена неадекватністю між формуванням інформаційної цивілізації і заходами по забезпеченню інформаційної безпеки. Інформаційна безпека забезпечується проведенням єдиної державної політики національної безпеки в інформаційній сфері, системою заходів економічного, політичного і організаційного характеру, адекватних загрозам та небезпекам національним інтересам особи, суспільства та держави в інформаційній сфері.

Основні завдання вирішуються у межах формалізованої складової механізму інформаційної безпеки, яка представлена органами публічної влади. Залежно від характеру завдань їх виконання є компетенцією державних органів різного рівня, які належать до різних гілок влади мають різні сфери діяльності та обсяги владних повноважень.

Для створення і підтримання належного рівня захисту інформаційних систем розробляється система правових норм, що регулюють відносини в інформаційній сфері, визначаються основні напрями діяльності в цій сфері, формуються або перетворюються органи та сили забезпечення інформаційної безпеки і механізм контролю та нагляду за їх діяльністю.

Система забезпечення інформаційної безпеки створюється і розвивається відповідно до Конституції України та інших нормативно-

правових актів, що регулюють суспільні відносини в інформаційній сфері. Основу даної системи складають органи, сили та засоби забезпечення інформаційної безпеки, які вживають систему адміністративно-правових, інформаційно-аналітичних, організаційно-управлінських, та інших заходів.

У найбільш загальному плані під системою забезпечення інформаційної безпеки у даному дослідженні будемо розуміти систему інформаційно-аналітичних, теоретико-методологічних, адміністративно-правових, організаційно-управлінських, спеціальних та інших заходів, спрямованих на забезпечення стійкого розвитку об’єктів інформаційної безпеки, а також інфраструктури її забезпечення.

Мета функціонування такої системи полягає в організації управління системою інформаційної безпеки через ефективне функціонування системи її забезпечення. Загалом така мета полягає у створенні правових і організаційних механізмів формування, розвитку і забезпечення ефективного використання національних інформаційних ресурсів в усіх сферах життєдіяльності громадянина, суспільства й держави, а також необхідних економічних і соціокультурних умов для цього. Відповідно ефективність системи державного управління національними інформаційними ресурсами та їхнім захистом значною мірою визначає загальний рівень національної безпеки в інформаційній сфері, а будь-які недоліки у структурі й функціонуванні системи державного управління цими процесами призводять до негативних наслідків для суспільства й держави. [37]

Головним завданням системи забезпечення інформаційної безпеки є створення умов для організації управління системою інформаційної безпеки.

Основним змістом системи забезпечення інформаційної безпеки є реалізація сукупності науково-обґрунтованих і апробованих на практиці з урахуванням світового і вітчизняного досвіду заходів, в контексті реалізації державної політики інформаційної безпеки.

Діяльність з реалізації функцій по забезпеченню інформаційної безпеки здійснюється за допомогою загальноприйнятих адміністративно-правових форм.

Під адміністративно-правовою формою забезпечення інформаційної безпеки ми розумітимемо здійснення передбачених нормативно-правовими актами, теорією та практикою державного управління однорідної діяльності посадовими та службовими особами органів виконавчої влади, за допомогою якої реалізується їх компетенція по забезпеченню інформаційної безпеки.

Названі форми поділяються на правові та не правові (організаційні та організаційно-правові) [24,267].Правові форми - це такі види здійснення функцій по забезпеченню інформаційної безпеки, які тягнуть за собою правові наслідки. До них належать: нормотворча, правореалізаційна та правоохоронна, форми.

Неправові форми (організаційні та організаційно-правові форми) по забезпеченню інформаційної безпеки не тягнуть за собою правових наслідків, і знаходять відображення у діяльності органів виконавчої влади щодо здійснення їх завдань і функцій у межах визначеної компетенції. До організаційних форм відносять: регламентуючу, матеріально-технічну, ідеологічну, виховну та ін. [15, 329].

У цілому ж слід зазначити, що вибір цілей і методів протидії конкретним загрозам та небезпекам інформаційній безпеці становить собою важливу проблему і складову частину діяльності по реалізації основних напрямів державної політики інформаційної безпеки.

Особливе значення для інформаційної безпеки має інститут захисту особистих даних, який набув розвитку в багатьох країнах світу. Багато країн вже давно прийняли закони в галузі захисту прав суб'єктів персональних даних і створили на їх основі незалежні від уряду державні органи по захисту таких прав. Ці органи, як правило колегіальні, зазвичай мають назви Комісії по захисту даних. Вперше такий орган було запроваджено в 1919 р. у Швеції, їй почали слідувати інші країни. На сьогодні такі органи діють в Австралії,

Австрії, Англії, Бельгії, Болгарії, Греції, Ізраїлі, Іспанії, Канаді, Кіпрі, Гайані, Маврикії, Нідерландах, Угорщині, Філіппінах, Фінляндії, Франції, ФРН, Швейцарії, Японії тощо [24, 135].

