МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ДОНЕЦЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ
КРИВОРІЗЬКИЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ

Т.Г. Павлиш, О.П. Цуркан

Інформаційне забезпечення професійної діяльності

навчальний посібник

Кривий Ріг -2021

УДК 004.775 (075.8)

Рекомендовано до друку вченою радою
Донецького юридичного інституту МВС України
(протокол № 16 від 25.06.2021р.)

Рецензенти:

Г.М. Устінова-Бойченко *– кандидатка юридичних наук, доцентка, завідувачка кафедри кримінально-правових дисциплін Криворізького факультету Національного Університету «Одеська юридична академія».*

О.В. Ковальова *– кандидатка юридичних наук, завідувачка кафедри оперативно-розшукової діяльності та інформаційної безпеки ДонДУВС.*

Павлиш Т.Г., Цуркан О.П.

Інформаційне забезпечення професійної діяльності: навчальний посібник. Кривий Ріг. 2021. 87 с.

Навчальний посібник підготовлений для вивчення дисципліни «Інформаційне забезпечення професійної діяльності» здобувачами вищої освіти за спеціальностями 081 «Право» та 262 «Правоохоронна діяльність» освітньо-кваліфікаційного рівня «бакалавр».

ЗМІСТ

ВСТУП

Існуючи в надзвичайно мобільному і динамічному світі, у світі, де кожного дня з'являються нові інформаційні технології, людина повинна бути готовою досить часто змінювати зміст своїх знань, постійно навчатися новому самостійно, застосовувати навички роботи з інформаційними технологіями як у повсякденному житті так і в професійній діяльності. З огляду цього, інформація, інформаційні, комп'ютерні, мультимедійні технології на сьогодні відіграють ключову роль у житті людини.

Використання нових інформаційних технологій забезпечують поширення прав громадян шляхом надання миттєвого доступу до різноманітної інформації, надають можливість активно створювати інформацію, а не тільки її споживати, дозволяють вирішувати складні професійні завдання.

Метою підготовки навчального посібника «Інформаційне забезпечення професійної діяльності» є надання необхідних знань для використання сучасних інформаційних технологій в практичній діяльності правоохоронних органів та напрямів використання інформаційних технологій у практиці боротьби із злочинністю, удосконалення навичок професійної роботи з комп'ютерними пристроями, програмами, комп'ютерними мережами та електронними документами.

Структурно посібник складається із двох частин: теоретичної та практичної, організованих за модульною системою:

Модуль 1. Правова інформація та інформаційно-комп'ютерні технології у юридичній практиці.

Модуль 2. Інформаційне забезпечення юридичної та правоохоронної діяльності в Україні.

У теоретичній частині міститься матеріал по кожній темі модулів. Практична частина містить плани семінарських занять.

МОДУЛЬ 1

Правова інформація та інформаційно-комп'ютерні технології у юридичній практиці

ТЕМА 1. ПРАВОВА ІНФОРМАЦІЯ ТА ПРАВОВА ІНФОРМАТИКА

1. Теоретичні та правові основи інформаційного забезпечення професійної діяльності
2. Поняття інформації, правової інформації та правової інформатики
3. Інформаційні технології в діяльності правоохоронних органів
4. Правові інформаційні системи та підсистеми
5. Автоматизоване робоче місце (АРМ) юриста

Теоретичні та правові основи інформаційного забезпечення професійної діяльності

Останнім часом в Україні спостерігається інтенсивне впровадження сучасних інформаційних технологій практично у всі сфери життєдіяльності держави, у тому числі в діяльність органів Національної поліції (ОНП). Створюються, впроваджуються та успішно використовуються у боротьбі зі злочинністю міжвідомчі банки даних та інші комп'ютеризовані системи [26].

У сучасних умовах протидії організованій, транснаціональній злочинності та тероризму застосування новітніх технологій у розкритті та розслідуванні злочинів набувають першочергового значення.

Багато десятиліть поспіль для встановлення особи громадянина поліцейським або іншим державним установам було потрібно перевірити посвідчення особи – паспорт. Для негласного спостереження за кимось використовували службу зовнішнього спостереження.

Науково-технічна революція надала для цього абсолютно нові можливості: тепер людину можна впізнати за відео зображенням, провести ідентифікацію за голосом, ДНК, відбитками пальців, сітківкою ока, унікальному малюнку вен на долонях та іншими параметрами. Технології GPS, мобільний зв'язок і Wi-Fi доступ в Інтернет уможливили фіксацію її пересування впродовж усього маршруту слідування [3].

Сьогодні людина, яка проходить під об'єктивом камери або розмовляє мобільним телефоном, може і не здогадуватися, що в цей момент автоматично встановлюється її особа і координати. Сучасні технології здатні на це, не повідомляючи об'єкт.

У межах створення «розумної» поліції розпочали активно використовувати безпілотні літальні апарати та роботів-поліцейських. Криміналісти дедалі частіше застосовують 3-D технології.

На основі нейронних мереж розробляються нові поліграфи. Глобальні навігаційні системи стали невід'ємним елементом у розслідуванні злочинів.

Основними тенденціями розвитку інформаційних технологій у правоохоронній сфері є: удосконалення форм та методів управління системами інформаційного забезпечення; централізація та інтеграція комп'ютерних банків даних; впровадження новітніх комп'ютерних інформаційних технологій для ведення кримінологічних та криміналістичних обліків; розбудова та широке використання ефективних та потужних комп'ютерних мереж; застосування спеціалізованих засобів захисту інформації; налагодження ефективного взаємообміну кримінологічною інформацією на міждержавному рівні. Все це забезпечує суттєве підвищення рівня боротьби зі злочинністю [26].

