«ЗАТВЕРДЖУЮ»
Завідувач кафедрою інформатики, кінезіології та кіберспорту
_____І.П. Заневський
(підпис,ініціали,прізвище)
_____20_____р

ЛЕКЦІЯ №1
з навчальної дисципліни

«КОМП'ЮТЕРНІ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ»
(найменування навчальної дисципліни)

КОМП'ЮТЕРНІ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТНЬОМУ ПРОЦЕСІ. СУЧАСНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ. РІШЕННЯ ПРОБЛЕМ СИСТЕМНОЇ ТА МЕРЕЖЕВОЇ БЕЗПЕКИ.
(повне найменування теми лекції)

Навчальний потік

для магістрів факультету педагогічної освіти, хореографія
(курс, напрям підготовки, спеціальність та спеціалізація)

Навчальна мета: Ознайомити студентів з методологією дисципліни і шляхами застосування новітніх інформаційних технологій в освітньому процесі, галузі ФКіС та культури і мистецтва, а також із законодавчою підтримкою питань захисту інформації.

Виховна мета: Практично застосовувати одержані знання під час виконання завдань спортивно-виховного характеру. Розширювати кругозір з інформатики, зацікавити комп'ютерною технікою, а також формувати систематизовані знання з комп'ютерних та інформаційних технологій.

Навчальні питання і розподілення часу:

Вступ _____ – - 10 хв.
1. Сутність інформації, інформаційних технологій в освітньому процесі, та їх класифікація – 10 хв.
2. Тенденції розвитку апаратного та програмного забезпечення -5 хв.
3. Конвергенція інформаційних і телекомунікаційних технологій – 10хв.
4. Хмарні технології. Системи штучного інтелекту – 10 хв.
5. Нейронні мережі - 5хв.
6. Види загроз безпеці інформації в комп'ютерних системах -5хв.
7. Сучасні програмні засоби захисту інформації, алгоритми криптографії, засоби ідентифікації і аутентифікації користувачів -10 хв.
8. Законодавча підтримка питань захисту інформації -10 хв.
9. Використання комп'ютерної техніки у освіті, фізичній культурі та спорті - 10хв.

Заключення та відповіді на запитання _____– 5хв.

Навчально-матеріальне забезпечення

Мультимедійний проектор_____
(наочні посібники,демонстрації,технічні засоби навчання і контролю знань, кінофрагменти,дидактичні,довідкові та інші навчальні матеріали)

Рекомендована література:

Основна:

1. Бакушевич Я.М., Капаціла Ю.Б. Інформатика та комп'ютерна техніка. -К.: Магнолія 2006, 2024.
2. Буйницька О. Інформаційні технології та технічні засоби навчання. Навч. посіб. -К: цент навч. літ-ри, 2019.
3. Качан О.В. Упровадження інноваційних технологій у фізкультурнооздоровчу та спортивну діяльність закладів освіти: навчально-методичний посібник Слов'янськ: Витоки, 2022.

4. Пасічник В.В., Пасічник О.В., Басюк Т.М., Думанський Н.О. Основи інформаційних технологій. Навч. посіб. -К: цент навч. лі-ри, 2020.
5. Windows 2010: навчальний посібник / Укладач: Дячук С. Ф. – Тернопіль: Вид-во ТНТУ імені Івана Пулюя, 2021.
6. Годлевський Л.С., Баязітов М.Р. Мандель О.В., Марченко С.В., Біднюк К.А., Ляшенко А.В. Телемедичні технології в системі охорони здоров'я Навчально-методичний посібник. ОНМедУ, Одеса- 2021.
7. Антомонов М.Ю. Математична обробка та аналіз медико-біологічних даних. 2-е видання-Київ: МЦ «Медінформ», 2018
8. Шинкарук О. А. Інноваційні та інформаційні технології у фізичній культурі, спорті, фізичній терапії та ерготерапії. – 2018.
9. О. Л. Тоцька. Сучасні інформаційні технології в професійній діяльності: лабор. практикум – Луцьк: Вежа-Друк, 2020.
10. Основи інформаційних технологій: навч. посібник для здобувачів професійної освіти / А. М. Гуржій, Л. І. Возненко, Н. І. Поворознюк, В. В. Самсонов. — Київ: Літера ЛТД, 2023.
11. Мирошниченко В.О. Використання сучасних інформаційних технологій: формування мультимедійної компетентності. Навч. посіб. -К: цент навч. лі-ри, 2020.
12. С. Е. Остапов, С. П. Євсеєв, О.Г. Король Кібербезпека: сучасні технології захисту. Навч. посіб. – Львів: «Новий Світ- 2000», 2020.
13. Речич Н. В. Інформатика: вебтехнології — Харків:/ Вид-во «Ранок», 2020.

Допоміжна:

1. Ільків О.С. Матвіїв В.І. Інформатика та комп'ютерна техніка (з елементами математичної статистики): Навч. посіб. –Львів: ЛДУФК, 2010.
2. Заневський І. П., Заневська Л. Г. Комп'ютерні та інформаційні технології в активній рекреації й спортивно-оздоровчому туризмі: навч. посіб. для магістрів фіз. виховання. – Л: ЛДУФК, 2010.
3. Є В. Павлиш, Л. Гліненко, Н. Шаховська Основи інформаційних технологій і систем- Львів: Львівська політехніка, 2018.
4. Сусіденко В. Інформаційні системи і технології в обліку. Навч. посіб. –К.: центр навч. лі-ри, 2019.
5. Сорока П.М., Харченко В.В., Харченко Г.А. Інформаційні системи і технології в управлінні організацією: Навч. посіб. – К.: ЦП «Компринт», 2019.
6. Антомонов М.Ю. Математична обробка та аналіз медико-біологічних даних. 2-е видання-Київ: МЦ «Медінформ», 2018.
7. Microsoft Access 2016: навчальний посібник в електронному вигляді / Укладачі В.О. Нелюбов, Ю.Ю. Білак. – Ужгород: ДВНЗ «УжНУ», 2019.
8. Нелюбов В. О., Куруца О. С. Основи інформатики. Microsoft Excel 2016: навчальний посібник. – Ужгород: ДВНЗ «УжНУ», 2018.
9. Нелюбов В. О., Куруца О. С. Основи інформатики. Microsoft Word 2016: навч. посіб. в ел. вигляді/ В. О. Нелюбов, О. С. Куруца // Ужгор. нац. ун-т, Центр інформ. техн. – Ужгород: ДВНЗ «УжНУ», 2018.

Інформаційні ресурси

1. https://www.kmu.gov.ua - Кабінет Міністрів України- ПРАВИЛА забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах
2. http://www.nbuv.gov.ua – Національна бібліотека України ім. В.І. Вернадського.
3. Закон України «Про доступ до публічної інформації» (2022). Вилучено з https://ips.ligazakon.net/document/T112939
4. https://vseosvita.ua/.../osnovni-polozenna-statisticnih-doslidz...- Основні положення статистичних досліджень у спорті.
5. http://inmeds.com.ua – веб-ресурс «Єдиний медичний простір»;
6. https://uk.wikipedia.org/wiki/ Список_нормативних_документів_щодо_інформаційної_безпеки_в_Україні
7. Главацька О. Л. Перспективи використання мультимедійних демонстрацій, створених засобами FLASH [Електронний ресурс] / О. Л. Главацька, І. М. Грод // Наукові записки Тернопільського національного педагогічного університету імені Володимира Гнатюка. Серія : Педагогіка. - 2022. - No 1. - С. 25-31. - Режимдоступу: http://nbuv.gov.ua/UJRN/NZTNPU_ped_2022_1_5
8. Задерейко О. В. Комп'ютерні мережі : навчально-методичний посібник [Електронне видання] / О. В. Задерейко, Багнюк Н.В., А. А. Толокнов. – Одеса : Фенікс, 2023. – 210 с. – URL: http://hdl.handle.net/11300/25951
9. Кирилова О. С. Мистецтво мультимедіа у підготовці фахівців спеціалізованої освіти [Електронний ресурс] / О. С. Кирилова // Освіта та розвиток обдарованої особистості. - 2022. - No 1. - С. 77-82. - Режим доступу:http://nbuv.gov.ua/UJRN/Otros_2022_1_13
10. Лучко Ю. І. Використання хмарних технологій навчання у професійній підготовці в закладах вищої освіти [Електронний ресурс] / Ю. І. Лучко // Вісник Луганського національного університету імені Тараса Шевченка. Педагогічні науки. - 2022. - No 3. - С. 274-282. - Режим доступу: http://nbuv.gov.ua/UJRN/vlup_2022_3_27

11. Крупа А. Технологія чат-бот як чинник комп'ютерно-посередницької комунікації цифрового суспільства [Електронний ресурс] / А. Крупа // Humanities studies. - 2022. - Вип. 12. - С. 130-141. - Режим доступу:http://nbuv.gov.ua/UJRN/humst_2022_12_17

Лекцію розробила : к.п.н., доц. О.С.Ільків
Обговорено на засіданні кафедри:інформатики, кінезіології та кіберспорту

1. Сутність інформації, інформаційних технологій та їх класифікація

Процеси світової глобалізації охопили практично усі сфери людської діяльності: економіку,осіту, культуру, медицину, інформаційний простір, технології та управління і багато інших. Це дало змогу говорити про розвиток відкритого інформаційного суспільства. Йому притаманний мережевий спосіб взаємодії між людьми в усіх напрямках їх діяльності. Результатом цього процесу стало, наприклад, створення віртуальних компаній, працівники яких можуть знаходитися в різних куточках світу і вести спільний бізнес за допомогою «віртуального офісу», поява засобів масової інформації нового типу, розвиток електронної комерції, виникнення «персоніфікованої реклами», поліпшення соціальної адаптації інвалідів, за рахунок можливості працювати, не виходячи з власної домівки, та багато іншого. Щоб скористатися результатами, які надає відкрите інформаційне суспільство, необхідно бути членом інформаційної мережі, мати відповідну інфраструктуру і сучасні засоби комунікації. Користувачі мережі повинні бути обізнаними в цій сфері, яка для більшості непрофесіоналів є новою. Наведені фактори, поряд з певною психологічною інертністю, є стримуючими для багатьох практичних працівників і навіть для значної частини науковців і освітян на шляху приєднання до очевидних досягнень світової цивілізації.

2. СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТІ, ТЕНДЕНЦІЇ РОЗВИТКУ

З розвитком інформаційних технологій зростає їх роль та використання у сфері освіти. Світовим трендом у сфері освіти стають відкриті онлайн-курси MOOCs і медіа-освіта.

З 2010 року в Україні набула чинності Концепція впровадження медіаосвіти в Україні, що має на меті «сприяння розбудові в Україні ефективної системи медіа-освіти заради забезпечення всебічної підготовки дітей і молоді до безпечної та ефективної взаємодії із сучасною системою медіа, формування у них медіа-обізнаності, медіа-грамотності і медіа-компетентності відповідно до їхніх вікових та індивідуальних особливостей». Онлайн-курси стали сьогодні дуже популярним засобом навчання. Така форма навчання дає змогу інтерактивного спілкування студентів та викладачів, а також прийому іспитів в режимі онлайн. Це одна із найновіших форм дистанційного навчання, яка активно розвивається у світовій освіті.

Використання в освітній практиці технологій, пов’язаних з Інтернетом, дозволяє реалізувати принцип безперервної освіти – «навчання впродовж усього життя», перейти від догматичного заучування до діяльнісного та компетентного підходу - підготовки

фахівців, здатних в умовах сучасного виробництва вирішувати наявні проблеми в нетривіальних умовах. Інформаційно-комунікаційні технології мають великі можливості для особистісного розвитку людини, розкриття її потенціалу, тому на сучасному етапі значну роль відіграють дистанційні форми та технології навчання й виховання. Сьогодні без широкого застосування дистанційного навчання навчальні заклади не можуть перемагати в конкурентній боротьбі на ринку освітніх послуг та забезпечувати підготовку кваліфікованих фахівців на сучасному рівні.

Весною 2014 року стартував проект інтерактивної онлайн-освіти EdEra, − який створює онлайн-курси та освітній контент широкого спектра з використанням IT. Мета проекту зробити освіту в країні доступною та якісною на зразок західних найкращих освітніх ініціатив.

Звичайно таке он-лайн навчання має як переваги так і певні недоліки.

До переваг ми відносимо:

− доступ до програм найкращих університетів і викладачів світу;
− найновіша інформація, технології, теорії;
− безкоштовне або доступніше за ціною, ніж денне навчанням в університеті;
− можливість навчатись будь-де і будь-коли.

Але сучасний студент зіштовхується і з труднощами у самомотивації, і з недостатньою кількістю спеціалізованих матеріалів вищого рівня складності (більшість матеріалів вступного рівня − для того, щоб охопити якомога більшу аудиторію). Ще одним недоліком онлайн навчання - ілюзія компетенції, тобто важко оцінити знання чи їх відсутність.

Отже, дистанційна форма навчання це сучасна платформа для отримання знань. І хоча Україна значно відстає від країн зарубіжжя з питань дистанційної освіти, але ми вже бачимо перші кроки які вітчизняна освіта робить у даному напрямі.

Найчастіше для проведення онлайн-уроків викладачі використовують Skype, проте існує безліч інших платформ, які нічим не гірше, а іноді і краще Скайпу. Наприклад - **платформа Zoom**. Zoom - сервіс для проведення відеоконференцій, онлайн-зустрічей і дистанційного навчання школярів.

Zoom Video Communications - компанія зі штаб-квартирою в Сан-Хосе, Каліфорнія, яка надає послуги віддаленої конференц-зв'язку з використанням хмарних обчислень. Zoom пропонує комунікаційне програмне забезпечення, яке об'єднує відеоконференції, онлайн-зустрічі, чат і мобільний спільну роботу.