Значну увагу захисту персональних даних приділено і світовим співтовариством. Так, одним з основних міжнародно-правових стандартів в цій галузі вважається прийнята в рамках Ради Європи Конвенція про захист осіб стосовно автоматизованої обробки даних особистого характеру.

Зокрема, згідно з цією Конвенціїєю (ст. 2) “дані особистого характеру” означають будь-яку інформацію, яка стосується конкретно визначеної особи або особи, що може бути конкретно визначеною („суб’єкт даних”). А “автоматизована обробка” включає такі операції, що здійснюються повністю або частково за допомогою автоматизованих засобів: зберігання даних, виконання логічних і/або арифметичних операцій з цими даними, змінення, знищення, вибірка або поширення даних.

Також передбачається, що для захисту даних особистого характеру, що зберігаються у файлах даних для автоматизованої обробки, вживаються відповідні заходи захисту, спрямовані на запобігання випадковому чи несанкціонованому знищенню або випадковій втраті, а також на запобігання несанкціонованому доступу, зміненню або поширенню (ст. 7 Конвенції).

Ще одним аспектом діяльності щодо захисту особистої інформації є забезпечення таємниці листування, телефонних розмов, телеграфної та іншої кореспонденції. Окрім конституційних гарантій, відповідні норми включено і до галузевого законодавства.

Підсумовуючи аналіз правового регулювання захисту інформації щодо приватного життя слід ще раз наголосити на наявності значних прогалин в правовому регулюванні і слабкому розвитку механізмів правозастосування, а іноді і певних правових колізій.

Основні дії щодо збирання, зберігання, передачі та розповсюдження суспільно значущої інформації, як відомо, здійснюються за допомогою спеціальних технічних засобів та технологій. З розвитком науки та техніки ці

інформаційні засоби і технології перетворюються на один із найважливіших компонентів інформаційних процесів, поряд із самою інформацією та суб'єктами інформаційних відносин. А це, у свою чергу, ставить відповідні вимоги щодо рівня безпеки інформаційних засобів і технологій та правового регулювання їх функціонування.

Дуже часто, при вирішенні питань інформаційної безпеки, інформаційні системи, що виступають об'єктом захисту, розглядають виключно крізь призму інформаційно-обчислювальної техніки, визначаючи, наприклад, інформаційно-телекомунікаційну систему як "організаційно-технічну сукупність, що складається з автоматизованої системи та мережі передачі даних"[9; 24;35].

Розглядаючи проблему безпеки інформаційної інфраструктури не можна не відзначити, що на сьогоднішній день найбільш складною є проблема правового регулювання відповідних аспектів функціонування глобальної світової мережі Інтернет. Труднощі починаються навіть з неоднозначності поглядів на сутність цього утворення, що для права є критичним фактором. А відсутність чітко окресленого предмета регулювання робить неефективним або взагалі унеможливлює саме це регулювання. При чому право повинно розглядати Інтернет не лише з технічної точки зору, але й з соціальної, оскільки відносно цієї мережі та всередині неї виникає новий тип суспільних відносин, що можливо повинен бути врегульований правом.

Таким чином, через цілий ряд обставин спроби дати формулювання або визначити зв'язок окремих ознак Інтернет в якості об'єкта права великого успіху не принесли. На сьогодні лише можливо визначити Інтернет як універсальну систему об'єднаних мереж, які дозволяють забезпечити включення будь-яких масивів інформації для надання її користувачам, надання довідникових послуг та інших інформаційних послуг, а також здійснення різних цивільно-правових угод на основі комбінації інформаційно-комунікаційних технологій [9, с. 209 – 210].

Важливим напрямом захисту інформаційної безпеки є встановлення правових засад захисту інформації, що передається або обробляється за допомогою інформаційно-телекомунікаційних систем. Основним нормативно-правовим актом в цій галузі вважається Закон “Про захист інформації в інформаційно-телекомунікаційних системах”[1].

Згідно з цим Законом (ст. 1),інформаційно-телекомунікаційна система – це сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле.

В Законі також визначено перелік неправомірних дій щодо інформації в інформаційно-телекомунікаційних систем (ст. 1), до яких відносяться:

- блокування інформації в системі - дії, внаслідок яких унеможливлюється доступ до інформації в системі;
- виток інформації - результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї;
- знищення інформації в системі - дії, внаслідок яких інформація в системі зникає;
- порушення цілісності інформації в системі - несанкціоновані дії щодо інформації в системі, внаслідок яких змінюється її вміст;

Об'єктами захисту від неправомірних зазіхань є інформація, що обробляється в інформаційно-телекомунікаційній системі, та програмне забезпечення, яке призначено для обробки цієї інформації.