Інформаційне забезпечення органів поліції – це комплекс методів, заходів, засобів різного характеру, які забезпечують створення та функціонування інформаційних технологій, а також їх ефективне використання для вирішення покладених на поліцію завдань. Інформаційні підсистеми як складові системи інформаційного забезпечення призначені для збирання, накопичення, зберігання та обробки інформації з певних напрямів обліків і орієнтовані на використання в діяльності більшості правоохоронних структур, мають загальний характер і належать до загальновідомчих інформаційних систем [4].

Інформація – це інтуїтивне поняття, яке не можна визначити, його можна тільки пояснити синонімами «відомості», «дані».

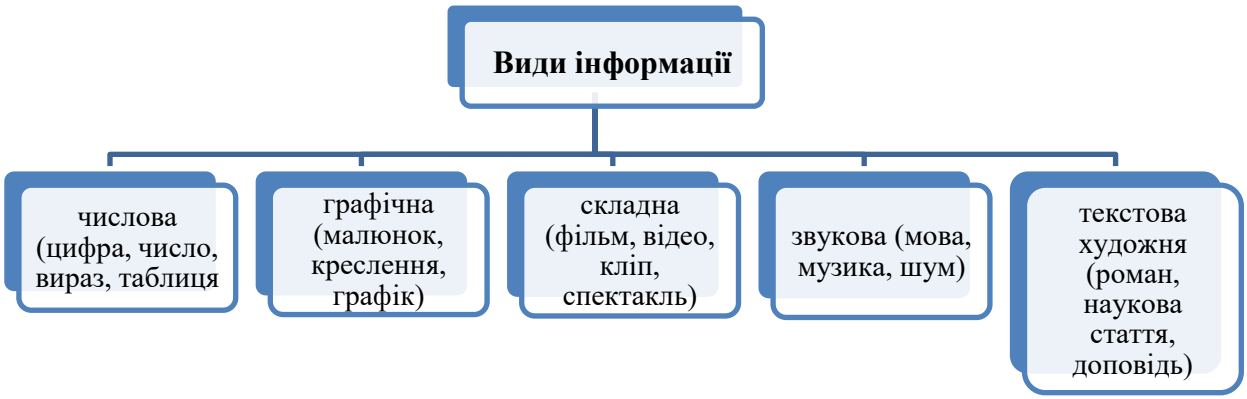


Рис 1. Види інформації

Рис 2. Властивості інформації

Інформаційні процеси – це обмін відомостями між людьми, людиною і автоматом, обмін сигналами між живою і неживою природою у тваринному і рослинному світі, а також генетична інформація. Інформаційні процеси завжди передбачають джерела і споживача інформації.

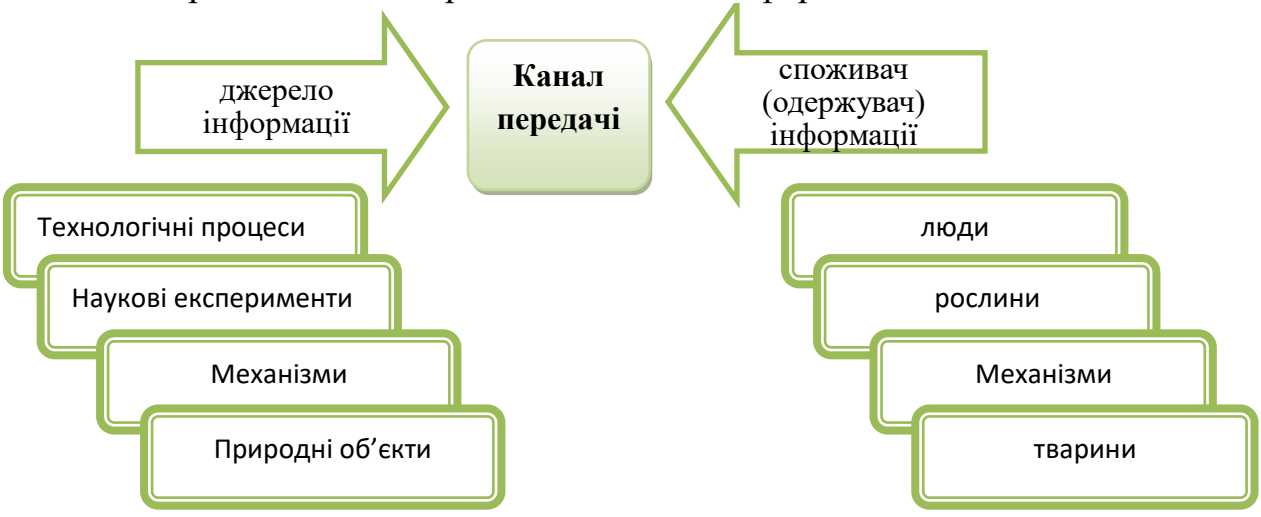


Рис.3. Інформаційний процес

Інформаційні процеси – послідовна зміна стану та (або) уявлення про інформацію в результаті дій, які з нею можна виконувати (створення, збирання, зберігання, обробка, відображення, передавання, розповсюдження, використання, захист, знищення інформації). Під час інформаційного

процесу дані перетворюються з одного виду в інший за допомогою певних методів [27].

Рис 4. Інформаційні процеси

Поняття правової інформації та правової інформатики

Відповідно до ст.1. Закону України «Про інформацію», «інформація– будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді» та ст. 17 «правова інформація − будь-які відомості про право, його систему, джерела, реалізацію, юридичні факти, правовідносини, правопорядок, правопорушення і боротьбу з ними та їх профілактику тощо» [13].