Засновник: Ерік Юань
Дата заснування: 21 квітня 2011 р
Генеральний директор: Ерік Юань (2011 р.-)
Штаб-квартира: Сан-Хосе, Каліфорнія, США

Організувати зустріч може будь-хто, який створив обліковий запис. Безкоштовний обліковий запис дозволяє проводити відеоконференцію тривалістю 40 хвилин. Вартість платного тарифу з необмеженою тривалістю конференцій всіх розмірів і з кількістю учасників до 100 чоловік - $ 14.99 в місяць. Є тарифні плани і з іншими умовами (бізнес, підприємства), але вартість у них набагато вище.

Переваги:

+ Відмінний зв'язок.

+ Відео та аудіо зв'язок з кожним учасником. У організатора є можливість вимикати і включати мікрофон, а також вимикати відео та запитувати включення відео у всіх учасників. Можна увійти в конференцію як учасник з правами тільки для перегляду.

+ Можна ділитися екраном (screensharing) вже зі звуком. Демонстрацію екрану можна поставити на паузу. Більше того, можна ділиться не всім екраном, а тільки окремими додатками, наприклад, включити демонстрацію браузера. В налаштуваннях можна дати всім учасникам можливість ділитися екранам, або включити обмеження, щоб робити це міг тільки організатор.

+ В платформу вбудована інтерактивна дошка, можна легко і швидко переходити з демонстрації екрану на дошку.

+ Є чат, в якому можна писати повідомлення, передавати файли усім або вибрати одного студента. Чат можна налаштувати на автоматичне збереження або зберігати вручну при кожній конференції (Чат → Детальніше → Зберегти чат).

+ Можна проводити запис уроку як на комп'ютер, так і на хмару. Зручно, що можна налаштувати авто включення запису, а також ставити його на паузу.

+ Під час конференції можна призначити спів-організатора, у якого будуть такі ж можливості як і у організатора: включати і вимикати мікрофон у окремих студентів, перейменовувати і ділити на кімнати.

Інформаційна система (ІС) — це сукупність інформації, методів, програмно-технічних засобів і спеціалістів, які працюють над обробкою даних та прийняттям рішень. Передусім ІС передбачає використання комп’ютерних та інформаційних технологій. Розглянемо суть інформації та інформаційних технологій.

Інформація — це відомості про властивості об'єкта будь-якої природи, які представлені в документах та на машинних носіях. Як предмет праці, інформація є об'єктом збору, реєстрації, обробки, зберігання та передачі.

Інформаційні технології - основа створення та функціонування інформаційних систем. Поняття "технологія" походить від грецького ТЕХНО - ремесло, майстерність і ЛОГОС — вчення, наука. З цього погляду поняття "інформаційні технології" (ІТ) — це сукупність прийомів, методів та засобів послідовного якісного перетворення інформації на таких етапах інформаційних процесів, як: збір, передача, зберігання, обробка, накопичення. **Комп'ютерні інформаційні технології —** це ІТ, які реалізуються на базі персональних комп'ютерів з використанням такого сучасного пакету програм, як "Microsoft Offise 2007" або "Microsoft Office XP" в середовищі Windows 98, Mileninum, 2000 Prof., XP). Впровадження

сучасних офісних ІТ змінює технологію управління, звільняє користувачів від трудомістких процедур обробки інформації, значно підвищує оперативність прийняття рішень, поліпшує комфортність праці.

Наукові інновації охоплюють всі області людських знань. Нагадаємо, що джерелами виникнення інновацій є: зміна потреб виробничого процесу; зміни в структурі галузі або ринку; демографічні зміни; зміни в сприйнятті і в ціннісних установках; нові наукові знання.

3. Конвергенція – це зближення і взаємопроникнення наук і технологій, при цьому кордони між ними стираються, а нові результати виникають на стику областей. Такий науково-технологічний уклад базується на так званих НБІК-технологіях (Н – нано, Б – біо, І – інфо, К – когні).

Пріоритет підтримки інформаційних технологій в освіті очевидний, це визначається рядом факторів. По-перше, впровадження ІКТ в освіту істотно прискорює передачу знань і накопиченого технологічного і соціального досвіду. По-друге, сучасні ІКТ, підвищуючи якість навчання і освіти, дозволяють людині успішніше і швидше адаптуватися до навколишнього середовища і соціальних змін. По-третє, активне і ефективне впровадження ІКТ в освіту є важливим фактором реформування та модернізації системи освіти.

І.Звукозапис у навчальному процесі. Звукова наочність дозволила суттєво посилити смислове навантаження, передати емоційне забарвлення, розвивати слухову пам'ять, формувати навички спостереження за мовленням викладача. Так, у практиці використовувалися комплекти, що складалися з аудіозаписів, макетів, паперових альбомів рисунків (схем, діаграм). Це дозволило фактично реалізовувати методичні посібники (приклад, на голові учня – навушники, а на столі перед очима – альбом).

ІІ. Кіно в навчальному процесі. У 30-х роках XX ст. почали з'являтися перші цілісні фільми, призначені спеціально для навчальних цілей. З'явилася можливість об'єднати зображення і звук, розкрити динаміку різних явищ, актуалізувалося питання про створення науково-методичних фільмів. До дидактичних особливостей кіно слід віднести:

1) емоційну сторону сприйняття;

2) цілеспрямовану форму викладання змісту;

3) можливість абстрагування;

4) можливість показу громадського, фізичного, хімічного або технічного явища в динаміці;

5) можливість показу явища в уповільненому або прискореному темпі;

6) організацію уваги;

7) наукову документальність і достовірність.

III. Навчальне телебачення. Перші телепередачі для студентів проводилися відповідно до постанови Ради Міністрів СРСР від 9 квітня 1964 «Про подальше поліпшення вищої і середньої спеціальної заочної та вечірньої освіти». У розвитку систем навчального телебачення визначають три основні напрями – лекційне, довідково-інформаційне, демонстраційне.

IV. Конвергенція інформаційних і комунікаційних технологій. Основними тенденціями системи освіти є: підвищення якості освіти шляхом її фундаменталізації; інформування студентів про сучасні досягнення науки в більшому обсязі і з більшою швидкістю; забезпечення націленості навчання на нові технології і методики навчання; забезпечення більшої доступності освіти для всіх верств населення; підвищення творчого компоненту освіти.

Після розробки World Wide Web і гіпертекстової системи наступним етапом стала конвергенція телекомунікаційних мереж. Здійснювалася інтеграція різних інформаційних середовищ, розроблювалися загальні інтерфейси та універсальні протоколи. Внаслідок еволюційного процесу конвергенції інформаційних і телекомунікаційних технологій відбувалася інтеграція мережних інфраструктур, в результаті чого неперервно формувалися умови для широкого впровадження у навчальний процес мережних технологій «електронного навчання» і розширення спектру форматів представлення навчальної інформації. Розвиток веб-технологій дозволив використовувати соціальні мережі, вибудовувати комунікаційне середовище людини – персональне (індивідуальне) навчальне середовище PLE (Personal Learning Environment). Студент став активним елементом системи, яка не тільки контролює та спрямовує його діяльність, але і дозволяє впливати на функціонування і наповнення самої системи. Реалізуються нові педагогічні ідеї та теорії навчальної діяльності (наприклад, коннективізм, пар агогіка таін.). З 2008 року широку практику набувають масові відкриті дистанційні курси MOOC (Massive Open On-line Course). За підтримки провідних університетів світу було розроблено платформи edX, Udacity, Coursera, FutureLearn та ін.

Таким чином, **процес конвергенції інформаційних технологій** сприяє розвитку відкритої освіти, важливим елементом якої є можливість вибору засобів, місця і часу навчання, типу комунікацій відповідно до потреб. «Сучасні ІКТ для підтримки масового неперервного навчання – це інтеграція класичної науки і наукового передбачення, інновацій та практики, каталізатором виступає педагогічна майстерність викладача, його досвід, уміння узагальнювати, примножувати і дивитися в майбутнє».

4. У 2017 році в сферу великих даних активно включилася технологія blockchain. Це змінить системи обліку контрактів, підходи до реалізації бізнесу та захисту банківської

та іншої супутньої ділової інформації. Окремо слід зазначити зростаючу важливість систем автоматичного самообслуговування. Це дасть змогу аналізувати зібрані дані про користувачів без залучення додаткових фахівців: комп'ютерні алгоритми справлятимуться із обробкою краще за відділ аналітиків. Особливо важливою буде ця зміна для сегмента малих та середніх підприємців, у яких немає бюджету для того, аби винайняти вчених-аналітиків.

Час працювати в «хмарах»

Хмарні технології спростять моделювання та обробку наборів даних. Як зазначає у аналітичній доповіді Magic Quadrant компанія Gartner Inc.: «Очікування зараз найбільші стосовно cloud-сервісів як альтернативного варіанту розгортання аналітичних систем. Завдяки їхній гнучкості, маневреності та оперативності у ціноутворенні за такі послуги.»

Тепер не лише топ-менеджери розуміють потребу працювати із хмарними платформами, але й представники середньої управлінської ланки. Тому і самі компанії працюють над розширенням можливостей співробітників самостійно опрацьовувати великі дані через хмарні сервіси. З іншого боку — зберігається низка ризиків та пересторог з боку топ-менеджменту компаній. Тому робота із big data через «хмари» — це «палиця, що б'є в обидва боки».

У 2016 році можна було спостерігати справжній «бум» серед великих брендів щодо виходу на ринок подібних рішень для дому та офісу. У 2017 році бачили перемоги одних виробників та відходу інших «на узбіччя». Зі скороченням розмаїття рішень варто чекати на регулювання і стандартизацію. Це буде на користь споживачам, для яких з'являться універсальніші рішення та захищеніші технології. Як тут не згадати про кібератаки на електронні мережі в Україні чи спроби зламу систем розумного контролю за електростанціями у 2016 році. Окремим сегментом ризиків та небезпек залишаються спроби хакерів отримати доступ до систем інтелектуального керування та автопілотів у автомобілях відомих брендів.

Академічні визначення штучного інтелекту містять згадку про здатність машини імітувати інтелектуальну поведінку людини. У 2016 році ми побачили, як голосовий помічник Alexa від Amazon здатен нарешті порозумітися із користувачами, які говорять не завченими командами, а звичайною мовою. Успіх цієї розробки говорить сам за себе. Вже понад 5 млн користувачів у світі включили Alexa та пристрої із підтримкою цього голосового помічника до складу своєї побутової техніки. Штучний інтелект нарешті став надбанням не науково-фантастичного кіно, а нашого із вами повсякдення.

Великі очікування щодо штучного інтелекту — у сфері охорони здоров'я. Число стартапів, котрі працюють над медиичними технологіями та використовують штучний

інтелект, із 20 проектів у 2012 році зросло до майже 70 компаній — у 2016-му. Не лише окремі команди працюють у цьому напрямку. У складі персоналу медичного гіганта Philips близько 60% дослідників, розробників та інженерів програмного забезпечення сьогодні працюють над інноваціями в галузі IT у медицині.

Штучний інтелект насамперед потрібен, щоби удосконалити інструменти та системи діагностики захворювань. Зміни у знімках та контрастних зображеннях, які пропускає людське око, може зауважити комп'ютер. Інтенсивна терапія, герантологія, боротьба із хронічними хворобами, превентивні обстеження, діагностика у людей похилого віку чи пацієнтів із груп ризику — такі ключові напрямки, над якими працюють медичні стартапи із штучним інтелектом.

Нещодавно об'єднана команда інженерів-програмістів, дизайнерів та інших фахівців створила і представила перше перевірене рішення для радіологів. При дистанційному моніторингу пацієнтів штучний інтелект може включити віртуальну допомогу для медсестер та діагнозів.

5. Вперше світ дізнався про машинне навчання та **нейронні мережі** завдяки Гугл. Саме цей сервіс пошуку вперше запровадив програму, яка була здатна запам'ятовувати, аналізувати та відтворювати інформацію. Тож, що таке нейрон?

Нейрон - закінчений елемент програмного коду, що формує нейронну сітку. Кожний нейрон сприймає вхідні дані, опрацьовує їх, та передає далі за допомогою синапсу. Говорячи більш зрозуміло, **нейрон** — це базова одиниця штучного інтелекту. **Нейронна мережа** — комп'ютерна реалізація мозку людини.

Нейронна мережа - математична модель, а також її програмне або апаратне втілення, побудована за принципом організації та функціонування біологічних нейронних мереж - мереж нервових клітин живого організму.

Для чого використовується нейронна мережа

Розвиток інтернету та процеси глобалізації сприяли тому, що з'явилося дуже багато інформації, опрацювати яку самотужки людина фізично не в змозі. Нейронні мережі знайшли застосування у:

- аналізі та класифікації даних за заданими параметрами;
- формуванні аналітичних прогнозів, керуючись вхідною інформацією;
- порівнянні та розпізнаванні ідентичних даних.

Останній пункт, наприклад, використовується в системах безпеки аеропортів. Виконується це шляхом фіксації обличчя людей, та порівняння їх із базою злочинців. Ще один приклад — функція Google по пошуку схожого зображення. Достатньо завантажити фото і система знайде усі схожі картинки.

Як виконуються обчислення

Існує декілька видів нейронного зв'язку. Найчастіше використовуються синапсоідальний та ReLU. В першому випадку нейронна мережа використовує дані в діапазоні від -1 до 1 (що фактично відповідає -100% до 100%). В другому вхідні дані передаються через значення 0 та inf (інформація любого характеру).