На наш погляд, варто вказати методи та заходи, які вже сьогодні впроваджено в систему забезпечення інформаційної безпеки. Це організаційні, правові, технічні, програмні та криптографічні методи захисту інформації, комп’ютерів, комп’ютерних систем та мереж.

Організаційні заходи захисту інформації та засобів комп'ютерної техніки містять у собі сукупність організаційних заходів щодо підбору, перевірки й інструктажу персоналу, який бере участь у всіх стадіях інформаційного процесу, здійснення режиму таємності при функціонуванні

комп'ютерних систем, забезпечення режиму фізичної охорони об'єктів, а саме організацію охорони обчислювальної техніки; створення особливого перепускного режиму в приміщеннях, де знаходиться комп'ютерна техніка або комп'ютерна інформація; ретельного добору персоналу; виключення випадків проведення особливо важливих робіт лише однією людиною; наявності типових планів дій керівників та обслуговуючого персоналу при виявленні порушень у роботі комп'ютерних мереж, спробах несанкціонованого доступу до інформації, пожежах, стихійному лихові тощо; розробки функціональних обов'язків робітників, допущених до роботи та обслуговування комп'ютерної техніки, комп'ютерної інформації; наявності плану відновлення працездатності обчислювального центру після виходу його з ладу; організації обслуговування та контролю за роботою сторонньої організації або особи, запрошених для обслуговування приміщень, техніки, обладнання комп'ютерних центрів; універсальності засобів захисту від усіх користувачів (в тому числі вищих посадових осіб та співробітників контрольних, правоохоронних органів); встановлення відповідальності та її розмежування між особами, які повинні забезпечувати безпеку комп'ютерної інформації; вибору місця розташування обчислювального (комп'ютерного) центру тощо; періодичного обстеження приміщень, в яких розміщена комп'ютерна техніка з метою виявлення встановлених невідомими особами пристроїв, що пристосовані для можливого зняття інформації, доступу до неї тощо.

Вище ми вже розглянули правові засоби забезпечення інформаційної безпеки. Так, під правовими заходами захисту комп’ютерної інформації та комп’ютерних технологій слід розуміти комплекс цивільно-правових і кримінально-правових норм, які регулюють суспільні відносини в сфері використання комп'ютерної інформації та передбачають відповідальність за несанкціоноване використання даних програмних та технічних засобів. До правових заходів необхідно також віднести питання суспільного контролю за комп’ютерними розробниками [24, 54]. І нарешті, до правових заходів, на нашу думку, треба віднести: розробку законодавства, яке передбачало б

відповідальність за комп'ютерні злочини; захист авторських прав розробників програмного забезпечення; удосконалення адміністративної, кримінальної, цивільної відповідальності в галузі надійного забезпечення функціонування комп'ютерних мереж і комп'ютерної інформації; контроль за розробками комп'ютерних систем певного характеру (правоохоронних, політичних, економічних, освітніх, військових, соціальних тощо).

Для інформаційної безпеки визначальними є два питання правової регламентації електронних інформаційних ресурсів:

1. засади створення і використання цих баз їх власником, щоб виключити можливість порушення прав та законних інтересів третіх осіб;
2. компетенцію та обов’язки органів публічної влади щодо ведення баз даних та надання інформації з них. Це надасть можливість зацікавленим особам звернутися до цих органів за необхідною інформацією.

Технічні заходи призначені для захисту від неправомірного доступу апаратних засобів та засобів зв'язку комп'ютерної техніки. Апаратні засоби і методи захисту реалізуються шляхом застосування різноманітних технічних пристроїв спеціального призначення [24, с. 320]. До технічних заходів, на нашу думку, потрібно віднести: захист від несанкціонованого доступу до системи; резервування особливо важливих комп'ютерних підсистем; організація роботи обчислювальних мереж із можливістю перерозподілу ресурсів у разі порушення працездатності окремих ланок; вжиття конструктивних заходів захисту від крадіжок, шантажу тощо; встановлення резервних систем електроживлення; обладнання приміщень, в яких знаходяться комп'ютери та комп'ютерна інформація системами сигналізації; обладнання приміщень технікою захисту від спроб копіювання інформації ззовні або сторонніми особами.

Важливим інструментом технічним захистом інформаційних систем є, також, стандартизація і сертифікація їхньої діяльності. Для цих цілей, зокрема,

встановлено, що Державний комітет стандартизації, метрології та сертифікації затверджує проекти державних стандартів технічного захисту інформації та проводить реєстрацію нормативних документів, відповідно до яких виготовляються засоби забезпечення технічного захисту інформації, виключно за погодженням з Департаментом спеціальних телекомунікаційних систем та захисту інформації Служби безпеки.