Джерелами правової інформації є Конституція України, інші законодавчі і підзаконні нормативно-правові акти, міжнародні договори та угоди, норми і принципи міжнародного права, а також ненормативні правові акти, повідомлення засобів масової інформації, публічні виступи, інші джерела інформації з правових питань.

До ненормативної правової інформації можна віднести документи, які не містять правових норм, а отже, мають рекомендаційний та інформаційний зміст. Її можна поділити на дві групи:

1. інформація про стан законності та правопорядку: відомості про дотримання прав і свобод людини, що містяться у звітах Уповноваженого з прав людини, офіційні дані про стан виконання Україною своїх міжнародних зобов’язань, матеріали комісій з прав людини; відомості про стан законності й правопорядку, ефективності прокурорського нагляду, що містяться в публікаціях засобів масової інформації, у періодичних виданнях правоохоронних і правозастосовних органів, інформація про форми і способи захисту прав громадян, про вжиті заходи з відновлення законності.
2. інформація, пов’язана з розкриттям і розслідуванням правопорушень: кримінологічна – відомості про злочинність та інші правопорушення, а також ефективність карних заходів; криміналістична – відомості, що

використовуються при доведенні факту злочину та ідентифікації особи чи групи осіб, які вчинили злочин; судово-експертна – відомості, що використовуються під час судових експертиз для доведення (або спростування) факту злочину і вини обвинуваченого; оперативно-розшукова – відомості, що відбивають хід і результати проведення оперативно-розшукових заходів з установлення та розшуку осіб, які вчинили кримінально карне діяння і переховуються від правосуддя, а також інші відомості та матеріали [8].

У сфері юридичної діяльності використовується інформація, що міститься не тільки в правових нормах, а й у низці інших джерел. Приміром, при розкритті й розслідуванні злочинів. Тут поряд із інформацією, що міститься в нормах Кримінально-процесуального та Кримінального кодексів України, органи, що здійснюють оперативну діяльність, дізнання і слідства широко використовують інформацію з таких джерел, як сліди злочинів і злочинця, а також з образів, які залишилися у свідомості людей (потерпілого, свідка і самого злочинця). Це джерела спеціальної криміналістичної інформації, які є різновидом правової інформації, оскільки саме на її основі вирішують завдання з розкриття й розслідування злочинів. Самостійним видом правової інформації є, наприклад, кримінологічна інформація [44].

У цьому сенсі правова інформатика є інструментальним засобом і джерелом знань, необхідних для вирішення багатьох проблем правового регулювання суспільних відносин.

Правова інформатика – це міждисциплінарна галузь знання про закономірності й особливості інформаційних процесів у сфері юридичної діяльності, про їх автоматизацію, про принципи побудови і методики використання автоматизованих інформаційних систем, які створюються для удосконалення і підвищення ефективності юридичної діяльності й вирішення правових задач на базі комплексного використання теорії та методології правових наук, засобів і методів математики, інформатики і логіки [44].

Інформаційні технології в діяльності правоохоронних органів

Інформаційна технологія – це організована сукупність процесів, елементів, пристроїв і методів, використовуваних для обробки інформації. Технологія обробки даних, що використовує персональні комп’ютери й телекомунікаційні засоби, пов’язані з відповідними програмними системами й компонентами для вирішення конкретних задач у обраній предметній області; комплекс методів, способів і засобів, що забезпечують збір, накопичування, зберігання, обробку, передачу й відображення інформації й орієнтованих на підвищення ефективності та продуктивності праці [62, с. 358].

Отримання інформації, придатної для її аналізу людиною, і прийняття на її основі рішення для виконання якої-небудь дії – ціль інформаційних технологій.

Основні напрями використання сучасних інформаційних технологій в правоохоронних органах:

1) використання комп'ютера як інструмента діловодства (створення, зберігання, редагування, друку, передачі за допомогою електронної пошти різноманітних документів).

Робота правоохоронця на будь-якій посаді пов'язана зі створенням, обробкою і зберіганням маси текстових документів, як: договори, позови, протоколи, висновки, рішення та всілякі додатки до них. Комп'ютер дозволяє не тільки виконати цю роботу, але в будь-який момент надрукувати документ на папері, зробити необхідні витяги, скопіювати документ на електронний носій, передати його абонентові на електронному носії або за допомогою електронної пошти.

2) використання комп'ютера та комп'ютерних мереж для створення та обробки інформації специфічної природи (табличних даних, баз даних, картографічних даних).

Значна частина юридичних документів для ефективної роботи вимагає особливої форми подання. Мова йде про таблиці як основні структури, призначені для зберігання інформації, та системи управління базами даних, які дозволяють створювати бази даних, виконувати необхідні користувачу запити і видавати їх результати в зручній формі. До документів такого роду відносяться всілякі картотеки з описом справ, клієнтів, бібліографій, а також книги, реєстри та інші документи подібного роду.

3) використання комп'ютера для самоосвіти та підтримки свого професійного рівня в галузі правознавства (за допомогою довідково-правових комп'ютерних систем).

Сьогодні юристів захлеснув потік нормативних актів, упоратися з яким без допомоги комп'ютера важко, і це викликало цілий напрям у комп'ютерних технологіях – розробку довідково-правових комп'ютерних систем.

4) професійне користування комп'ютером впливає на якість роботи правоохоронців (дозволяє збільшити обсяг методичної інформації, необхідної для розслідування справ, дозволяє моделювати ситуації, здійснювати експертизи, аналіз та прийняття рішень).

5) використання комп'ютера для вирішення задач оперативно-розшукової діяльності та попередження й розслідування кіберзлочинів [56, с.15-16].

Правові інформаційні системи та підсистеми

Термін «інформаційні технології» нерозривно пов'язаний із терміном «інформаційна система» (ІС).