Для того, щоб пояснити, як проходить системний аналіз, краще підходить синапсоідальна функція, оскільки обмежений діапазон вхідної інформації дає більше наочності. Алгоритм обчислення:

- дані поступають на нейрон;
- обчислюється їх вага;
- результати обчислень передаються на наступний нейрон;
- процес повторюється.

Кількість обчислень задається шляхом встановлення кількості шарів. Сучасні нейронні мережі мають десятки, а іноді навіть сотні шарів обчислення. Книги з програмування містять приклади коду на Java, що свідчить про розвиток технології не тільки в сфері десктопних програм, а також і для мобільних платформ. Це свідчить про ефективність нейронних мереж.

Як проходить навчання

Як зрозуміло із попереднього розділу, вхідні дані для нейронної мережі слід привести до встановленого виду. Що це значить? Розглянемо наступний приклад: проаналізувати динаміку ринку акцій.

Ціни в даному випадку будуть значно більше від одиниці. Тому можна звести дані до різниці цін, яка буде виражена через проценти. На виході отримаємо діапазон значень від -1 до 1.

Описана послідовність дій називається нормалізацією вхідних даних. Це перший і основний крок перед початком машинного навчання. Система повинна отримувати інформацію у тому виді, який вона може обробити.

Наступний крок — отримання першого результату обчислень. У 99% випадків він буде відрізнятися від того, що мало бути насправді. Ця обставина пояснюється просто: мережа не має достатньо інформації для правильної аналітики (тобто релевантного розподілення ваги).

На цьому етапі створюється алгоритм навчання — тренувальний сет. Це набір операнд, які задають параметри обробки вхідних даних та допомагають нейронній мережі правильно оцінювати вагу. В залежності від складності задачі може використовуватися від 4 до декількох сотень формул.

Проходження циклу операнд назветься епохою. На момент створення нейронна мережа має епоху під номером 0. Після першого циклу навчання наступає епоха 1, і так далі. З кожним циклом навчання похибка обчислень зменшується. Коли цей показник не

перевищує декількох процентів, вважається, що мережа пройшла навчання і придатна для вирішення реальних задач.

Також слід відмітити що нейронні мережі та штучний інтелект — це хоча і схожі, але все ж таки різні терміни. Нейронні мережі мають модулярну систему, де обчислення виконуються на основі встановлених правил. Система вчиться аналізувати лише конкретні дані і підходить для вирішення однієї чітко сформованої задачі.

Добре розвинена та навчена нейронна мережа легко замінить штатного аналітика, але лише в межах одного діапазону даних. Штучний інтелект, говорячи максимально просто, це здатність комп'ютера самотужки створювати та навчати нейронні мережі.

Однією з перспективних галузей сучасної інформатики на сьогодні є нейроінформатика.

Нейроінформатика – це принципово новий підрозділ інформатики, що стосується аналізу та переробки інформації, базується на використанні моделей штучного нейрона та побудові на їх основі нейронних мереж.

Розвиток штучних нейронних мереж тісно пов'язаний з біологією. Штучний нейрон – це спрощена модель біологічного нейрона. Математично він представляє собою деяку нелінійну функцію (функцію активації) від одного аргументу, що є лінійною комбінацією вхідних сигналів. Зв'язки між нейронами, за аналогією зі зв'язками між природними нейронами, називаються синапсами.

Штучний нейрон має єдиний вихід, який інколи називають аксоном. Штучні нейрони об'єднують, утворюючи при цьому штучні нейронні мережі.

Важливою властивістю нейронних мереж - паралельна обробка інформації одночасно великою кількістю нейронів. Завдяки цьому досягається значне пришвидшення обробки інформації. Іншою не мнеш важливою особливістю нейронних мереж є здатність до навчання та узагальнення інформації. Таким чином досягається деяка схожість з роботою головного мозку людини.

Поняття штучного нейрона та штучної неронної мережі відносно нове. Вперше роботу штучних нейронів та представлення моделі нейронної мережі було описано у статті нейрофізіолога Уоррена Маккалоха та математика Вольтера Піттса у 1943 р. Стартовою точкою для розробки алгоритмів навчання нейронних мереж був принцип, розроблений Дональдом Хеббом і описаний у його книзі «Організація поведінки» в1949 р.

У 1950-ті – 1960-ті роки було здійснено спроби об'єднати на той час існуючі біологічні та фізіологічні підходи та створити перші нейронні мережі. В цей час з'являються перші програмні моделі нейронних мереж.

Проблемами нейронних мереж займалися такі зарубіжні науковці, як Джон фон Нейман, Марсіан Хофф, Френк Розенблатт та ін.

Серед сучасних вітчизняних науковців варто виділити Акулова П.В. та Станіслава Осовського. Так, зокрема, в сферу діяльності Акулова П.В. входять питання вирішення задач за допомогою нейронних мереж. Станіслав Осовський займається дослідженнями нейронних мереж у сфері обробки інформації.

Останнім часом спостерігається тенденція зростання інтересу до використання нейронних мереж для вирішення різних завдань і застосування їх в різних сферах людського життя.

З використанням нейронних мереж відкрилися можливості проведення обчислень в сферах, що до цього відносилися лише до сфери людського інтелекту. З'явилися можливості створення систем, які здатні вчитися, запам'ятовувати та аналізувати інформацію, що дуже нагадує розумові здібності людини.

Типовими задачами, що можуть бути вирішеними за допомогою нейронних мереж та нейрокомп'ютерів є: задача класифікації, автоматизація прогнозування, автоматизація процесу ухвалення рішень, управління, кодування і декодування інформації, розпізнавання образів та ін.

Нейронні мережі можуть використовуватися майже в усіх галузях і сферах діяльності людини: економіці, медицині, зв'язку і безпеці охоронних систем, обробці інформації.

Прикладом успішного застосування нейронних обчислень у галузі економіки, зокрема фінансовій сфері, є системи управління кредитними ризиками, що успішно застосовуються у деяких відомих банках США. Як відомо, для оцінки вірогідності завдання збитків від несвоєчасно повернених кредитів, банки, до видачі кредиту, проводять розрахунки по фінансовій надійності позичальника. Такі обчислення базуються на оцінці кредитної історії, динаміці розвитку компанії, стабільності її основних фінансових показників і багатьох інших чинників. Нейромережеві технології дають змогу ефективно провести зазначені розрахунки і точно встановити потенційних неплатників.

Іншими важливими сферами застосування нейронних обчислень в галузі економіки є прогноз ситуації на фондовому ринку, оцінка вартості нерухомості, прогнозування динаміки біржових курсів, оптимізація товарних і грошових потоків, автоматичне зчитування чеків і форм тощо.

У галузі медицини нейронні мережі використовуються переважно в діагностиці захворювань. Зокрема, прикладом систем діагностики є програмний пакет для кардіодіагностики, розроблений R Informati . Подібні системи успішно використовуються

у деяких госпіталях Англії для попередження інфаркту міокарда та інших серцево-судинних захворювань, що дає можливість знижувати їх рівень.

Нейромережеві технології застосовуються також і в діагностиці онкологічних захворювань. Вчені з університету Дюка (США) розробили нейронну систему для розпізнання злоякісні тканини, яка успішно застосовується для діагностики раку молочної залози.

Нейронні мережі мають практичне застосування у проектуванні і оптимізації мереж зв'язку. З їх допомогою успішно вирішується важливе завдання в сфері телекомунікацій – знаходження оптимального шляху трафіку між вузлами. Окрім управління маршрутизацією потоків, нейронні мережі використовуються для отримання ефективних рішень в сфері проектування нових телекомунікаційних мереж, а також для швидкого кодування та декодування даних, стиснення відеоінформації тощо.

У галузі безпеки і охоронних системах нейронні мережі необхідні для ідентифікації особи, розпізнавання голосу, осіб в натовпі, розпізнавання автомобільних номерів, аналіз аэро-космічних знімків, моніторингу інформаційних потоків, виявлення підробок.

У галузі обробки інформації нейронні мережі можуть застосовуватися для обробки чеків, розпізнавання підписів, відбитків пальців і голосу.

Розроблені італійською фірмою R Informati нейромережеві пакети серії FlexR d, використовуються для розпізнавання і автоматичного введення рукописних платіжних документів і податкових декларацій. У першому випадку вони застосовуються для розпізнавання не тільки кількості товарів і їх вартості, але також і формату документа. У разі податкових декларацій розпізнаються фіскальні коди і суми податків.

Отже, нейроінфоматикою та дослідженнями нейромереж у різних галузях займаються науковці з усього світу. За допомогою штучних нейронних мереж можна опрацьовувати, аналізувати та узагальнювати інформації, що аналогічно роботі головного мозку людини. Нейтронні мережі використовуються у економіці, медицині, зв'язку, безпеці та охоронних системах, введенні та обробці інформації. Безумовно, даний перелік не повний, проте він дозволяє отримати уявлення про характер застосування нейромережевих технологій.

6.1. Види загрози безпеці інформаційних систем

За метою впливу розрізняють **три основні типи** загроз безпеці інформаційних систем:

- загрози порушення конфіденційності інформації;
- загрози порушення цілісності інформації;
- загрози порушення працездатності системи (відмови в обслуговуванні).

Загрози порушення конфіденційності направлені на розголошення конфіденційної чи секретної інформації. При реалізації цих загроз інформація стає відомою особам, які не повинні мати до неї доступ.

Заг**рози порушення цілісності інформації**, що зберігається в комп'ютерній системі чи передається по каналу зв'язку, направлені на її зміну чи спотворення, що приводить до порушення її якості чи повного знищення. Цілісність інформації може бути порушена спеціально зловмисноком, а також в результаті впливу зовнішнього середовища, що оточує систему. Ця загроза є особливо актуальна для систем передачі інформації – комп'ютерних мереж та систем телекомунікацій.

Загрози порушення працездатності (відмова в обслуговуванні) направлені на створення таких ситуацій, коли певні навмисні дії або знижують працездатність ІС, або блокують доступ до її ресурсів. Наприклад, якщо один користувач системи робить спробу отримати доступ до деякої служби, а інший здійснює дії з блокування цього доступу, то перший користувач отримує відмову в обслуговуванні. Блокування доступу до ресурсу може бути постійним чи тимчасовим.

Порушення конфіденційності та цілісності інформації, а також доступності і цілісності певних ресурсів ІС можуть бути викликані різними небезпечними впливами на інформаційну систему. Сучасні автоматизовані системи обробки інформації представляють собою складну систему, що складається з великої кількості компонент різного ступеня автономності, які зв'язані між собою та обмінюються даними. Практично кожний компонент може піддаватися зовнішньому впливу чи вийти з ладу. Компоненти інформаційної системи можна розділити на такі групи:

- апаратні засоби;
- програмне забезпечення;
- дані;
- персонал

Небезпечні впливи на ІС можна поділити на **випадкові та навмисні.** Аналіз досвіду проектування, виготовлення та експлуатації інформаційних систем показує, що інформація піддається різним випадковим впливам на всіх етапах функціонування інформаційної системи. **Причинами випадкових впливів** можуть бути:

- аварійні ситуації, пов'язані зі стихійними лихами та відключеннями електричного живлення;
- відмови та збої апаратури;
- помилки в програмному забезпеченні;
- помилки в роботі обслуговуючого персоналу та користувачів;
- завади в лініях зв'язку, спричинені впливом зовнішнього середовища.

Навмисні загрози пов'язані з цілеспрямованими діями порушника. Порушником може бути співробітник, відвідувач, конкурент, найманець тощо. Дії порушника можуть бути зумовлені різними мотивами: невдоволенням співробітника своєю кар'єрою, матеріальною зацікавленістю, цікавістю, конкурентною боротьбою, прагненням самоствердження та ін. Виходячи з можливості виникнення найнебезпечнішої ситуації, зумовленої діями порушника, можна скласти гіпотетичну модель потенційного порушника:

- кваліфікація порушника може бути на рівні розробника даної системи;
- порушником може бути як стороння особа, так і законний користувач системи;
- порушнику відома інформація про принципи роботи системи;
- порушник вибирає найслабшу ланку в захисті.

Можна виділити такі приклади навмисних загроз:

- несанкціонований доступ сторонніх осіб, що не належать до числа співробітників, та ознайомлення з конфіденційною інформацією;
- ознайомлення співробітників з інформацією, до якої вони не повинні мати доступ;
- несанкціоноване копіювання програм і даних;
- викрадення носіїв інформації, що містять конфіденційну інформацію;
- викрадення роздрукованих документів;
- навмисне знищення інформації;
- несанкціонована модифікація співробітниками фінансових документів, звітності та баз даних;
- фальсифікація повідомлень, що передаються по каналах зв'язку;
- відмова від авторства повідомлення, переданого каналом зв'язку;
- відмова від факту отримання інформації;
- пошкодження інформації, викликане впливом вірусів;
- пошкодження архівної інформації, розміщеної на змінних носіях;
- викрадення обладнання.

Несанкціонований доступ є найбільш розповсюдженим та різностороннім видом комп'ютерних порушень. Суть несанкціонованого доступу полягає в отриманні користувачем (порушником) доступу до об'єкту з порушенням правил розмежування доступу, встановлених у відповідності до прийнятої в організації політики безпеки. Несанкціонований доступ використовує будь-яку помилку в системі захисту та можливий при нераціональному виборі засобів захисту, некоректному їх встановленні та настроюванні. Несанкціонований доступ може бути здійснений як штатними засобами ІС, так і спеціально створеними апаратними і програмними засобами.