До цієї групи методів захисту відносять:

• засоби захисту кабельної системи. За даними різних досліджень саме збої кабельної системи спричиняють більш як половину відказів ЛОМ. Найкращим способом попередити подібні збої є побудова структурованої кабельної системи (СКС), в якій використовуються однакові кабелі для організації передавання даних в ІС, сигналів від датчиків пожежної безпеки, відеоінформації від охоронної системи, а також локальної телефонної мережі. Поняття «структурованість» означає, що кабельну систему будинку можна поділити на кілька рівнів залежно від її призначення і розміщення. Для ефективної організації надійної СКС слід додержувати вимог міжнародних стандартів;

• засоби захисту системи електроживлення. Американські дослідники з компанії Best Power після п'яти років досліджень проблем електроживлення зробили висновок: на кожному комп'ютері в середньому 289 раз на рік виникають порушення живлення, тобто частіш ніж один раз протягом кожного робочого дня. Найбільш надійним засобом попередження втрат інформації в разі тимчасових відімкнень електроенергії або стрибків напруги в електромережі є установка джерел безперебійного живлення. Різноманітність технічних і споживацьких характеристик дає можливість вибрати засіб, адекватний вимогам. За умов підвищених вимог до роботоздатності ІС можливе використання аварійного електрогенератора або резервних ліній електроживлення, підімкнених до різних підстанцій;

• засоби архівації та дублювання інформації. За значних обсягів інформації доцільно організовувати виділений спеціалізований сервер для

архівації даних. Якщо архівна інформація має велику цінність, її варто зберігати у спеціальному приміщенні, що охороняється. На випадок пожежі або стихійного лиха варто зберігати дублікати найбільш цінних архівів в іншому будинку (можливо, в іншому районі або в іншому місті);

• засоби захисту від відпливу інформації по різних фізичних полях, що виникають під час роботи технічних засобів, — засоби виявлення прослуховувальної апаратури, електромагнітне екранування пристроїв або приміщень, активне радіотехнічне маскування з використанням широкосмугових генераторів шумів тощо. [24;35].

Програмні заходи містять в собі розробку спеціального програмного забезпечення, яке не дозволило б сторонній людині отримувати інформацію з системи. Це засоби захисту інформаційних ресурсів, захисту від копіювання та від комп'ютерних вірусів.

Розглядаючи програмні засоби захисту, доцільно спинитись на криптографічних методах. Під криптографічними заходами слід розуміти спеціальні методи шифрування, кодування або іншого перетворення інформації, в результаті чого її зміст стає недоступним. У наш час найбільш ефективними методами шифрування інформації є криптографія та стеганографія, які найчастіше застосовуються у сукупності. Мета стеганографії – сховати сам факт існування конфіденційної інформації, а мета криптографії – блокування несанкціонованого доступу до інформації [35, 93].

Слово «стеганографія» означає приховане письмо, яке не дає можливості сторонній особі взнати про його існування. Одна з перших згадок про застосування тайнопису датується V століттям до н. е. Сучасним прикладом є випадок роздрукування на ЕОМ контрактів з малопомітними викривленнями обрисів окремих символів тексту - так вносилась шифрована інформація про умови складання контракту.

Криптографія стала не лише справою спецслужб, як би вони того не бажали. 70 – 80-ті рр. XX ст. відзначаються підсиленням суспільного інтересу до криптографії. Виявилось, що криптографічні засоби можуть бути добрим

інструментом захисту прав громадян на конфіденційність листування і переговорів. Цьому сприяло відкриття односторонніх функцій і криптографії з відкритими ключами, так званих “хеш-функцій” (спеціальних ознак повідомлень, за якими легко ідентифікувати повідомлення і виявити його модифікації); механізмів цифрового підпису (аналога звичайного рукописного підпису, який надає електронним документам юридичної сили) тощо [21].

Засіб криптографічного захисту інформації представляє собою програмний, апаратно-програмний, апаратний або інший засіб функціональним призначенням якого є криптографічний захист інформації. Ці засоби є елементами криптографічної системи яка складається з сукупності засобів КЗІ та необхідної ключової, нормативної, експлуатаційної, а також іншої документації .

Щодо впровадження засобів програмно-технічного захисту в ІС, розрізняють два основні його способи:

• додатковий захист — засоби захисту є доповненням до основних програмних і апаратні засобів комп'ютерної системи;

• вбудований захист — механізми захисту реалізуються у вигляді окремих компонентів ІС або розподілені за іншими компонентами системи.