Інформаційна система – це:

1) сукупність організаційних і технічних засобів для збереження та опрацювання інформації з метою забезпечення інформаційних потреб користувачів;
2) система, яка здійснює або в якій відбуваються інформаційні процеси [13];
3) поняття, що використовується для посилань на системи, які забезпечують збирання, збереження й доступ користувачів до накопичених даних. Такі системи звичайно включають до свого складу апаратні й технічні засоби підтримки вищевказаних процесів. Завжди вирішують завдання пошуку або логічної обробки інформації; це організаційно впорядкована сукупність документів (масивів документів) та інформаційно-комп'ютерних технологій, зокрема, з використанням засобів комп'ютерної техніки й зв'язку, що реалізовують інформаційні процеси [62, с. 354].

Рис. 5. Склад інформаційної системи (ІС)

Функціонування будь-якої системи правового характеру завжди пов'язане зі збором, обробкою та використанням інформації.

Правова система – це база даних, у якій містяться нормативні і відомчі акти органів влади, міністерств і відомств. Основна задача, яка вирішується правовою системою – забезпечення користувача повною, оперативною, актуальною і достовірною правовою інформацією. Серед найбільше поширених правових інформаційних систем можна назвати такі як «Ліга: ЗАКОН», «Кодекс», «Українське законодавство» (сайт Верховної Ради України).

Інформаційно-правова система (інформаційно-пошукова система, довідково-правова система) – особливий клас баз даних, в яких зібрано нормативні документи органів державної влади, консультації спеціалістів

щодо їхнього застосування, матеріали спеціалізованої преси, бланки типових документів та інше [44].

Інформаційно-пошукова система – система, призначена для пошуку документів в інформаційних масивах, БД і всій сукупності інформаційних ресурсів. Комплекс інформаційно-пошукових масивів, їхніх носіїв, інформаційно-пошукової мови, правил її використання, критерії видачі розшукуваних матеріалів, програмних і технічних засобів [62, с. 356].

Інформаційно-пошукові системи, інформаційне забезпечення яких складається з кількох (багатьох) баз даних, взаємопов'язаних між собою на рівні системи, називають інтегрованими інформаційно-пошуковими системами (ІІПС) або автоматизованими банками даних.

Однією з найважливіших складових системи інформаційного забезпечення МВС України є інтегрована інформаційно-пошукова система (ІІПС) МВС України

Інтегрована інформаційно-пошукова система МВС України – це сукупність організаційно-розпорядчих заходів, програмно-технічних та інформаційно-телекомунікаційних засобів, що забезпечують формування та ведення довідково-інформаційних, оперативно-розшукових обліків, авторизований доступ до інформаційних ресурсів ІІПС.

ІІПС МВС України – в практичному виді реалізована в програмно-апаратному комплексі «АРМОР» та включає в себе такі підсистеми: «Особа», «Адміністративне правопорушення», «Розшук», «Розшук СНД», «Доставлені», «Пізнання», «Мігрант», «Єдиний облік», «Злочин», «Угон», «Річ», «Антикваріат», «Викрадені (втрачені) документи», «Домашній арешт», «Кримінальна зброя», «Зареєстрована зброя», «Кримінальна статистика», «Корупція».

Прикладами інформаційних підсистем в правоохоронних органах України є:

Єдиний реєстр досудових розслідувань – це створена за допомогою автоматизованої системи електронна база даних, відповідно до якої здійснюється збирання, зберігання, захист, облік, пошук, узагальнення даних про кримінальні правопорушення та хід досудового розслідування у кримінальних провадженням. Досудове розслідування розпочинається з моменту внесення відомостей до Єдиного реєстру досудових розслідувань. Відомості з Реєстру надаються у вигляді витягу.

«АРМОР» – інтегрована інформаційно-пошукова система Міністерства внутрішніх справ України (ІІПС «Армор», також ІІПС ОВС), розроблена УМВСУ в Луганській області, прийнята за базову у всіх обласних МВСУ з 2003 року. Використовується система керування базами даних Oracle. Автоматизовані робочі місця встановлені у міських районних відділах, зв'язок переважно забезпечується за технологією DSL, мобільні робочі місця можуть під'єднуватись до системи віртуальними приватними каналами стільникових операторів зв'язку.

Система централізованого управління нарядами патрульної служби

«ЦУНАМІ» – комплекс апаратних та програмних засобів, а також персоналу, призначений для управління силами й засобами Національної поліції України.

Дана система забезпечує користувачів необхідними інформаційними, технічними та аналітичними ресурсами для виконання функціональних обов'язків та прийняття ефективних управлінських рішень. Система фіксує, зберігає та робить доступними для аналізу та контролю повідомлення і результати реагування на них [39, с. 22].

Законом України «Про Національну поліцію України» статтями 26, 27, 28 передбачено формування, використання інформаційних ресурсів та відповідальність за протиправне використання інформаційних ресурсів.