Наведемо перелік основних каналів несанкціонованого доступу, через які зловмисник може отримати доступ до компонентів ІС та здійснити крадіжку, модифікацію і/або пошкодження інформації:

- усі штатні канали доступу до інформації (комп'ютери користувачів, оператора, адміністратора системи; засоби відображення та документування інформації; канали зв'язку) при їх використанні порушниками, а також законними користувачами за межами їх повноважень;
- технологічні пульти управління;
- лінії зв'язку між апаратними засобами ІС;
- побічні електромагнітні випромінювання від апаратури, ліній зв'язку, мереж електричного живлення, заземлення тощо.

Із всього розмаїття способів та прийомів несанкціонованого доступу зупинимося на найбільш розповсюджених та зв'язаних між собою порушеннях:

- перехоплення паролів;
- „маскарад";
- незаконне використання привілеїв.

Перехоплення паролів здійснюється спеціально розробленими програмами. При спробі законного користувача ввійти в систему програма-перехоплювач імітує на екрані введення логіну та паролю користувача, які пересилаються власнику програми-перехоплювача після чого на екран виводиться повідомлення про помилку і управління повертається операційній системі. Користувач вважає, що допустив помилку при введенні паролю. Він повторює введення і отримує доступ в систему. Власник програми-перехоплювача, отримавши логін та пароль законного власника, може тепер їх використовувати в своїх цілях. Існують й інші способи перехоплення паролів.

„***Маскарад"***– це виконання якихось дій одним користувачем від імені іншого, що має відповідні повноваження. Метою „маскараду"є приписування якихось дій іншому користувачу або присвоєння повноважень та привілеїв іншого користувача. Прикладами реалізації „маскараду"є:

- вхід в систему під іменем та паролем іншого користувача (такому „маскараду" передує перехоплення паролю);
- передача повідомлень в мережі від імені іншого користувача.

„Маскарад"є особливо небезпечним в банківських системах електронних платежів, де неправильна ідентифікація клієнта із-за „маскараду" зловмисника може привести до великих втрат законного клієнта банку.

Незаконне використання привілеїв. Більшість систем захисту встановлюють певні набори привілеїв для виконання заданих функцій. Кожний користувач отримує свій набір привілеїв: звичайні користувачі – мінімальний, адміністратори – максимальний. Несанкціоноване захоплення привілеїв, наприклад засобами „маскараду", приводить до

можливості виконання порушником певних дій в обхід системи захисту. Слід зазначити, що незаконне захоплення привілеїв можливе або за наявності помилок в системі захисту, або із-за халатності адміністратора при управлінні системою та призначенні привілеїв.

Окремо слід зупинитися на загрозах, яким можуть піддаватися комп'ютерні мережі. Основна особливість будь-якої комп'ютерної мережі полягає в тому, що її компоненти розподілені в просторі. При вторгненні в комп'ютерну мережу зловмисник може використовувати як **пасивні, так і активні методи** вторгнення. При ***пасивному вторгненні*** (перехопленні інформації) порушник тільки спостерігає за проходженням інформації по каналу зв'язку, не втручаючись ні в інформаційний потік, ні в зміст інформації.

При ***активному вторгненні*** порушник прагне підмінити інформацію, що передається в повідомленні. Він може вибірково модифікувати чи змінювати повідомлення, затримувати чи змінювати порядок слідування повідомлень. Зловмисник може також анулювати і затримувати усі повідомлення, що передаються по каналу. Такі дії можна кваліфікувати як відмову в передачі повідомлень.

Комп'ютерні мережі характерні тим, що крім звичайних локальних атак, які здійснюються в межах однієї системи, проти об'єктів мереж здійснюють так звані, ***віддалені атаки***. Зловмисник може перебувати за тисячі кілометрів від атакованого об'єкта, при цьому нападу може піддаватися не тільки конкретний комп'ютер, а й інформація, що передаються по мережним каналам зв'язку.

У табл. 6.1 показані основні шляхи реалізації загроз безпеці ІС при впливі на її компоненти. Ця таблиця дає тільки загальну картину того, що може відбутися з системою, а конкретні обставини та особливості повинні розглядатися окремо.

Таблиця 6.1.Шляхи реалізації загроз безпеці ІС

Об'єкти впливу	**Порушення конфіденційності інформації**	**Порушення цілісності інформації**	**Порушення працездатності системи**
Апаратні засоби	Несанкціонований доступ – підключення; використання ресурсів; викрадення носіїв	Несанкціонований доступ – підключення; використання ресурсів; модифікація, зміна режимів	Несанкціонований доступ – зміна режимів; виведення з ладу; пошкодження
Програмне забезпечення	Несанкціонований доступ – копіювання; викрадення; перехоплення	Несанкціонований доступ – впровадження „троянських коней", „вірусів", „черв'яків"	Несанкціонований доступ – спотворення; знищення; підміна
Дані	Несанкціонований доступ – копіювання; викрадення; перехоплення	Несанкціонований доступ – спотворення; модифікація	Несанкціонований доступ – спотворення; знищення; підміна
Персонал	Розголошення;	„Маскарад"; вербування;	Покидання робочого

	передача відомостей про захист; халатність	підкуп персоналу	місця; фізичне усунення

„***Троянський кінь“*** представляє собою програму, яка поряд з діями, описаними в її документації, виконує деякі інші дії, що ведуть до порушення безпеки системи та деструктивних результатів. Аналогія такої програми з давньогрецьким „троянським конем“ повністю виправдана, оскільки в обидвох випадках оболонка, що не викликає підозр, містить в собі серйозну загрозу. Термін „троянський кінь“ було вперше використано Даном Едвардсом, який пізніше став співробітником Агенства Національної Безпеки США. „Троянський кінь“ використовує обман для того, щоб змустити користувача запустити програму з прихованою загрозою всередині. Зазвичай для цього стверджується, що така програма виконує деякі корисні функції. Зокрема, такі програми маскуються під якісь корисні утиліти.

Небезпека „троянського коня“ полягає в додатковому блоці команд, вбудованому у вихідну корисну програму, яка потім надається користувачам. Цей блок команд може спрацьовувати при настанні якоїсь умови (дати, стану системи) або по команді ззовні. Користувач, який запустив таку програму, піддає небезпеці як свої ресурси, так і всю ІС в цілому. Наведемо для прикладу деякі деструктивні функції, що реалізуються „троянськими конями“ :

- ***знищення інформації***. Вибір об’єктів та способів знищення визначається фантазією та цілями автора зловмисної програми;
- ***перехоплення та передача інформації***. Зокрема, відомі програми, які здійснюють перехоплення паролів, що набираються на клавіатурі;
- ***цілеспрямована модифікація тексту програми***, яка реалізує функції безпеки та захисту системи.

Загалом, „троянські коні“ завдають збитки ІС шляхом викрадення інформації та явного пошкодження програмного забезпечення системи. „Троянський кінь“ є однією з найнебезпечніших загроз безпеці ІС. Радикальний спосіб захисту від цієї загрози полягає у створенні замкнутого середовища виконання програм, які повинні зберігатися і захищатися від несанкціонованого доступу. При цьому встановлення нового програмного забезпечення на комп’ютер повинно бути дозволено тільки адміністраторам, чого зазвичай складно досягти.

Комп’ютерні „віруси“ – це певний тип програмних об’єктів, які володіють рядом властивостей, притаманних живим організмам, – вони народжуються, розмножуються та помирають. Термін „вірус“ стосовно до комп’ютерів був запропонований Фредом Коеном із Університету Південної Каліфорнії. Історично перше визначення, дане Ф. Коеном звучало так: „***Комп’ютерний вірус*** – це програма, яка може заражати інші програми, змінюючи їх шляхом включення в них своєї, можливо, зміненої копії, причому остання

зберігає здатність до подальшого розмноження“. Ключовими поняттями у визначенні комп’ютерного вірусу є здатність вірусу до саморозмноження та модифікації коду заражених програм.

Мережний „черв’як“ – це різновид програми-вірусу, яка розповсюджується глобальною мережею і не залишає своєї копії на магнітному носії (хоча є й інші варіанти „черв’яків“, які зберігаються на фізичних носіях у вигляді файлів). Перші варіанти „черв’яків“ були розроблені для пошуку в мережі інших комп’ютерів з вільними ресурсами щоб забезпечувати можливість проведення розподілених обчислень. При правильному використанні технологія „черв’яків“ може бути надзвичайно корисною. Наприклад, „черв’як“ World Wide Web Worm формує індекс пошуку ділянок Web. Проте „черв’як“ легко перетворюється у шкідливу програму.

Мережні „черв’яки“є найнебезпечнішим видом зловмисних програм, оскільки об’єктом їх нападу може стати будь-який з величезної кількості комп’ютерів, підключених до глобальної мережі Інтернет, чи інших мереж. Для захисту від „черв’яка“ застосовують засоби, направлені на блокування несанкціонованого доступу до внутрішньої мережі.

Слід зазначити, що „троянські коні“, комп’ютерні віруси та мережні „черв’яки“ відносяться до найнебезпечніших загроз ІС. Для захисту від зловмисних програм необхідно застосовувати ряд заходів:

- виключення несанкціонованого доступу до виконуваних файлів;
- тестування нових програм;
- контроль цілісності виконуваних файлів та системних областей;
- створення замкнутого середовища виконання програм.

6.2. Забезпечення безпеки інформаційних систем

Основним призначенням інформаційної системи є збір, зберігання, обробка та видача інформації, у зв’язку з чим проблема забезпечення інформаційної безпеки є для ІС центральною. Забезпечення безпеки ІС передбачає організацію протидії будь-якому несанкціонованому вторгненню в процес функціонування ІС, а також спробам модифікації, викрадення, виведення з ладу чи знищення її компонентів, – захист усіх компонентів ІС – апаратних засобів, програмного забезпечення, даних та персоналу. Існує два підходи до проблеми забезпечення безпеки ІС: **фрагментарний та комплексний.**

Фрагментарний підхід направлений на протидію чітко визначеним загрозам у заданих умовах. Прикладами такого підходу є окремі засоби управління доступом, автономні засоби шифрування, спеціалізовані антивірусні програми тощо. Перевагою такого підходу є висока вибірковість до конкретної загрози. Суттєвим недоліком такого підходу є відсутність єдиного захищеного середовища обробки інформації. Фрагментарні

міри захисту інформації забезпечують захист конкретних об'єктів ІС тільки від конкретної загрози. Навіть невеликі видозміни загрози приводять до втрати ефективності захисту.

Комплексний підхід орієнтований на створення захищеного середовища обробки інформації в ІС, яке об'єднує в єдиний комплекс різноманітні заходи протидії загрозам. Організація захищеного середовища обробки інформації дозволяє гарантувати певний рівень безпеки ІС, що є неодмінною перевагою комплексного підходу. Основними недоліками цього підходу є: обмеження на свободу дій користувачів ІС, велика чутливість до помилок встановлення та настроювання засобів захисту, складність управління.

Комплексний підхід застосовують для захисту ІС великих організацій, та для невеликих ІС, що виконують відповідальні задачі чи обробляють особливо важливу інформацію. Порушення безпеки інформації в ІС великих організацій може принести великі збитки як самим організаціям, так і їх клієнтам. Тому такі організації вимушені надавати особливу увагу гарантіям безпеки та реалізовувати **комплексний захист**. Комплексного підходу притримуються більшість державних та крупних комерційних підприємств та закладів.

Під ***системою захисту*** ІС розуміють сукупність правових та морально-етичних норм, адміністративно-організаційних заходів, фізичних та програмно-технічних засобів, направлених на протидію загрозам ІС з метою зведення до мінімуму можливості нанесення збитків.

Процес побудови системи захисту включає такі етапи:

- аналіз можливих загроз ІС;
- планування системи захисту;
- реалізація системи захисту;
- супровід системи захисту.

Етап аналізу можливих загроз ІС необхідний для фіксації стану ІС (конфігурації апаратних і програмних засобів, технології обробки інформації) та визначення можливих впливів на компоненти системи. Практично неможливо забезпечити захист інформаційної системи від усіх впливів, оскільки неможливо повністю встановити (визначити) усі загрози та способи їх реалізації.

На ***етапі планування*** формулюється система захисту, як єдина сукупність заходів протидії загрозам різної природи. За способами реалізації усі міри забезпечення безпеки комп'ютерних систем поділяються на:

- правові (законодавчі);
- морально-етичні;
- адміністративні;
- фізичні;
- апаратно-програмні.

Перелічені заходи безпеки ІС можна розглядати як послідовність бар'єрів чи кордонів захисту інформації. Для того, щоб отримати доступ до захищеної інформації, потрібно послідовно подолати кілька кордонів захисту.

До ***правових мір*** захисту інформації відносяться діючі в країні закони, укази та інші нормативні акти, які регламентують правила використання інформації обмеженого використання та відповідальність за їх порушення. Цим вони перешкоджають несанкціонованому використанню інформації та є стримуючим фактором для потенційних порушників.

Другий кордон захисту утворюють ***морально-етичні засоби***. Етичний момент у дотриманні вимог захисту має дуже велике значення. Надзвичайно важливо, щоб особи, які мають доступ до комп'ютерів, працювали в здоровому морально-етичному кліматі. До морально-етичних засобів протидії відносяться різноманітні норми поведінки, які традиційно склалися чи складаються в суспільстві у зв'язку з розповсюдженням комп'ютерів у країні

Третім кордоном, який перешкоджає неправочинному використанню інформації, є **адміністративні заходи**. Адміністратори усіх рангів з врахуванням усіх правових норм та соціальних аспектів визначають адміністративні заходи захисту інформації. ***Адміністративні заходи*** захисту відносяться до заходів організаційного характеру. Вони регламентують:

- процеси функціонування ІС;
- використання ресурсів ІС;
- діяльність персоналу;
- порядок взаємодії користувачів із системою для того, щоб якомога сильніше ускладнити чи виключити можливість реалізації загроз безпеці.