Перший спосіб є більш гнучким, його механізми можна додавати і вилучати за потребою, але під час його реалізації можуть постати проблеми забезпечення сумісності засобів захисту між собою та з програмно-технічним комплексом ІС. Вмонтований захист вважається більш надійним і оптимальним, але є жорстким, оскільки в нього важко внести зміни. Таким доповненням характеристик способів захисту зумовлюється те, що в реальній системі їх комбінують.

Деякі науковці розглядають ще морально-етичні засоби. До цієї групи належать норми поведінки, які традиційно склались або складаються з поширенням ЕОМ, мереж і т. ін. Ці норми здебільшого не є обов'язковими і не затверджені в законодавчому порядку, але їх невиконання часто призводить до падіння авторитету та престижу людини, групи осіб, організації або країни.

Морально-етичні норми бувають як неписаними, так і оформленими в деякий статут. Найбільш характерним прикладом є Кодекс професійної поведінки членів Асоціації користувачів ЕОМ США.

Розглянемо більш детальніше принципи інформаційної безпеки та технічного захисту інформації організації.

Загальна мета інформаційної безпеки організації – впустити перевірених користувачів, але не допустити до системи несанкціонованих суб'єктів. Три основні принципи, що підтримують це правило, – конфіденційність, цілісність та доступність. Це називається тріадою ЦРУ або трьома стовпами всіх сучасних засобів захисту інформації.

Конфіденційність - це принцип, згідно з яким інформація має бути доступна лише тим, хто має відповідні повноваження на доступ до цих даних. Цілісність - це принцип, за яким інформація є послідовною, точною і заслуговує на довіру. Доступність говорить про те, що дані відкриті лише для тих, у кого є відповідні дозволи.

Ці три принципи не існують ізольовано та впливають одне на одного. Отже, будь-яка інформаційна система включатиме баланс цих факторів. Як приклад, інформація, доступна на папері, що знаходиться в сховищі, є конфіденційною, але отримати доступ до неї нелегко. Інформація, висічена на камені, що знаходиться у вестибюлі, має повну цілісність, але не є конфіденційною.

Технічний та організаційний захист даних – найважливіша сфера сучасних інформаційних технологій. Хоча перелічені три принципи становлять основу політики та орієнтир для прийняття рішень у сфері пошуку та усунення загрози інформаційній безпеці, існують також й інші фактори.

Оскільки сфера infosec включає баланс конкурентних факторів, вона пов'язана з управлінням ризиками. Мета цього процесу – максимізувати позитивні результати та мінімізувати негативні. Організації використовують принципи управління, щоб визначити рівень ризику, який вони готові взяти на себе під час впровадження системи. [42].

Класифікація інформації також має бути врахована для приділення особливої уваги даним, що залишаються або суворо конфіденційними, або доступними для всіх. Сфера infosec не обмежується цифровою інформацією чи комп'ютерними системами. Повна політика інформаційної безпеки також охоплює фізичні, друковані та інші види носіїв.

## Висновки до другого розділу

Інформаційна безпека – це стан захищеності інформаційного простору, що забезпечує формування та розвиток цього простору в інтересах особистості, суспільства та держави. Інформаційна безпека являє собою одне з найважливіших понять в науці і в різних сферах людської діяльності.

Провідними елементами системи інформаційної безпеки, у тому числі щодо захисту інформації в інформаційно-телекомунікаційних системах, є такі найважливіші чинники:

- провідний предмет суспільних правовідносин – інформація в інформаційно-телекомунікаційних системах;

- суб’єкти – окремі люди, їх спільноти, різного роду організації, суспільство, держава, інші держави, їх союзи, світове співтовариство.

- об’єкт – правовідносини між суб’єктами (суспільні відносини), які визначаються за певними об’єктивно існуючими критеріями.

До числа найбільш поширеного визначення поняття «інформаційна безпека підприємництва а організації» слід віднести: це суспільні відносини щодо створення та підтримання на належному (бажаному, можливому) рівні життєдіяльності відповідної інформаційної системи, у тому числі підприємництва та організації.

Система забезпечення інформаційної безпеки - це систему інформаційно-аналітичних, теоретико-методологічних, адміністративно-правових, організаційно-управлінських, спеціальних та інших заходів,

спрямованих на забезпечення стійкого розвитку об’єктів інформаційної безпеки, а також інфраструктури її забезпечення.

До методів та заходів, які вже сьогодні впроваджено в систему забезпечення інформаційної безпеки слід віднести організаційні, правові, технічні, програмні та криптографічні методи захисту інформації, комп’ютерів, комп’ютерних систем та мереж.

# ВИСНОВКИ

До інформаційних систем нового покоління належать системи підтримки прийняття рішень (СППР) та інформаційні системи, побудовані на штучному інтелекті (інтелектуальні автоматизовані системи).