Стаття 26. Формування інформаційних ресурсів поліцією:

1. Поліція наповнює та підтримує в актуальному стані бази (банки) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України, стосовно:

1) осіб, щодо яких поліцейські здійснюють профілактичну роботу;

2) виявлених кримінальних та адміністративних правопорушень, осіб, які їх учинили, руху кримінальних проваджень; обвинувачених, обвинувальний акт щодо яких направлено до суду;

3) розшуку підозрюваних, обвинувачених (підсудних) осіб, які ухиляються від відбування покарання або вироку суду;

4) розшуку осіб, зниклих безвісти;

5) установлення особи невпізнаних трупів та людей, які не можуть надати про себе будь-яку інформацію у зв'язку з хворобою або неповнолітнім віком;

6) зареєстрованих в органах внутрішніх справ кримінальних або адміністративних правопорушень, подій, які загрожують особистій чи публічній безпеці, надзвичайних ситуацій;

7) осіб, затриманих за підозрою у вчиненні правопорушень (адміністративне затримання, затримання згідно з дорученнями органів правопорядку, затримання осіб органами досудового розслідування, адміністративний арешт, домашній арешт);

8) осіб, які скоїли адміністративні правопорушення, провадження у справах за якими здійснюється поліцією;

9) зареєстрованих кримінальних та адміністративних правопорушень, пов'язаних з корупцією, осіб, які їх учинили, та результатів розгляду цих правопорушень у судах;

10) іноземців та осіб без громадянства, затриманих поліцією за порушення визначених правил перебування в Україні;

11) викрадених номерних речей, цінностей та іншого майна, які мають характерні ознаки для ідентифікації, або речей, пов'язаних із учиненням правопорушень, відповідно до заяв громадян;

12) викрадених (втрачених) документів за зверненням громадян;

13) знайдених, вилучених предметів і речей, у тому числі заборонених або обмежених в обігу, а також документів з ознаками підробки, які мають індивідуальні (заводські) номери;
14) викрадених транспортних засобів, які розшукуються у зв'язку з безвісним зникненням особи, виявлених безгосподарних транспортних засобів, а також викрадених, втрачених номерних знаків;
15) виданих дозвільних документів у сфері безпеки дорожнього руху та дозволів на рух окремих категорій транспортних засобів;
16) зброї, що перебуває у володінні та користуванні фізичних і юридичних осіб, яким надано дозвіл на придбання, зберігання, носіння, перевезення зброї;
17) викраденої, втраченої, вилученої, знайденої зброї, а також добровільно зданої зброї із числа тієї, що незаконно зберігалася;
18) бази даних, що формуються в процесі здійснення оперативно-розшукової діяльності відповідно до закону.
2. Під час наповнення баз (банків) даних, визначених у пункті 7 частини першої цієї статті, поліція забезпечує збирання, накопичення мультимедійної інформації (фото, відео-, звукозапис) та біометричних даних (дактилокартки, зразки ДНК).
3. Поліція забезпечує внесення відомостей до Єдиного реєстру осіб, зниклих безвісти за особливих обставин, та здійснює підтримання таких відомостей в актуальному стані в межах, визначених законодавством.

Стаття 27. Використання поліцією інформаційних ресурсів:
1. Поліція має безпосередній оперативний доступ до інформації та інформаційних ресурсів інших органів державної влади за обов'язковим дотриманням Закону України «Про захист персональних даних».
2. Інформація про доступ до бази (банку) даних повинна фіксуватися та зберігатися в автоматизованій системі обробки даних, включно з інформацією про поліцейського, який отримав доступ, та про обсяг даних, доступ до яких було отримано.
3. Кожна дія поліцейського щодо отримання інформації з інформаційних ресурсів, передбачених статтями 26, 27 цього Закону, фіксується у спеціальному електронному архіві, ведення якого покладається на службу інформаційних технологій Міністерства внутрішніх справ України.

В електронному архіві фіксуються прізвище, ім'я, по батькові та номер спеціального жетона поліцейського, вид отриманої інформації, реєстр, з якого отримувалася інформація, час отримання інформації та інші дані, необхідні для ідентифікації поліцейського, який отримував інформацію з реєстрів.

Стаття 28. Відповідальність за протиправне використання інформаційних ресурсів.
1. Поліція вживає всіх заходів для недопущення будь-яких порушень прав і свобод людини, пов'язаних з обробкою інформації.

2. Поліцейські несуть персональну дисциплінарну, адміністративну та кримінальну відповідальність за вчинені ними діяння, що призвели до порушень прав і свобод людини, пов’язаних з обробкою інформації.
3. Міністерство внутрішніх справ України у межах компетенції здійснює контроль за дотриманням вимог законів та інших нормативно-правових актів під час формування та користування поліцейськими інформаційними базами (банками) даних у порядку, визначеному у статтях 26, 27 цього Закону [18].

Автоматизоване робоче місце (АРМ) юриста

Автоматизоване робоче місце юриста − це комплекс технічних і програмних засобів, що забезпечують юридичну діяльність, а саме підготовку, редагування, пошук необхідних документів і даних, з метою отримання правового результату.

*Виходячи з основних функцій юриста (*підготовка шаблонів основних документів організації: зразки договорів, зовнішніх звітів, довідок, переданих стороннім організаціям та ін.; юридичний супровід угод) вважаємо, що до моделі відповідного автоматизованого робочого місця слід включити наступні основні компоненти (Рис.6):

Технічне забезпечення АРМ юриста – сукупність взаємопов'язаних і взаємодіючих технічних засобів (обчислювальної і організаційної техніки), призначених для автоматизованої обробки інформації, спираючись на результати якої приймаються управлінські рішення. Воно включає наступні види апаратури:

− персональні комп'ютери (ноутбуки);
− периферійні пристрої, що забезпечують введення-виведення і документування інформації (текстової, числової, графічної, мультимедійної) на різних носіях: принтер, сканер, диктофон, фотоапарат та ін.
− пристрої оперативного зв'язку, призначені для передачі інформації до місця її обробки і далі безпосередньо споживачам;
− зовнішні запам'ятовуючі пристрої, що забезпечують зберігання довідкової інформації, оперативних відомостей, результатів обробки, типових рішень та ін.

В даний час в якості таких пристроїв використовуються електронні бібліотеки та сховища даних;

− технічні засоби телекомунікаційного доступу і зв'язку, що забезпечують організацію і функціонування мережевої інформаційної системи, яка підтримує працездатність АРМ юриста;
− пристрої, що забезпечують комунікаційну взаємодію з технологічним обладнанням, що виключають використання проміжних носіїв завдяки безпосередній передачі необхідних даних;
− периферійні пристрої підготовки даних і текстів програм на різних носіях без використання комп'ютера.