Четвертим кордоном є ***фізичні засоби захисту***. До фізичних засобів захисту відносяться різноманітні механічні, електро- та електронно-механічні пристрої чи споруди, які спеціально призначені для створення фізичних перешкод на можливих шляхах проникнення та доступу потенційних порушників до компонентів системи та захищеної інформації.

П'ятим кордоном є ***апаратно-програмні засоби захисту***. До них відносяться різноманітні електронні пристрої та спеціальні програми, які реалізують самостійно чи в комплексі з іншими засобами наступні способи захисту:

- ідентифікацію (розпізнавання) та автентифікацію (перевірка справжності) суб'єктів (користувачів, процесів) ІС;
- розмежування доступу до ресурсів ІС;
- контроль цілісності даних;
- забезпечення конфіденційності даних;
- реєстрацію та аналіз подій, що відбуваються в ІС;
- резервування ресурсів та компонентів ІС.

Більшість з перелічених методів захисту реалізуються криптографічними методами захисту інформації.

7. 1 Апаратно-програмні засоби захисту комп'ютерної інформації

Перші операційні системи для персональних комп'ютерів не мали власних засобів захисту, що і породило проблему створення додаткових засобів захисту. Актуальність цієї проблеми практично не зменшилася з появою більш потужних ОС з розвинутими підсистемами захисту. Це обумовлено тим, що більшість систем не здатні захистити дані, які перебувають за її межами, наприклад при використанні мережного інформаційного обміну. Апаратно-програмні засоби, що забезпечують підвищений рівень захисту, можна розбити на п'ять основних груп, рис. 7.1.

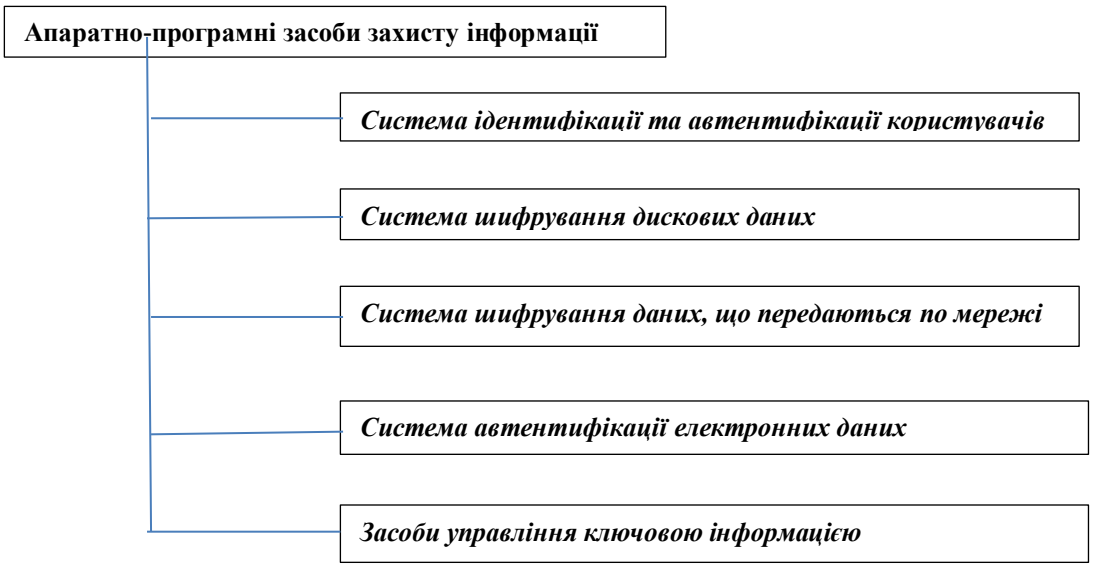

Рис. 7.1. Апаратно-програмні засоби захисту комп'ютерної інформації

Першу групу утворюють ***системи ідентифікації та автентифікації користувачів***. Такі системи застосовуються для обмеження доступу випадкових та незаконних користувачів до ресурсів комп'ютерної системи. Загальний алгоритм роботи цих систем полягає в тому, щоб отримати від користувача інформацію, яка посвідчує його особу, перевірити її справжність і потім надати (чи не надати) цьому користувачу можливість роботи з системою. При побудові подібних систем виникає проблема вибору інформації, на основі якої здійснюються процедури ідентифікації та автентифікації користувача. Можна виділити наступні типи:

1. секретна інформація, якою володіє користувач (пароль, персональний ідентифікатор, секретний ключ тощо); цю інформацію користувач повинен запам'ятати або ж можуть бути застосовані спеціальні засоби зберігання такої інформації;

2. фізіологічні параметри людини (відбитки пальців, рисунок райдужної оболонки ока) чи особливості поведінки людини (особливості роботи на клавіатурі – „клавіатурний почерк" тощо).

Системи ідентифікації, що базуються на першому типі інформації, прийнято вважати ***традиційними***. Системи ідентифікації, що використовують другий тип інформації, називають ***біометричними***. Слід відзначити тенденцію все більшого використання біометричних систем ідентифікації.

Другу групу засобів, що забезпечують підвищений рівень захисту, складають системи ***шифрування дискових даних***. Основна задача, що вирішується такими системами, полягає у захисті від несанкціонованого використання даних, розміщених на магнітних носіях інформації. Робота прикладних програм з дисковими накопичувачами складається з двох етапів – ***логічного*** та ***фізичного***.

Логічний етап відповідає рівню взаємодії прикладної програми з операційною системою (наприклад, виклик сервісних функцій читання/запису даних). На цьому рівні основним об'єктом є файл.

Фізичний етап відповідає рівню взаємодії операційної системи та апаратури. У якості об'єктів цього рівня виступають структури фізичної організації даних – сектори диску.

В результаті системи шифрування даних можуть здійснювати криптографічні перетворення даних на рівні файлів (захищаються окремі файли) та на рівні дисків (захищаються цілі диски).

Іншою класифікаційною ознакою систем шифрування дискових даних є спосіб їх функціонування. За способом функціонування системи шифрування дискових даних поділяються на два класи:

1. системи ***прозорого*** шифрування;
2. системи, які спеціально викликаються для здійснення шифрування.

У системах ***прозорого шифрування*** (шифрування „на льоту") криптографічні перетворення здійснюються в режимі реального часу непомітно для користувача. Наприклад, користувач записує підготовлений у текстовому редакторі документ на захищуваний диск, а система в процесі запису здійснює його шифрування. Системи другого класу зазвичай представляють собою утиліти, які необхідно спеціально викликати для виконання шифрування. До них відносяться, наприклад, архіватори з вбудованими засобами парольного захисту.

До третьої групи засобів, що забезпечують підвищений рівень захисту, відносяться ***системи шифрування даних, що передаються по комп'ютерних мережах***. Розрізняють два основних способи шифрування: ***канальне*** шифрування та ***кінцеве*** (абонентське, термінальне) шифрування.

У випадку ***канального шифрування*** захищається уся інформація, що передається по каналу зв'язку, включаючи і службову.

Кінцеве(***абонентське***) ***шифрування*** дозволяє забезпечити конфіденційність даних, що передаються між двома прикладними об'єктами (абонентами). Даний спосіб дозволяє уникнути проблем, пов'язаних із шифруванням службової інформації, але при цьому виникають інші проблеми. Зокрема, зловмисник, який має доступ до каналів зв'язку комп'ютерної мережі, отримує можливість аналізувати інформацію про структуру обміну повідомленнями, наприклад, про відправника і отримувача, про час і умови передачі даних, а також про об'єм даних, що передаються.

Четверту групу засобів захисту складають ***системи автентифікації електронних даних***. При обміні електронними даними по мережах зв'язку виникає проблема автентифікації автора документу та самого документу – встановлення справжності автора та перевірка відсутності змін в отриманому документі. Для автентифікації електронних даних застосовують ***код автентифікації повідомлення*** (***імітовставку***) чи ***електронний цифровий підпис***. При формуванні коду автентифікації повідомлення та електронного цифрового підпису використовують різні типи систем шифрування.

Код автентифікації повідомлення формують за допомогою симетричних систем шифрування даних.

Електронний цифровий підпис (ЕЦП) представляє собою відносно невеликий об'єм додаткової автентифікуючої цифрової інформації, що передається разом із „підписаними" даними. Для реалізації ЕЦП використовуються принципи асиметричного шифрування. Система ЕЦП включає процедуру формування цифрового підпису відправником з використанням секретного ключа відправника та процедуру перевірки підпису отримувачем з використанням відкритого ключа відправника.

П'яту групу засобів, що забезпечують підвищений рівень захисту, утворюють ***засоби управління ключовою інформацією***. Під ключовою інформацією тут розуміється сукупність усіх використовуваних в комп'ютерній системі чи мережі криптографічних ключів. Безпека будь-якого криптографічного алгоритму визначається використовуваними криптографічними ключами. У випадку ненадійного управління ключами зловмисник може заволодіти ключовою інформацією та отримати повний доступ до всієї інформації в комп'ютерній системі чи мережі.

7. 2Принципи криптографічного захисту інформації

Криптографія - це сукупність методів перетворення даних, направлених на те, щоб зробити ці дані незрозумілими для усіх крім респондента, якому адресуються дані.

Такі перетворення дозволяють розв'язати дві головні проблеми захисту даних: ***проблему конфіденційності*** (шляхом усунення можливості отримання корисної інформації з каналу зв'язку) та ***проблему цілісності*** (шляхом усунення можливості змінювати повідомлення противником). Проблеми конфіденційності та цілісності інформації тісно зв'язані між собою, у зв'язку з чим методи розв'язання однієї з них часто можна застосовувати для розв'язання іншої.

Узагальнена схема криптографічної системи, що забезпечує шифрування інформації при її передачі по каналах зв'язку, наведена на рис. 7.1.

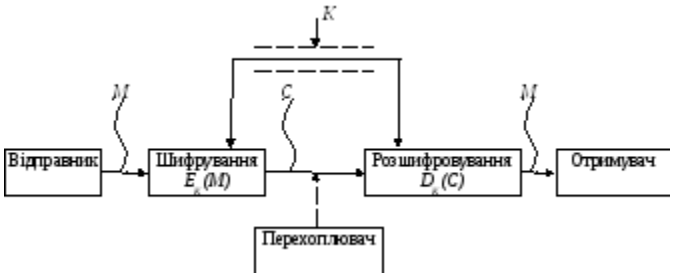

Рис. 7.1. Узагальнена схема криптосистеми

Відправник генерує ***відкритий текст*** вихідного повідомлення *M*, яке повинно бути передане законному ***отримувачу*** по незахищеному каналу. За каналом слідкує ***перехоплювач*** з метою перехопити та розкрити повідомлення. Для того, щоб перехоплювач не зміг розкрити зміст повідомлення *M*, відправник його шифрує за допомогою оборотного перетворення E_K та отримує ***шифротекст*** (чи ***криптограму***) $C=E_K(M)$, який відправляє отримувачу.

Законний отримувач, прийнявши шифротекст *C*, розшифровує його за допомогою оберненого перетворення $D=E_K^{-1}$ та отримує вихідне повідомлення у вигляді відкритого тексту *M*: $D_K(C)=E_K^{-1}(E_K(M))=M$.

Перетворення E_K вибирається із сімейства криптографічних перетворень, які називаються ***криптоалгоритмами***. Параметр, за допомогою якого вибирається окреме використовуване перетворення, називається ***криптографічним ключем*** *K*. Краптосистеми мають різні варіанти реалізації: набір інструкцій, апаратні засоби, комплекс комп'ютерних програм, які дозволяють зашифрувати відкритий текст та розшифрувати шифротекст різними способами, один з яких вибирається за допомогою конкретного ключа *K*. Висловлюючись більш формально, криптографічна система – це одно параметричне сімейство $(E_K)_{K\in\overline{K}}$ оборотних перетворень $E_K:\overline{M}\to\overline{C}$ з простору $\overline{M}$ повідомлень відкритого тексту в простір $\overline{C}$ шифрованих текстів. Параметр *K* (ключ) вибирається з кінцевої множини $\overline{K}$, яка називається ***простором ключів***.

Взагалі кажучи, перетворення шифрування може бути симетричним чи асиметричним по відношенню до перетворення розшифровування. Ця важлива властивість функції перетворення визначає два класи криптосистем:

- ***симетричні*** (одноключові) криптосистеми;
- ***асиметричні*** (двохключові) криптосистеми (з відкритим ключем).

Схема симетричної криптосистеми з одним секретним ключем була представлена на рис. 6.1. В ній використовуються однакові секретні ключі в блоках шифрування та розшифровування. Узагальнена схема асиметричної криптосистеми з двома різними ключами K_1 та K_2 представлена на рис. 7.2. В цій криптосистемі один із ключів є відкритим, а другий – секретним.

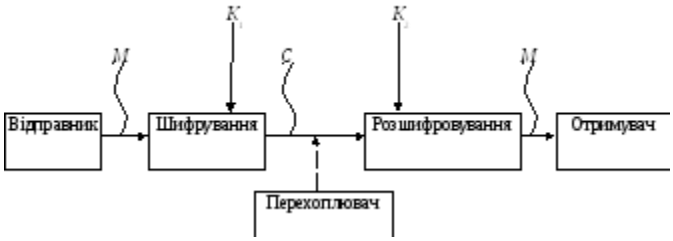

Рис. 7.2. Узагальнена схема асиметричної криптографії з відкритим ключем

У симетричній криптосистемі секретний ключ потрібно передавати відправнику та отримувачу по захищеному каналу розповсюдження ключів, наприклад такому, як кур'єрська служба. На рис. 6.1 цей канал показано „екранованою" лінією. В асиметричній криптосистемі передають по незахищеному каналу тільки відкритий ключ, а секретний ключ зберігають на місці його генерації.