1. Система підтримки прийняття рішень – це інтерактивна комп'ютерна система, яка призначена для підтримки різних видів діяльності при прийнятті рішень із слабоструктурованих або неструктурованих проблем. Інтерес до СППР, як перспективної галузі використання обчислювальної техніки та інструментарію підвищення ефективності праці в сфері управління економікою, постійно зростає.

Експертна система повинна мати можливість пояснити, чому запропоновано саме цей розв'язок і довести його обґрунтованість. Користувач повинен отримати всю інформацію, необхідну йому для того, аби переконатись в обґрунтованості запропонованого розв'язку. Експертна система - це програма, що поводиться подібно експерту в деякій, звичайно вузькій прикладній області. Типові застосування експертних систем містять у собі такі задачі, як медична діагностика, локалізація несправностей в устаткуванні й інтерпретація результатів вимірів.

При розробці експертної системи прийнято поділяти її на три основних модулі: база знань; машина логічного висновку; інтерфейс із користувачем. База знань містить знання, що відносяться до конкретної прикладної області, у тому числі окремі факти, правила, що описують чи відносини що описують чи відносини явища, а також, можливо, методи, евристики і різні ідеї, що відносяться до рішення задач у цій прикладній області. Машина логічного висновку вміє активно використовувати інформацію, що міститься в базі знань. Інтерфейс із користувачем відповідає за безперебійний обмін інформацією між користувачем і системою; він також дає користувачу можливість спостерігати за процесом рішення задач, що протікають у машині логічного висновку.

2. Системами підтримки прийняття рішень називають інтелектуальні системи, за допомогою яких особи, що приймають рішення (ОПР), мають змогу аналізувати ситуації, формулювати задачі, виробляти, контролювати й оцінювати варіанти рішень, які забезпечують досягнення поставленої мети. Згідно з таким узагальненим визначенням можна тлумачити СППР як одну з категорій управлінських інформаційних систем.

Для позначення певних типів СППР (іноді із суто маркетинговою метою) вживають багато специфічних термінів. Основні категорії систем підтримки прийняття рішень розглядають залежно від того, який із головних компонентів системи взято за домінуючий.

Системи підтримки прийняття рішень, зорієнтовані на дані, – це тип СППР, який зосереджується передусім на доступі й маніпуляції великими базами структурованих даних. До цієї категорії відносять: системи підготовки управлінських звітів; сховища даних; системи аналізу даних (ALOP); виконавчі інформаційні системи (інформаційна система керівника); географічні ІС;

Другу велику категорію становлять СППР, зорієнтовані на доступ та маніпуляцію моделями – статистичними, фінансовими, оптимізаційними і/або імітаційними. Здебільшого такі системи використовують дані й параметри, що їх надають ОПР, але, як правило, не потребують великих обсягів даних. Приклади таких СППР: засоби аналізу рішень, які допомагають ОПР розбити проблему на складові й структурувати її; засоби лінійного програмування; імітаційні засоби.

3. Інформаційна безпека – це стан захищеності інформаційного простору, що забезпечує формування та розвиток цього простору в інтересах особистості, суспільства та держави. Інформаційна безпека являє собою одне з найважливіших понять в науці і в різних сферах людської діяльності.

Провідними елементами системи інформаційної безпеки, у тому числі щодо захисту інформації в інформаційно-телекомунікаційних системах, є такі найважливіші чинники:

- провідний предмет суспільних правовідносин – інформація в інформаційно-телекомунікаційних системах;

- суб’єкти – окремі люди, їх спільноти, різного роду організації, суспільство, держава, інші держави, їх союзи, світове співтовариство.

- об’єкт – правовідносини між суб’єктами (суспільні відносини), які визначаються за певними об’єктивно існуючими критеріями.

До числа найбільш поширеного визначення поняття «інформаційна безпека підприємництва а організації» слід віднести: це суспільні відносини щодо створення та підтримання на належному (бажаному, можливому) рівні життєдіяльності відповідної інформаційної системи, у тому числі підприємництва та організації.

Загрози інформаційної безпеки в організації поділені за трьома ознаками: джерело загрози; об'єкт загрози; методи та засоби реалізації загрози.

4. Система забезпечення інформаційної безпеки - це систему інформаційно-аналітичних, теоретико-методологічних, адміністративно-правових, організаційно-управлінських, спеціальних та інших заходів, спрямованих на забезпечення стійкого розвитку об’єктів інформаційної безпеки, а також інфраструктури її забезпечення. До методів та заходів, які вже сьогодні впроваджено в систему забезпечення інформаційної безпеки слід віднести організаційні, правові, технічні, програмні та криптографічні методи захисту інформації, комп’ютерів, комп’ютерних систем та мереж.

# СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

## Нормативний матеріал:

1. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР. URL: http://zakon.rada.gov.ua/laws/show/80/94-вр

2. Закон України «Про інформацію» від 02.10.1992 № 2657-12. URL: http://zakon.rada.gov.ua/laws/show/2657-12

3. Закон України «Про Національну програму інформатизації» від 04.02.1998 № 74/98-ВР. URL: http://zakon.rada.gov.ua/laws/show/74/98-вр

4. Указ Президента України «Про рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України» від 27 січня 2016 р., № 96/2016. URL: http://zakon1.rada.gov.ua. – Назва з екрану

5. Указ Президента України «Про Національний координаційний центр кібербезпеки» від 07.06.2016 № 242/2016. URL: http://zakon1.rada.gov.ua.

6. Указ Президента України «Про Стратегію національної безпеки України» від 06.05.2015 № 287/2015. URL: http://zakon1.rada.gov.ua.

## Спеціальна література та періодичні видання

7. Адміністративне право України. Повний курс: підручник / за ред. В. Галунька. Видання третє. Київ: Академія адміністративно-правових наук, 2020. 466 с.

8. Андрійчук О.В. Метод визначення змістової подібності об'єктів баз знань експертних систем підтримки прийняття рішень: автореф. дис. . канд. техн. наук: 01.05.04 / О.В. Андрійчук; Нац. техн. ун-т України "Київ. політехн. ін-т". Київ, 2015. 20 с.

9. Арістова І.В. Державна інформаційна політика: організаційно-правові аспекти: Монографія / За загальною редакцією О.М. Бандурки. Харків: Ун-т внутрішніх справ, 2000. 368 с.

10. В Україні буде створена Національна система кібербезпеки. Режим доступу: http://zaxid.net/news

11. Великий тлумачний словник сучасної української мови /укл. О. Єрошенко. Донецьк : ТОВ «Глорія Трейд», 2012. 864 с.

12. Гавловський В.Д. Інформатизація управління соціальними системами: Організаційно-правові питання теорії і практики: навч. посіб. / В.Д. Гавловський, Р.А. Калюжний, В.С. Цимбалюк та ін. К.: МУАП, 2003. 336 с.

13. Голубєв В. О., Гавловський В. Д., Цимбалюк В. С. Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій. Монографія / За заг. ред. д-ра юрид. наук Калюжного Р. А. Запоріжжя: Просвіта, 2001.

14. Грохольський В.Л., Ісмайлов К.Ю., Форос Г.В. Науково-практичний коментар до Закону України «Про основні засади забезпечення кібербезпеки України» / за заг. ред. д. ю. н., проф. В. Л. Грохольського. Одеса. ОДУВС, 2020. 134 с.

15. Державне управління : підручник: у 2 т. /Нац. акад. держ. упр. при Президентові України ; ред. кол. : Ю. В. Ковбасюк (голова), К. О. Ващенко (заст. голови), Ю. П. Сурмін (заст. голови) [та ін.]. К. ; Дніпропетровськ : НАДУ, 2012. Т. 1. 564 с.

16. Державне управління: європейські стандарти, досвід та адміністративне право / Аверянов В.Б., Дерець В.А., Школик А.М. та ін.; За аг. Ред.. Аверянова В.Б. К.: Юстініан, 2007. 288 с.

17. Державне управління: підручник: у 2 т. /Нац. акад. держ. упр. при Президентові України ; ред. кол. : Ю. В. Ковбасюк (голова), К. О. Ващенко (заст. голови), Ю. П. Сурмін (заст. голови) [та ін.]. К. ; Дніпропетровськ : НАДУ, 2013. Т. 2. 324 с.

18. Інтелектуальні системи прийняття рішень та проблеми обчислювального інтелекту. зб. наук. пр. міжнар. наук. конф., 24 - 28 трав. 2016 р., Залізний Порт. - Херсон : Вишемирський В.С., 2016. - 381 с. - укр. - рус. - англ.

19. Інформатизація, право, управління (організаційно-правові питання): Монографія / Р.А. Калюжний, О.Д. Крупчан, В.Д. Гавловський та ін. - К., 2002.

20. Інформаційне забезпечення управлінської діяльності в умовах інформатизації: організаційно-правові питання теорії і практики. Монографія. К., 2002. 296 с.

21. Інформаційно-аналітичне забезпечення безпеки підприємництва (збір та пошук інформації): навч. посіб. Кн. 2 / під заг. ред. Є. В. Позднишева. К.: Видавець Позднишев, 2007. 74 с.