Інформаційне забезпечення АРМ юриста слід розглядати як інформаційний ресурс, який об'єднує різноманітні дані і відомості, необхідні для автоматизованого управління функціонуванням господарюючого суб'єкта та прийняття обґрунтованих рішень (ЛІГА: Закон, Нормативні акти України, Юрист-плюс, Законодавство України: сайт Верховної Ради України та ін.). Ці дані можуть бути представлені на різних носіях у вигляді документів, що містять відомості довідкового характеру, що описують об'єкти і ситуації (з сайту Верховного суду, рішення судів із Реєстру судових рішень).

В арсеналі юриста (адвоката) повинна бути спеціальна юридична література за різними напрямами адвокатської діяльності, методичні посібники по тактиці та методиці захисту.

На кожний із напрямків (видів діяльності) заводиться окрема папка з відповідною назвою і створені папки розміщуються в одній загальній папці під назвою «Галузі права».

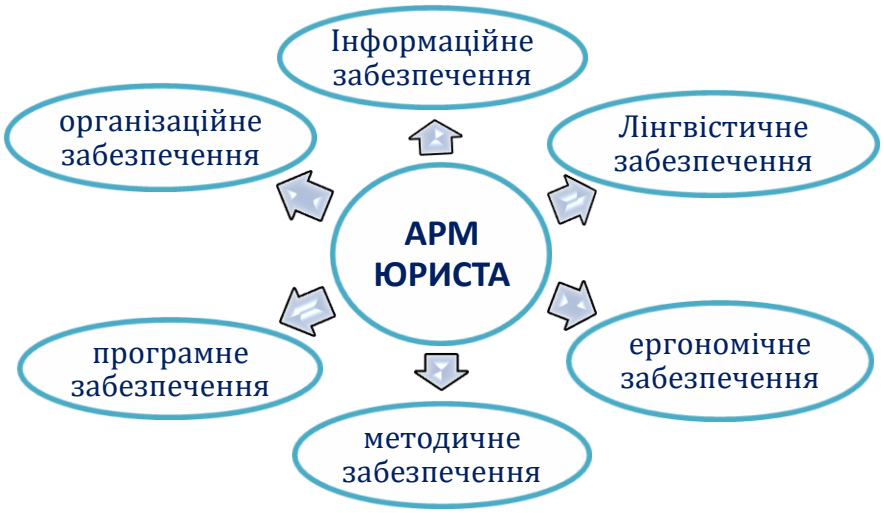


Рис.6. Модель автоматизованого робочого місця юриста

Математичний апарат відображує специфіку предметних областей користувачів АРМ і об'єднує моделі, методи і алгоритми, що реалізують функції управління через відповідний інтелектуальний інтерфейс. Даний апарат може бути надзвичайно широкий і різноманітний, містити як інваріантні компоненти, так і специфічні, притаманні лише даній предметної області.

Програмне забезпечення, що підтримує функціонування АРМ. В якості операційної системи може бути задіяна будь-яка з нині застосовуваних (Microsoft Windows, MacOS від Apple Inc, різновиди Linux).

Що стосується інструментальних засобів, то їх спектр в даний час практично необмежений. Це можуть бути різні системи програмування, системи управління базами даних, експертні системи в сукупності з базами знань, CASE-засоби, спеціалізовані засоби проектування та розробки програмних продуктів та ін.

Програмне забезпечення в основному визначає інтелектуальні можливості АРМ, його професійну спрямованість, повноту реалізації функцій управління, ефективне використання можливостей апаратури. Програмні продукти АРМ повинні гарантувати надійність його функціонування, передбачати збереження інформації, виключати несанкціонований доступ до неї, забезпечувати неухильний захист інформаційних ресурсів та каналів транспортування даних.

Таким чином, до складу автоматизованого робочого місця юриста слід включити текстовий процесор, особисту інформаційну систему (органайзер), СУБД, Web-браузери, програму електронної пошти, спеціалізовані довідково-правові системи.

Лінгвістичне забезпечення АРМ − сукупність мовних засобів, що застосовуються для написання модулів, що підтримують автоматизований процес управління та прийняття рішень. Крім того, необхідно мати мовні засоби, призначені для спілкування фахівця з комп'ютером; даний клас повинен бути орієнтований на професійного виконавця. Це пов'язано з відмінностями, обумовленими не тільки професійною приналежністю та підготовкою користувачів, а й ієрархією службового становища, освітнім рівнем, характером виконуваної роботи, видом використовуваних відомостей. Основу спілкування фахівця-юриста з комп'ютером повинен складати заздалегідь визначений набір термінів з лексичних одиниць конкретної предметної (юридичної) області, а також опис способів, за допомогою яких можуть вводитися нові терміни, замінюючи або доповнюючи існуючі. Крім того, необхідно мати спрощений синтаксис для завдання мовних конструкцій різного ступеня складності, включаючи різноманітні запити.

Ергономічне забезпечення АРМ спрямоване на створення оптимальних умов професійної діяльності юриста на його робочому місці. Головну увагу при цьому слід приділяти не функціонуванню апаратури, а створенню комфортних умов роботи з урахуванням всіх ергономічних параметрів основних і допоміжних засобів праці. До них, зокрема, відносяться:

− оптимальний набір засобів і предметів праці (їх номенклатура, якість, склад, сумісність, легкість в освоєнні);
− зручна для роботи просторова структура робочого місця (свобода рухів під час роботи, свобода переміщень при технічному обслуговуванні обладнання, функціональне розташування елементів відповідно до технологічного процесу, ефективне використання часу, економія фізичних зусиль);
− нормальні умови праці (по освітленості, рівню шуму, кольоровій гамі приміщення і обладнання, температурі, вологості);
− дотримання норм техніки безпеки.