На рис. 7.3 показано потік інформації у криптосистемі у випадку активних дій перехоплювача. Активний перехоплювач не тільки зчитує усі шифротексти, що передаються по каналу, а також може спробувати змінити їх на свій розсуд.

Будь-яка спроба зі сторони перехоплювача розшифрувати шифротекст C для отримання відкритого тексту M чи зашифрувати свій власний текст M' для отримання правдоподібного шифротексту C', не маючи справжнього ключа, називається ***криптоаналітичною атакою***. Якщо спроби криптоаналітичних атак не досягають поставленої мети і криптоаналітик не може, не маючи справжнього ключа, вивести M із C чи C' із M', то вважають, що така криптосистема є ***крипостійкою***.

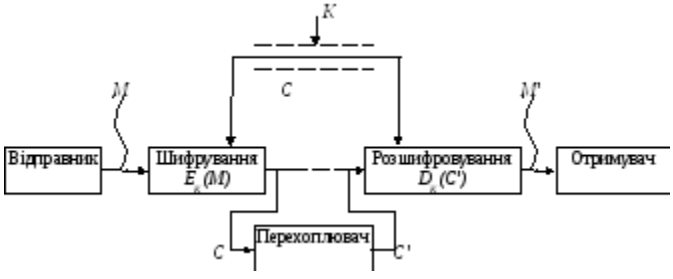

Рис. 7.3. Потік інформації в криптосистемі при активному перехопленні повідомлень

Криптоаналіз – це наука про розкриття вихідного тексту зашифрованого повідомлення без доступу до ключа.

Успішний аналіз може розкрити вихідний текст чи ключ. Він дозволяє також виявляти слабкі місця в криптосистемі, що, в підсумку, приводить до тих же результатів.

Фундаментальне правило криптоаналізу, вперше сформульоване голландцем А. Керкхоффом ще в XIX столітті, полягає в тому, що стійкість шифру (криптосистеми) повинна визначатися тільки секретністю ключа. Іншими словами, правило Керкхоффа полягає в тому, що весь алгоритм шифрування, крім знання секретного ключа, відомий криптоаналітику противника.

Розрізняють шість основних типів криптоаналітичних атак. Усі вони формулюються вважаючи, шо криптоаналітику відомий алгоритм шифрування та шифротексти повідомлень.

Криптоаналітична атака за наявності тільки відомого шифротексту. Криптоаналітик має тільки шифротексти C_1, C_2, … C_i кількох повідомлень, причому усі вони зашифровані з використанням одного і того ж алгоритму шифрування E_K. Робота криптоаналітика полягає у тому, щоб розкрити вихідні тексти M_1, M_2, … M_i якомога більшої кількості повідомлень чи, ще краще, вирахувати ключ K, використаний для шифрування цих повідомлень з тим, щоб розшифрувати й інші повідомлення, зашифровані цим ключем.

Криптоаналітична атака при наявності відомого відкритого тексту. Криптоаналітик має доступ не тільки до шифротекстів C_1, C_2, …C_i кількох повідомлень, а й до відкритих текстів M_1, M_2, … M_i цих повідомлень. Його робота полягає у знаходженні ключа K, що використовується при шифруванні цих повідомлень, чи алгоритму розшифровування D_K будь-яких нових повідомлень, зашифрованих тим же самим ключем.

Криптоаналітична атака при можливості вибору відкритого тексту. Криптоаналітик не тільки має доступ до шифротекстів C_1, C_2, …C_i та зв'язаних з ними відкритих текстів M_1,M_2, …M_i кількох повідомлень, а й може за бажанням вибрати відкриті тексти, які потім отримує у зашифрованому вигляді. Такий криптоаналіз є ефективнішим, порівняно з відомим відкритим текстом, тому, що криптоаналітик може вибрати для шифрування такі блоки відкритого тексту, які дадуть більше інформації про ключ. Робота криптоаналітика полягає у пошуку ключа K, використаного для шифрування повідомлень, чи алгоритму розшифровування D_K нових повідомлень, зашифрованих тим же ключем.

Криптоаналітична атака з адаптивним вибором відкритого тексту. Це особливий варіант атаки з вибором відкритого тексту. Криптоаналітик може не тільки вибирати відкритий текст, який потім зашифровується, а й змінювати свій вибір залежно від результатів попереднього шифрування. При криптоаналізі з простим вибором відкритого тексту криптоаналітик зазвичай може вибрати кілька крупних блоків відкритого тексту для їх шифрування, тоді як при криптоаналізі з адаптивним вибором відкритого тексту він має можливість спочатку вибрати менший пробний блок відкритого тексту, потім вибрати наступний блок на основі першого вибору і т.д. Така атака надає криптоаналітику ще більше можливостей, порівняно з першими трьома типами.

Криптоаналітична атака з використанням вибраного шифротексту. Криптоаналітик може вибрати для розшифровування різні шифротексти C_1, C_2, … C_i та має доступ до розшифрованих відкритих текстів M_1, M_2, …M_i. Наприклад, криптоаналітик отримав доступ до захищеного від несанкціонованого доступу блоку, який виконує автоматичне розшифровування. Завдання криптоаналітика полягає в знаходженні ключа. Цей тип криптоаналізу представляє особливий інтерес для розкриття алгоритмів з відкритим ключем.

Криптоаналітична атака методом повного перебору усіх можливих ключів. Ця атака передбачає використання криптоаналітиком відомого шифротексту та здійснюється шляхом повного перебору усіх можливих ключів з перевіркою, чи є осмисленим відкритий текст. Такий підхід вимагає залучення надзвичайно потужних обчислювальних ресурсів і іноді називається ***силовою атакою***.

Існують і інші, менш розповсюджені криптоаналітичні атаки.

8. Законодавча підтримка захисту інформації

1. Основні положення

Проблема безпеки інформації в період загальної інформатизації, широкого впровадження електронних технологій є однією з найактуальніших у суспільстві. Комплексне вирішення проблем безпеки інформації як складової частини національної безпеки держави в цілому ґрунтується на розробленні загальної стратегії. Необхідно створити єдину правову, організаційну та матеріально-технічну базу з урахуванням міжнародних норм і правил безпеки інформації, а також оптимізувати чинні в країні нормативні, організаційні та регламентуючі документи.

Серед способів захисту інформації виокремлюють способи її захисту від пошкоджень і способи захисту від несанкціонованого доступу.

2. Захист інформації від пошкоджень

Захистити інформацію від пошкоджень можна за допомогою антивірусних програм, резервування інформації, технічних і адміністративних заходів.

Антивірусні програми. Ці програми призначені для захисту від спеціально створених програм пошкодження інформації — вірусів, які класифікують за такими характеристиками.

1. Середовище перебування. Виокремлюють:
   - *файлові* — ті, що додаються до файлів з розширенням exe, com;
   - *завантажувальні* — ті, які додаються до Ьoot-сектора;
   - *мережні* — ті, що поширюються по комп'ютерній мережі;
   - *макровіруси* — ті, які заражають файли Microsoft Office. Вони пошкоджують копію шаблону Normal.dot який завантажується в оперативну пам'ять комп'ютера під час роботи, внаслідок чого всі файли, з якими проводиться робота, стають ураженими.
2. Способи зараження комп'ютера. У цій групі існують такі віруси:
   - *резидентні* — ті, що вміщуються в оперативну пам'ять і додаються до всіх об'єктів (файлів, дисків), до яких звертається ОС;
   - *нерезидентні* — ті, що додаються до оперативної пам'яті і є активними лише короткий час.
3. Функціональні можливості. Виділяють такі гру пи вірусів:
   - *нешкідливі* — ті, що не впливають на роботу комп'ютера (наприклад, збільшують розмір файла);
   - *безпечні* — ті, що заважають роботі, але не пошкоджують інформацію (наприклад, дають якісь повідомлення, перезавантажують комп'ютер тощо);
   - *небезпечні* — ті, що пошкоджують інформацію файлів, зумовлюючи «зависання» комп'ютера;
   - *дуже небезпечні* — ті, що зумовлюють утрату програм, знищення інформації із системних областей, форматування жорсткого диска.
4. Особливості алгоритму. За цією ознакою віруси поділяють на такі групи:
   - *віруси-супутники* — віруси, які не змінюють файлів, але створюють однойменні файли з розширенням сот, що завантажуються першими;
   - *віруси-черв'яки* — віруси, що поширюються автоматично в комп'ютерній мережі за знайденою адресою в адресній книзі;
   - *віруси-паразити* — віруси, які розпізнаються за зміненим змістом дискових секторів і файлів;
   - *Stealth-віруси* — ті, що фальсифікують інформацію, яка читається з диска. Вірус перехоплює вектор переривання int13h і видає активній програмі хибну інформацію, яка показує, що на диску все гаразд. Цей принцип використовується як у файлових, так і в завантажувальних вірусах;
   - *віруси-мутанти* — віруси, що мають зашифрований програмний код;
   - *ретровіруси* — звичайні файлові віруси, які намагаються заразити антивірусні програми, щоб знищити їх або зробити недієздатними.

Антивірусні програми, що дають змогу виявити вірус, відкоригувати або вилучити пошкоджені файли, поділяють на детектори, фаги (лікарі), ревізори, сторожі, вакцини.

Детектори (сканери) перевіряють оперативну або зовнішню пам'ять на наявність вірусу за допомогою розрахованої контрольної суми або сигнатури (частина коду, що повторюється) і складають список ушкоджених програм. Якщо детектор — резидентний, то програма перевіряється, і тільки в разі відсутності вірусів вона активізується. Детектором є, наприклад, програма MS AntiVirus.

Фаги (поліфаги) виявляють і знешкоджують вірус (фаг) або кілька вірусів. Сучасні версії поліфагів, як правило, можуть здійснювати евристичний аналіз файла, досліджуючи його на наявність коду, характерного для вірусу (додавання частини цієї програми в іншу, шифрування коду тощо). Фагами є, наприклад, програми Aidstest, DrWeb.

Ревізори — програми, що контролюють можливі засоби зараження комп'ютера, тобто можуть виявити вірус, не відомий програмі. Ці програми перевіряють стан BOOT-сектора, FAT-таблиці, атрибути файлів (обсяг, час створення тощо). При виявленні будь-яких змін

користувачеві видається повідомлення (навіть у разі відсутності вірусів, але за наявності змін). Ревізором є, наприклад, програма Adinf.

Сторожі — резидентні програми, які постійно зберігаються у пам'яті й у визначений користувачем час перевіряють оперативну пам'ять комп'ютера (включаючи додаткову та розширену), файли, завантажувальний сектор, FAT-таблицю. Сторожем є, наприклад, програма AVP, що може виявити понад ЗО тис. вірусів.

Вакцини — програми, які використовуються для оброблення файлів та завантажувальних секторів з метою завчасного виявлення вірусів.

Резервування інформації. Архіватор WinZip. Основними способами резервування інформації є:

- її зберігання в захищених місцях (спеціальних приміщеннях, сейфах та ін.);
- зберігання інформації в територіально розподілених місцях.

Архіватор WinZip призначений для ущільнення інформації при її резервуванні. Він забезпечує:

- створення нового архіву;
- перегляд і відкривання існуючого архіву;
- додавання (вилучення) файлів до архіву;
- підтримку інтерфейсу WINDOWS 98/2000;
- Internet-підтримку для форматів Internet-файлів — gzip стиснення — Uunix, UUEncode, XXencode, BinHex, ARJ, LZH;
- створення саморозпаковувальних архівів;
- вірусну перевірку.

Для відкривання існуючого архіву його активізують, клацаючи правою клавішею миші (команда **Открыть**). Меню **File** містить команди для виконання таких дій, як відкривання та закривання архіву, створення нового, перегляд усіх архівів диска, вилучення, копіювання, переміщення, друкування архіву.

Меню **ACTIONS** містить команди для роботи з одним вибраним із архіву файлом (додавання, копіювання, вилучення, перейменування, створення саморозпаковувального файла). Для розпакування архівного файла вигористовується команда **Extract** або відповідна кнопка панелі інструментів.

Меню **ACTIONS** містить також команду **Make.Exe File**, яка використовується для створення саморозпаковувальних архівів. Робота з таким архівом не потребує програми-архіватора.

Для створення архіву файл виділяють, клацають правою клавішею миші та активізують команду **Add to**.

Технічні заходи. Один із технічних заходів захисту інформації — використання безперебійних джерел живлення (UPS), які дають змогу коректно завершити роботу і вийти з програми в разі перебою електропостачання. Ці пристрої залежно від складності задачі та потужності встановленого комп'ютерного обладнання можуть підтримувати роботу системи від 20 хв. до кількох годин. Більш надійна робота забезпечується при підключенні до запасної енергопідстанції. На підприємствах, що мають неперервний робочий цикл перероблення інформації (наприклад, головні банки), слід використовувати власні енергогенератори.

Адміністративні заходи. Керівники інформаційних відділів повинні:
чітко визначити функції всіх учасників інформаційного процесу;

- досліджувати й аналізувати ризики безпеки інформації;
- створити інструкції щодо дій персоналу в разі виникнення загроз безпеці інформації;

- мінімізувати ризик для тих, хто працює з важливою інформацією, та їх родин із метою запобігання їх викраденню та вимаганню інформації;
- визначити стратегію резервування, створити окрему інструкцію з резервування (наприклад, «Цю інформацію копіювати кожен день о 12 год.»). При цьому слід ураховувати *фізичне* руйнування магнітних носіїв з часом. Копій має бути як мінімум дві, одна з яких зберігається у вогнетривкому сейфі біля комп'ютера, інша — якнайдалі від офісу (на випадок вибуху, пожежі, землетрусу).