22. Ковтунець В. В. Безпека систем підтримки прийняття рішень: навч. посіб. / В. В. Ковтунець, О. В. Нестеренко, О. І. Савенков; Нац. акад. упр. Київ : Нац. акад. упр., 2016. 189 с.

23. Кормич Б.А. Інформаційне право: навчальний посібник. Х.: БУРУН і К, 2011. 334 с.

24. Кормич Б.А. Організаційно-правові засади політики інформаційної безпеки України: монографія. Одеса.: Юридична література, 2003. 471 с.

25. Ліпкан В.А. Правові засади розвитку інформаційного суспільства в Україні: монографія. За заг. ред. В. А. Ліпкана. К. : ФОП О. С. Ліпкан, 2015. 664 с.

26. Марущак А.І. Інформаційне право: регулювання інформаційної діяльності: навчальний посібник. К.: Дакор, 2011. 344 с.

27. Миронова Н.О. Методи та інформаційна технологія багатокритеріального колективного експертного оцінювання з використанням нечітких оцінок: автореф. дис. ... канд. техн. наук : 05.13.06 / Н. О. Миронова; Одес. нац. політехн. ун-т. Одеса, 2016. 24 с.

28. Основи інформаційного права України: навчальний посібник /В.С. Цимбалюк, В.Д. Гавловський, .В.М. Брижко. К.: Знання, 2009. 414 с.

29. Рада зробила перший крок до створення національної системи кібербезпеки. Режим доступу: http://espreso.tv/news/2016/09/20

30. Рудник Л. І. Право на доступ до інформації: дис… канд. юрид. наук: 12.00.07 / Національний університет біоресурсів і природокористування України. К., 2015. 247 с.

31. Рудь І. Закон про кібербезпеку: основні положення, оцінки експертів та розвиток вітчизняного інформаційного простору. Україна: події, факти, коментарі. 2017. № 19. С. 42–48. Режим доступу: http://nbuviap.gov.ua/images/ukraine/2017/ukr19.pdf.

32. Савенко Р.Г., Лисенко М.В. Інформаційні системи та технології в економіці Навчальний посібник. Полтава: ПолтНТУ, 2013. 299 с.

33. Сороківська О. А. Інформаційна безпека підприємства: нові загрози та перспективи / О. А. Сороківська, В. Л. Гевко // Вісник Хмельницьк. нац. ун-ту. 2010. № 2. Т. 2. С. 32-35.

34. Ковтунець В.В., Нестеренко О.В., Савенков О.І. Безпека систем підтримки прийняття рішень: навч.посібник. К.: Національна академія управління, 2016. 190 с.

35. Танцюра М. Ю. Забезпечення ефективності системи інформаційного забезпечення підприємства (на прикладі туристичних підприємств АР Крим) : автореф. дис. на здобуття наук. ступеня канд. екон. наук : спец. 08.00.04 / М. Ю. Танцюра. Сімферополь, 2012. 21 с.

36. Україна у фокусі кібератак. Режим доступу: https://scienceukraine.in.ua/sciblogs/ukraina-v-fokusi-kiberatak

37. Україна у фокусі кібератак. Режим доступу: https://scienceukraine.in.ua/sciblogs/ukraina-v-fokusi-kiberatak

38. Хорошко В.О., Чередниченко В.С., Шелест М.Є. Основи інформаційної безпеки / За ред. проф. В.О. Хорошка. К.: ДУІКТ, 2008. 186 с.

39. Цимбалюк В. Інформаційна безпека підприємницької діяльності: визначення сутності та змісту поняття за умов входження України до інформаційного суспільства (глобальної кіберцивілізації) / В. Цимбалюк // Підприємництво, господарство і право. 2004. № 3. С. 88-91.

40. Цимбалюк В.С. Основи інформаційного права України: Навч. посіб. / В.С. Цимбалюк, В.Д. Гавловський, В.В. Гриценко та ін. За ред. М.Я. Швеця, Р.А. Калюжного та П.В. Мельника. К.: Знання, 2004. 274 с.

41. Черноног О. О. Напрями підвищення ефективності забезпечення кібербезпеки інформаційних технологій в системі публічного управління. Режим доступу: mino.esrae.ua

42. Шеломенцев В. П. Сутність організаційного забезпечення системи кібернетичної безпеки України та напрями його удосконалення // Боротьба з організованою злочинністю і корупцією (теорія і практика). Київ: Міжвідом. наук.-дослід. центр з проблеми боротьби з організ. злочинністю, 2012. № 2 (28). С.299-309

43. Що таке безпека інформаційних систем (infosec)? - визначення з техопедії - Безпека - 2022. https://uk.theastrologypage.com/information-systems-security

44. Яременко О. Державне управління інформаційною сферою в Україні: структурно-функціональний аспект // Правова інформатика. 2008. №2. С.18.