Знання індивідуальних особливостей користувачів конкретних АРМ, їх порівняння з нормативними характеристиками дозволяє правильно оцінити наявне або спроектувати передбачуване робоче місце.

Основу *методичного забезпечення* АРМ складають: спеціальна юридична література в друкованому вигляді та електронному виді, кодекси за усіма видами юридичної діяльності: цивільний, господарчий, адміністративний, кримінальний і процесуальний до нього, сімейний, земельний та інші кодекси.

Організаційне забезпечення АРМ містить: закони, положення, інструкції, накази, документи, які слід організувати на робочому комп'ютері у вигляді папок.

ТЕМА 2. ЗАХИСТ ПРАВОВОЇ КОМП'ЮТЕРНОЇ ІНФОРМАЦІЇ

1. Сутність поняття «інформаційна безпека»
2. Правові засади інформаційної безпеки
3. Кіберзлочинність. Стан злочинності у сфері інформаційних відносин
4. Технології захисту інформації в комп'ютерних мережах
5. Рекомендації щодо захисту персональних даних в комп'ютерних мережах

Сутність поняття «інформаційна безпека»

Сьогодні в нашій державі відбувається швидкий процес інформатизації суспільства, що робить інформацію, інформаційні, комп'ютерні, мультимедійні технології ключовим об'єктом у житті людини. Спостереження за розвитком комп'ютерних технологій та створеного за їх допомогою специфічного середовища – кіберпростору дає підстави говорити про розвиток нового соціального простору, який все частіше стає об'єктом юридичної науки [7, с. 39].

Стрімкий розвиток інформаційних технологій поступово трансформує світ. Відкритий та вільний кіберпростір розширює свободу і можливості людей, збагачує суспільство, створює новий глобальний інтерактивний ринок ідей, досліджень та інновацій, стимулює відповідальну та ефективну роботу влади і активне залучення громадян до управління державою та вирішення питань місцевого значення, забезпечує публічність та прозорість влади, сприяє запобіганню корупції.

Водночас переваги сучасного цифрового світу та розвиток інформаційних технологій обумовили виникнення нових загроз національній та міжнародній безпеці. Поряд із інцидентами природного (ненавмисного) походження зростає кількість та потужність кібератак, вмотивованих інтересами окремих держав, груп та осіб.

Поширюються випадки незаконного збирання, зберігання, використання, знищення, поширення, персональних даних, незаконних фінансових операцій, крадіжок та шахрайства у мережі Інтернет. Кіберзлочинність стає транснаціональною та здатна завдати значної шкоди інтересам особи, суспільства і держави [35].

У сучасному суспільстві для задоволення його потреб виникають проблеми інформаційного забезпечення всіх сфер діяльності людини. Одна з таких проблем – забезпечення надійного захисту інформації. Особливої гостроти вона набуває у зв'язку з масовою комп'ютеризацією всіх видів діяльності людини, при об'єднанні ЕОМ у комп'ютерні мережі та підключення до Internet. Тому для спеціалістів різноманітного профілю актуальною є підготовка в галузі захисту інформації [44, с. 34].

Інформаційна безпека – це стан захищеності систем обробки і зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації, використання й розвиток в інтересах громадян або комплекс заходів, спрямованих на забезпечення захищеності інформації особи, суспільства і держави від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки запису чи знищення.

Інформаційна безпека держави характеризується ступенем захищеності і, отже, стійкістю основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи, суспільної свідомості і т. д.) стосовно небезпечних (дестабілізаційних, деструктивних, суперечних інтересам країни тощо), інформаційним впливам, причому як до впровадження, так і до вилучення інформації.

Поняття інформаційної безпеки не обмежується безпекою технічних інформаційних систем чи безпекою інформації у чисельному чи електронному вигляді, а стосується усіх аспектів захисту даних чи інформації незалежно від форми, у якій вони перебувають [21].

Визначення терміну «інформаційна безпека» знаходимо в термінологічному словнику на сайті Верховної Ради України: «інформаційна безпека – це стан захищеності інформаційного середовища суспільства, що забезпечує її формування, використання і розвиток в інтересах громадян, організацій, держави» [31].

Відповідно до Концепції інформаційної безпеки України, «інформаційна безпека – це стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, при якому запобігається завдання шкоди через неповноту, несвоєчасність і недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив та умисне спричинення негативних наслідків застосування інформаційних технологій» [41].

Законом України «Про основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки» запропоноване наступне

визначення поняття «інформаційна безпека»: «інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації» [11].

Відмінним є тлумачення, «інформаційна безпека – захищеність (стан захищеності) основних інтересів особистості, суспільства і держави в сфері інформації, включаючи інформаційну і телекомунікаційну інфраструктуру і власне інформацію та її параметри, такі, як повнота, об'єктивність, доступність і конфіденційність» [65, с. 8].

Таким чином, «інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається завдання шкоди через: негативний інформаційний вплив за допомогою, насамперед, несанкціонованого створення, розповсюдження, використання свідомо спрямованої із визначеною метою неповної, невчасної, невірогідної та упередженої інформації; негативні наслідки застосування інформаційних технологій; несанкціоноване порушення режиму доступу до інформації з подальшим її розповсюдженням та використанням» [36].