Простота та велика кількість способів доступу та модифікації інформації, велика кількість кваліфікованих фахівців, широке використання у громадському виробництві спеціальних технічних засобів дозволяють зловмиснику практично в будь-який момент та в будь-якому місці здійснювати дії, що представляють загрозу інформаційній безпеці як в локальному, так і в глобальному масштабах.

Державна політика у сфері формування інформаційних ресурсів та інформатизації повинна бути направлена на створення умов для ефективного та якісного інформаційного забезпечення розв’язання стратегічних та оперативних задач соціального і економічного розвитку країни. Державні і недержавні організації, а також громадяни мають рівні права на розробку і виробництво інформаційних систем, технологій та засобів їх забезпечення.

Як показують численні дослідження, найчастіше загроза інформаційним системам виходить від самих співробітників підприємства, хоча великої шкоди також завдають „хакери“ та промисловий шпіонаж. У зв’язку з цим, як рекомендують фахівці з безпеки, особливу увагу слід звертати на нових співробітників – фахівців у галузі комп’ютерної техніки, програмування та захисту комп’ютерної інформації.

Організаційно-правове забезпечення інформаційної безпеки - сукупність рішень, законів, нормативів, що регламентують як загальну організацію робіт із забезпечення інформаційної безпеки, так і створення та функціонування систем захисту інформації на конкретних об’єктах.

Організаційно правова база має такі основні функції:

1. Розробка основних принципів віднесення відомостей, що мають конфіденційний характер, до захищуваної інформації.
2. Визначення системи органів та посадових осіб, що відповідають за забезпечення інформаційної безпеки в країні та порядку регулювання діяльності підприємств і організацій в цій області.
3. Створення повного комплексу нормативно-правових матеріалів, що регламентують питання забезпечення інформаційної безпеки як у країні в цілому, так і на конкретному об’єкті.
4. Визначення міри відповідальності за порушення правил захисту.

5. Визначення порядку вирішення спірних і конфліктних ситуацій з питань захисту інформації.

Під юридичними аспектами організаційно-правового забезпечення захисту інформації розуміється сукупність законів та інших нормативно-правових актів, за допомогою яких мали б досягатися наступні цілі:

- усі правила захисту інформації є обов'язковими для дотримання усіма особами, що мають відношення до конфіденційної інформації;
- узаконюються усі міри відповідальності за порушення правил захисту інформації;
- узаконюються (набувають юридичної сили) техніко-математичні рішення питань організаційно-правового забезпечення захисту інформації;
- узаконюються процесуальні процедури розв'язування ситуацій, що виникають у процесі функціонування системи захисту.

Створенням законодавчої бази в області інформаційної безпеки кожна держава прагне захистити свої інформаційні ресурси. Інформаційні ресурси держави у першому наближенні можуть бути розділені на три великі групи:

- ***відкрита інформація*** – на розповсюдження та використання такої інформації немає ніяких обмежень;
- ***запатентована інформація*** – охороняється внутрішньодержавним законодавством чи міжнародними угодами як об'єкт інтелектуальної власності;
- ***інформація, що захищається її власником*** – власник самостійно захищає цю інформацію з використанням відпрацьованих механізмів захисту державної, комерційної чи іншої таємниці; до цього виду зазвичай відносять інформацію, яка не відома іншим особам, яка або не може бути запатентована, або зумисно не патентується з метою уникнення чи зменшення ризику заволодіння нею суперниками та/чи конкурентами.

Захищають і охороняють, як правило, не всю, чи не всяку інформацію, а найважливішу, цінну для власника, обмеження розповсюдження якої приносить йому якусь користь чи прибуток, можливість ефективно вирішувати поставлені перед ним задачі. До захищуваної відносять наступні види інформації:

- ***Секретну інформацію***. До секретної інформації відносять відомості, що містять державну таємницю.
- ***Конфіденційну інформацію***. До цього виду захищуваної інформації зазвичай відносять відомості, що містять комерційну таємницю, а також таємницю, що стосується особистого (не службового) життя та діяльності громадян.

Таким чином, під захищуваною інформацією розуміють відомості, на використання і розповсюдження яких введено обмеження їх власником і такі, що характеризуються поняттям „таємниця.

До подібного виду таємниці відноситься засекречування підприємством відомостей, які допомагають йому ефективно вирішувати задачі виробництва та вигідної реалізації продукції. Сюди ж відносяться і таємниці особистого життя громадян, які зазвичай охороняються державою: таємниця переписки, лікарська таємниця, таємниця грошового вкладу в банку тощо. Класифікацію інформації з точки зору її власника можна представити у вигляді таблиці (табл. 8.1). Курсивом виділена та інформація, захист якої забезпечується державою.

Таблиця 8.1 Класифікація інформації стосовно її власника

Власник	**Вид інформації**				
	Захищаєма		**Запатентована**		**Відкрита**
	Секретна	**Конфі-денційна**	**Патент**	**Авторське право**	
Особа		особиста таємниця; персональні дані	*Патент фізичної особи*	*Авторське право фізичної особи*	
Суспільство		*Комерційна таємниця*	*Патент юридичної особи*	*Авторське право юридичної особи*	
Держава	*Державна таємниця*	*Службові відомості*	*Державний патент*		

Відмінною властивістю інформації, яка захищається, є те, що засекречувати її може тільки її власник чи уповноважені ним на те особи. Власниками захищуваної інформації можуть бути:

- ***держава та її структури (органи)***; в цьому випадку до неї відносяться відомості, які є державною, службовою таємницею, інші види захищуваної інформації, що належить державі чи відомству, до них можуть бути віднесені і відомості, які є комерційною таємницею;
- ***підприємства, товариства, акціонерні товариства та ін.*** – інформація є їх власністю та складає комерційну таємницю;
- ***громадяни держави*** (їх права – таємниця переписки, телефонних та телеграфних розмов, лікарська таємниця, персональні дані та ін. – гарантуються державою. Особисті таємниці – їх особиста справа; слід зазначити, що держава не несе відповідальності за збережуваність особистих таємниць).

Державна таємниця(також – ***секретна інформація***) – вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визначені у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою.

Цим же Законом про державну таємницю визначено які відомості можуть бути віднесені до державної таємниці. До них відносяться відомості: у сфері оборони; у сфері економіки, науки і техніки; у сфері зовнішніх відносин а також у сфері державної безпеки та охорони правопорядку.

Таким чином, ***засекречування інформації*** – це сукупність організаційно-правових заходів, регламентованих законами та іншими нормативними актами, по введенню обмежень на розповсюдження і використання інформації в інтересах її власника.

8.2. Правовий захист інформації в інформаційних системах

Сам по собі факт призначення обчислювальної системи для широкого кола користувачів створює певний ризик у плані безпеки, оскільки не всі клієнти будуть виконувати вимоги з її забезпечення. Порядок зберігання носіїв інформації повинен бути чітко визначеним у відповідному правовому акті і передбачати збережуваність носіїв інформації, контроль за роботою з інформацією, відповідальність за несанкціонований доступ до носіїв інформації з метою зняття з них копій, зміни чи пошкодження.

Окремо слід звернути увагу на правові аспекти захисту інформації, які можуть виникнути при недостатньо продуманому чи зловмисному використанні електронно-обчислювальної техніки. До них відносяться:

1. Правові питання захисту масивів інформації від спотворень та встановлення юридичної відповідальності за порушення збереженості інформації.
2. Юридичні та технічні питання захисту інформації від несанкціонованого доступу до неї, які виключають можливість неправомірного її використання.
3. Встановлення юридично закріплених норм та методів захисту авторських прав та пріоритетів розробників програмного продукту.
4. Розробка заходів з надання юридичної сили електронним документам та засобів, які перешкоджають фальсифікації таких документів.
5. Правовий захист інтересів експертів, які передають свої знання до фондів банків даних.
6. Встановлення правових норм та юридичної відповідальності за використання електронно-обчислювальних засобів в особистих цілях, що суперечать інтересам інших осіб та суспільства і можуть завдати їм шкоду.

Відсутність належної реєстрації та контролю робіт, низька трудова і виробнича дисципліна персоналу, доступ сторонніх осіб до обчислювальних ресурсів створюють умови для зловживань і ускладнюють їх виявлення. У кожному обчислювальному центрі прийнято встановлювати та строго дотримуватися регламенту доступу в різні службові приміщення для різних категорій співробітників.

Метою захисту інформації є:

- запобігання витоку, викраденню, втраті, спотворенню, підробці інформації;
- запобігання загрозам безпеки особи, суспільства, держави;
- запобігання несанкціонованим діям по знищенню, модифікації, спотворенню, копіюванню, блокуванню інформації;
- запобігання іншим формам незаконного втручання в інформаційні ресурси та інформаційні системи;
- забезпечення правового режиму документованої інформації, як об'єкта власності;
- захист конституційних прав громадян на зберігання особистої таємниці та конфіденційності персональних даних, доступних в інформаційних системах;
- зберігання державної таємниці, конфіденційності документованої інформації відповідно до законодавства;
- гарантування прав суб'єктів в інформаційних процесах та при розробці, виробництві і використанні інформаційних систем, технологій та засобів їх забезпечення.

Захисту підлягає будь-яка документована інформація, неправомірне використання якої може нанести збитки її власнику, користувачу чи іншій особі. Контроль за дотриманням вимог до захисту інформації та експлуатації спеціальних програмно-технічних засобів захисту, а також забезпечення організаційних мір захисту інформаційних систем, що обробляють інформацію з обмеженим доступом в недержавних структурах, здійснюється органами державної влади. Організації, що працюють з інформацією з обмеженим доступом, яка є власністю держави, створюють спеціальні служби, які забезпечують захист інформації.

Власник документу, масиву документів, інформаційних систем забезпечує рівень захисту інформації відповідно до законодавства. Власник інформаційних ресурсів чи уповноважені ним особи мають право здійснювати контроль за виконанням вимог із захисту інформації та забороняти чи призупиняти обробку інформації у випадку невиконання цих вимог. Власник документованої інформації має право звертатися до органів державної влади для оцінки правильності виконання норм і вимог із захисту його інформації в інформаційних системах. Власник інформаційних ресурсів чи уповноважені ним особи відповідно до закону встановлюють порядок надання користувачу інформації із вказуванням місця, часу, відповідальних посадових осіб а також необхідних процедур і забезпечують необхідні умови доступу користувачів до інформації.

Ризик, пов'язаний із використанням не сертифікованих інформаційних систем і засобів їх забезпечення лежить на власнику цих систем і засобів. Ризик, пов'язаний з використанням інформації, отриманої **із не сертифікованої системи**, лежить на споживачі інформації.

Під інформаційною безпекою України розуміється стан захищеності її національних інтересів в інформаційній сфері, який визначається сукупністю збалансованих інтересів особи, суспільства та держави і здійснюється **Службою Безпеки України.**

Державна система забезпечення інформаційної безпеки призначена для розв'язання наступних проблем, що вимагають законодавчої підтримки:

1. захист персональних даних;
2. боротьба з комп'ютерною злочинністю, насамперед у фінансовій сфері;
3. захист комерційної таємниці та забезпечення сприятливих умов для підприємницької діяльності;
4. захист державних секретів;
5. створення системи взаємних фінансових розрахунків в електронній формі з елементами цифрового підпису;
6. забезпечення безпеки автоматизованих та автоматичних систем управління потенційно небезпечних виробництв;
7. страхування інформації та інформаційних систем;
8. сертифікація та ліцензування в галузі безпеки, контроль безпеки інформаційних систем;
9. організація взаємодії у сфері захисту даних з іншими державами.

Структура нормативної бази з питань інформаційної безпеки включає:

- Конституцію України;
- Закони України;
- кодекси України (кримінальний, цивільний, господарський;
- укази Президента України та постанови Кабінету Міністрів України;
- відомчі нормативні акти, державні стандарти, інші нормативні документи.

Серед законів слід відмітити наступні:

- „Про інформацію";
- „Про державну таємницю";
- „Про ліцензування певних видів господарської діяльності;
- „Про захист інформації в інформаційно-телекомунікаційних системах";
- „Про телекомунікації";
- „Про Службу безпеки України»;
- „Про електронний цифровий підпис ".

7.3. Законодавство із захисту інформаційних технологій

Українським кримінальним та адміністративним законодавством передбачена відповідальність за здійснення злочинів та правопорушень при роботі з документацією, вираженою документально. Досить детально розроблено питання встановлення відповідальності за розголошення відомостей, що складають державну таємницю.

Існуюче законодавство дозволяє класифікувати та встановлювати відповідальність за різні форми злочинів і правопорушень, зв'язаних з інформацією, представленою у вигляді відомостей чи документів.

Аналіз суб'єктів інформаційних відносин показує, що серед них виділяються наступні категорії осіб:

- власники інформаційних систем;
- персонал інформаційних систем;
- власники інформації;
- джерела інформації;
- користувачі;
- сторонні особи.

У сфері традиційної обробки інформації усі вказані категорії можна розділити на дві групи: особи, яким дозволено доступ до інформації, та особи, яким такий доступ не дозволений. Правопорушення та злочини можуть бути здійснені:

- по необережності (некомпетентності);
- по халатності;
- зумисно.

При класифікації правопорушень та злочинів слід керуватися також: їх високою громадською небезпекою, що вимагає класифікувати навіть ті дії, які не нанесли збитків, але створили передумови для їх нанесення (порушення технології обробки, порушення норм захищеності, неприйняття потрібних мір з організації захисту). При цьому збитки від злочину можуть виражатися у формі:

- втраченої вигоди;
- прямих фінансових втрат;
- моральних збитків.

Іноді задача оцінки інформації у вартісному виразі є надто проблематичною і часто напряму не може бути розв'язана, наприклад при виникненні загроз інформаційним системам, що обробляють секретну інформацію. В цьому випадку відповідальність встановлюється по аналогії до діючих норм кримінального права.

Правовий захист програмного забезпечення за своєю проблематикою багато в чому співпадає з більш широкою задачею – правовим захистом інтелектуальної власності. На даний час **є п'ять основних правових механізмів захисту програмного забезпечення**:

- авторське право;
- патентне право;
- право промислових таємниць;
- право, що відноситься до недобросовісних методів конкуренції;
- контрактне право.

Два основних гравці на цій арені – ***авторське*** та ***патентне право***. Три останніх механізми часто об'єднують в одну групу. Термін дії патентів зазвичай є меншим часу

існування програмних продуктів, у зв'язку з чим їх рідко використовують для захисту програмного забезпечення, у зв'язку з чим основним механізмом захисту програмного забезпечення є авторське право. Однак без реєстрації власник авторського права не може реалізувати свої права. Наприклад він не може подати до суду для захисту його прав і не може отримати компенсацію.

Авторське право надає автору наступні п'ять прав :

- відтворення;
- підготовка похідних творів;
- розповсюдження копій;
- публічне відтворення;
- виставка.

Авторське право, як уже говорилося, захищає не ідею, а її вираження, конкретну форму представлення. Тому в основу захисту програм **авторським правом покладено наступні поняття:**

Послідовність команд. Програма – це послідовність команд, у зв'язку з чим вона може розглядатися як „вираження" ідеї автора, як його твір.

Копіювання. Це поняття, що використовується у авторському праві, може бути розповсюджене на перенесення програм з одного носія на інший, в тому числі на носій іншого типу. Робити висновок про ідентичність програм на різних носіях можна за багатьма ознаками, наприклад, за їх однаковими функціональними властивостями, але співпадання функціональних властивостей не захищається авторським правом, адже однаковість функціональних властивостей іще не свідчить про відтворення „форми" (про копіювання).

Творча активність. Подібно до інших форм відображення, які захищаються авторським правом, комп'ютерна програма є результатом творчості. Хоча ця форма вираження чи відображення все ще не є загальновідомою, рівень творчої активності, умілості та винахідливості, необхідний для створення програми, дозволяє стверджувати, що програми підлягають захисту авторським правом не менше, ніж будь-які інші твори, що захищаються ним. Той факт, що комп'ютерні програми мають практичне призначення, на це не впливає.

Стиль. Творчість, умілість та винахідливість автора проявляються в тому, як створюється програма. Спосіб, яким це все досягається, надає програмі її характерні особливості і навіть стиль.

Алгоритм. Алгоритми – це, власне, кроки, з яких складається розв'язання задачі, що представляють собою елементи, з яких будується програма і які не можуть захищатися

від неавторизованого використання авторським правом. Це аналоги слів у літературі чи мазків пензлем у живопису.

Відбір та поєднання елементів. Як і у випадку інших творів, захист комп'ютерних програм розглядається з точки зору відбору та об'єднання автором базових елементів, в чому і проявляється його творчість та вмілість, що і відрізняє його твір від творів інших авторів.

Оригінальність програми. Основна вимога авторського права базується на оригінальності відбору і поєднання загальновідомих елементів.

Успішність. Успіх у розв'язанні задачі у значній мірі визначається тим відбором та поєднанням елементів, який автор здійснив на кожному кроці створення програми. Тому програма може працювати швидше, бути простішою та надійнішою у використанні, легше сприйматися і бути більш продуктивною ніж її попередники чи конкуренти.

Усі ці та ряд інших міркувань і покладено в основу захисту програм авторським правом.

9. Особливості використання інформаційних технологій

Використання інформаційних технологій залежить від специфіки діяльності об'єкта. Якщо у користувача виникла потреба автоматизувати на практиці додаткову ділянку обробки інформації з використанням відповідних інформаційних технологій, йому необхідно:

- по-перше, описати постановку задачі (визначити, які документи та довідники використовуються і яка їх структура;
- по-друге, вибрати програмне забезпечення та методи обробки інформації;
- по-третє, налагодити розв'язок

Слід зазначити, що при обробці інформації використовується відповідне інформаційне забезпечення. Інформаційне забезпечення - це сукупність вхідних даних для розв'язання задачі. Вихідна інформація однієї задачі може бути інформаційним забезпеченням, тобто сукупністю вхідних даних розв'язання наступної задачі.

Безумовно при використанні інформаційних технологій обробки інформації необхідно знати алгоритм реалізації задачі. **Алгоритм** - це сукупність технологічних операцій послідовного перетворення інформації.

Використання інформаційних технологій обумовлює також вибір програмного забезпечення: типового на базі пакету програм Microsoft Office або спеціалізованого.

Визначившись з програмним засобом, у подальшому необхідно обрати методи реалізації інформаційних технологій, тобто методи послідовного перетворення вхідної інформації у вихідну. До таких методів належать:

- інтерфейсні;
- використання мов об'єктно-орієнтованого програмування;

• візуального програмування, в тому числі використання:

- прототипів об'єктів ("будівельних блоків"), тобто базових класів;

- мови засобу програмування (наприклад, Visual Basic for Application) для автоматизованої побудови макросів управління обробкою Інформації.

Сучасний типовий пакет програм Microsoft Offise (наприклад, Excel, СУБД Access) має такі засоби автоматизованого візуального програмування, як використання базових класів та Visual Basic for Applicatioп (VBA).

Використання ПК в освіті, фізичній культурі та спорті.

Особливість вищої фізкультурної освіти полягає в тому, що студенти готуються для здійснення педагогічного процесу, основою якого є навчання людей різного віку техніці фізичних вправ і вихованню у них фізичних якостей. Необхідні для цього знання, уміння і навики формуються при вивченні спортивно-педагогічних дисциплін: гімнастики, спортивних і рухомих ігор, легкої атлетики, плавання, лижного спорту, спортивного єдиноборства, туризму і інших видів спорту. Ефективність їх викладання, перш за все в частині проектування учбового процесу, може бути істотно підвищена при використанні засобів комп'ютерної техніки і сучасних інформаційних технологій.

Сучасні комп'ютерні і інформаційні технології відрізняються від традиційних дидактичних засобів. Їх унікальні властивості дозволяють ефективно вирішити наступні завдання:

1) візуалізація учбового матеріалу;
2) формування інформаційних ресурсів;
3) підтримка ухвалення рішень;
4) забезпечення асоціативного методу навчання;
5) моделювання процесів і явищ;
6) здійснення порційної видачі інформації;
7) автоматизація контролю знань.

Доцільність використання сучасних інформаційних технологій в учбовому процесі по спортивно-педагогічних дисциплінах диктується тим, що у студентів повинне бути сформоване цілісне уявлення про ідеальну техніку виконання відповідних фізичних вправ. Традиційно для цього використовуються засоби демонстрації, показ і практичне виконання вправ. Фізичні вправи демонструються студентам як в статиці (малюнки, фотографії і кінограми), так і в динаміці (учбові відеофільми). Метод показу звичайно реалізується викладачем або одним із студентів, який володіє відповідною технікою. І, нарешті, найбільш поширеним є метод практичного виконання, коли в процесі занять у студентів виробляються рухові уміння і навики, що формує «правильні» м'язові відчуття. У результаті студенти на основі знання ідеальної техніки фізичних вправ повинні уміти:

1) створювати уявлення у тих, що займаються про правильну техніку;

2) аналізувати демонстровану техніку;
3) розрізняти основні і додаткові елементи техніки;
4) виділяти помилки і похибки в демонстрованих фізичних вправах.

Комп'ютерна візуалізація техніки рухових дій значно ширша за традиційні дидактичні засоби. Сучасні комп'ютерні технології дозволяють виконувати якісне моделювання рухів людини в тривимірному просторі. На відміну від звичайного відеозображення, анімована тривимірна модель надає необмежені можливості для вивчення техніки руху з різних ракурсів. Особливий інтерес комп'ютерна техніка представляє для повноцінного аналізу фізичних вправ. В даний час створені [1] програмно-апаратні комплекси, що дозволяють на основі фото- або відеозображень фіксувати різноманітні біомеханічні параметри з подальшим аналізом і складанням рекомендацій по їх вдосконаленню. Підвищення доступності пристроїв відеозйомки, збільшення місткості джерел зберігання даних, мініатюризація обчислювальної техніки роблять можливою термінову візуалізацію техніки вправ. У учбовому процесі по спортивно-педагогічних дисциплінах за допомогою термінової візуалізації можна формувати у студентів уміння аналізувати техніку, виявляти помилки, дізнаватися правильну техніку.

Таким чином, аналіз педагогічної доцільності використання засобів комп'ютеризації і інформатизації в учбовому процесі по спортивно-педагогічних дисциплінах дозволяє рекомендувати наступний зміст матеріалів:

1) електронні бази даних:
- документи планування (учбовий план, учбова і робоча програми курсів);
- електронні версії навчально-методичної літератури;
- екзаменаційні матеріали;
- перелік профільних ресурсів глобальної мережі Internet;
- проблемні виробничі ситуації і сценарії їх рішення;
- описи дидактичних ігор;
2) відеоматеріали:
- правильна техніка фізичних вправ;
- техніка фізичних вправ, що виконуються з помилками;
- вправи, що приводять до навчання відповідній техніці;
3) електронні учбові курси:
- статичний матеріал (текст, графіка);
- відео і анімація;
- імітаційне моделювання;
4) електронні засоби контролю знань.

Для **сучасної спортивної науки** широке впровадження ІТ здійснюється за багатьма напрямами, але провідними є використання **інструментальних систем** для вимірювання та оброблення інформації про характеристики рухів і створення моделей, що відображають суттєві елементи рухів спортсменів.

В галузі фізичної культури та спорту застосування КІТ науковці поділяють на три взаємопов'язані групи:

- ✓ **довідково-методичні:** розроблення мультимедійних посібників, створення інформаційних баз даних;
- ✓ **пов'язані з вивченням фізичних аспектів організму спортсмена**: біомеханічні, психологічні і статистичні напрями;
- ✓ **аналітичні:** моделювання спортивних рухів і створення комп'ютерних тренажерів-стимуляторів.

Ще один напрямок використання КІТ пов'язаний з **розробленням програм для оздоровчої фізичної культури.**

Програми цього напряму можна диференціювати на:

- ✓ **керівні** (комп'ютер взаємодіє з користувачем за принципом зворотного зв'язку: видає завдання, контролює їх виконання, а за результатами тестів дає відповідні рекомендації),
- ✓ **діагностичні** (дають змогу фахівцеві швидше поставити діагноз),
- ✓ **діагностично-рекомендаційні** (разом з діагнозом користувачеві пропонується певний набір рекомендацій, відповідний виявленому рівневі здоров'я і рухової активності).

Для удосконалення організації занять **оздоровчим фітнесом**, корекції статури жінок, підвищення їхньої фізичної підготовленості і рівня соматичного здоров'я - є розроблена **комп'ютерна програма «Fitball training»,** яка містить 24 моделі занять для 4 рівнів фізичної підготовленості (по 6 моделей для кожного), і, тим самим, позитивно впливати на фізкультурно-оздоровчий процес.

Дослідження свідчать про важливість впровадження сучасних інформаційних технологій для забезпечення спортсменів і тренерів докладною та об'єктивною інформацією про виконання спортивних вправ.

В автоматичних системах спостереження (наприклад, Expert Vision Analysis [EVA], Motion Analysis Corp., Vicon, Oxford Metrics, CODA, Charnwood Dynamics) передбачено використання різноманітних технологій для відстеження і фіксації рухів, деякі в режимі реального часу.

Системи відеоаналізу рухів і складні комп'ютерні комплекси-імітатори поліпшують зворотний зв'язок і сприяють формуванню рухових умінь і навичок та підвищують рівень спортивних результатів.

ВИСНОВОК: Класифікація та практичне використання інформаційних технологій, які побудовані на викладених вище методах, будуть розглянуті у подальших розділах.

Питання для самоконтролю:

1. Що таке інформація, інформаційні технології?
2. Охарактизувати платформу Zoom.
3. Що таке Конвергенція?
4. Призначення нейронної мережі?
5. Що таке системи автентифікації електронних даних?
6. Що таке криптографія, криптоаналіз?
7. Що таке електронний цифровий підпис?
8. Які ви знаєте об'єктно-орієнтовані мови програмування?
9. Які види загрози безпеці інформаційних систем?
10. За якими ознаками виокремлюють основні групи вірусів?
11. Охарактеризуйте роботу антивірусних програм.

12. Вкажіть адміністративні дії, що використовуються для захисту інформації від пошкоджень.
13. Назвіть основні функції програми-архіватора WinZip.
14. На які види класифікується загрожувальна інформація?
15. Що таке несанкціонований доступ?
16. Які ви знаєте програми-віруси?
17. Які є підходи до проблеми забезпечення безпеки ІС?
18. Які етапи включає процес побудови системи захисту в ІС?
19. Які є апаратно-програмні засоби захисту комп'ютерної інформації?
20. Які поняття покладено в основу захисту програм авторським правом?
21. Які права надає автору авторське право ?
22. Що в себе включає структура нормативної бази з питань інформаційної безпеки?
23. Які ви знаєте закони інформаційної безпеки?