Види інформаційної безпеки:

1) Інформаційна безпека держави характеризується мірою захищеності держави (суспільства) та стійкості основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи тощо) відносно небезпечних (дестабілізуючих) інформаційних впливів, причому як з упровадження, так і добування інформації. Інформаційна безпека держави визначається здатністю нейтралізувати такі впливи.
2) Інформаційна безпека особистості – це захищеність психіки й свідомості людини від небезпечних інформаційних впливів: маніпулювання свідомістю, дезінформування, спонукання до образ, самогубства тощо [17].

Інформаційна безпека, як складова особистої безпеки особи – характеризується як стан захищеності особистості, соціальних груп та об'єднань людей від впливів, здатних проти їхньої волі та бажання змінювати психічні стани і психологічні характеристики людини, модифікувати її поведінку та обмежувати свободу вибору [47].

Таким чином, інформаційну безпеку можна розглядати з різних позицій: як інформаційну безпеку держави, як інформаційну безпеку суспільства, як інформаційну безпеку підприємства (установи), як інформаційну безпеку особистості.

Правові засади інформаційної безпеки

Правовою основою інформаційної безпеки є Конституція України, а також закони України, укази та розпорядження Президента України,

міжнародно-правові акти, що пов’язані із забезпеченням як міжнародної, так і національної безпеки, постанови та розпорядження Кабінету Міністрів України, відомчі нормативні акти у формі наказів, директив, положень, правил, інструкцій. воінформаційної безпеки є Конституція України, а також закони України, укази та розпорядження Президента України, міжнародно-правові акти, що пов’язані із забезпеченням як міжнародної, так і національної безпеки, постанови та розпорядження Кабінету Міністрів України, відомчі нормативні акти у формі наказів, директив, положень, правил, інструкцій.

В Україні регулювання інформаційної безпеки здійснюється за допомогою таких нормативно-правових актів: Закон України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки», Закон України «Про інформацію», Закон України «Про Національну програму інформатизації», Указ Президента України «Про Доктрину інформаційної безпеки України», Концепція національної безпеки України та Конституція України. Також інформаційна безпека регулюється рядом наступних міжнародних стандартів та норм: CoBiT (Control Objectives for Information and Related Technology), ITIL (Information Technology Infrastructure Library), ISO/IEC 27001:2005, ISO/IEC 17799, ISO/IES 15408. Варто зазначити, що механізми управління інформаційною безпекою суттєво відстають у розвитку від сучасного рівня інформатизації, що сприяє зростанню рівня кіберзлочинності, яка у свою чергу спричиняє важкі, а іноді й незворотні наслідки для держави, підприємства, суспільства, особи. У глобальному плані спостерігається широкий діапазон кіберзлочинів, які включають злочини, що здійснюються в цілях отримання фінансової вигоди, злочини, пов’язані з використанням інформації, яка міститься в комп’ютері, а також злочини, спрямовані проти конфіденційності, цілісності та доступності комп’ютерних систем [27, с. 8].

Закон України «Про внесення змін до Закону України «Про інформацію» надає таке визначення поняття «захист інформації»: «сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї. Безпека інформації – склад та стан інформації, а також дії з нею, за якого забезпечується визначений рівень інформаційної безпеки» [37].

Загрози інформаційній безпеці – сукупність умов і факторів, що створюють небезпеку життєвоважливим інтересам особистості, суспільства й держави в інформаційній сфері. Основні загрози інформаційній безпеці поділяють на три групи:

1) загрози впливу неякісної інформації (недостовірної, фальшивої, дезінформації) на особистість, суспільство, державу;

2) загрози несанкціонованого й неправомірного впливу сторонніх осіб на інформацію і інформаційні ресурси (їх виробництво, системи формування й використання);

3) загрози інформаційним правам і свободам особистості (праву на виробництво інформації, її поширення, пошук, одержання, передавання та використання; праву на інтелектуальну власність на інформацію, в тому числі й речову) [12].

Держави – члени Ради Європи та ін. підписали Конвенцію про кіберзлочинність, згідно якої визначається ефективна боротьба з кіберзлочинністю, що є необхідною для зупинення дій, спрямованих проти конфіденційності, цілісності і доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами і даними, шляхом встановлення кримінальної відповідальності за таку поведінку, як це описано у Конвенції, надання повноважень, достатніх для ефективної боротьби з такими кримінальними правопорушеннями шляхом сприяння їхньому виявленню, розслідуванню та переслідуванню, як на внутрішньодержавному, так і на міжнародному рівнях, і укладення домовленостей щодо швидкого і надійного міжнародного співробітництва. Конвенцією визначені злочини, пов’язані з використанням комп'ютерів, а саме: підробка з використанням комп'ютерів; шахрайство з використанням комп'ютерів; правопорушення, пов’язані зі змістом даних; правопорушення, пов’язані з дитячою порнографією; правопорушення, пов’язані з порушенням авторського права та суміжних прав [33].

Інформаційна безпека особистості забезпечується Законом України «Про захист персональних даних». Цей Закон поширюється на діяльність з обробки персональних даних, яка здійснюється повністю або частково із застосуванням автоматизованих засобів, а також на обробку персональних даних, що містяться у картотеці чи призначені до внесення до картотеки, із застосуванням неавтоматизованих засобів [60].

Кіберзлочинність. Стан злочинності у сфері інформаційних відносин

Злочинність у віртуальному просторі – явище нове, але частина злочинів, скоєних у сфері високих технологій – це знайомі крадіжки, шахрайства, вимагання. І для дослідження проблеми кіберзлочинності необхідно дати коректні визначення таких явищ, як віртуальний простір, кіберзлочинність, комп'ютерні злочини, кібертероризм, щоб відмежувати їх один від одного і від суміжних понять.

Кіберзлочинність – незаконні дії, які здійснюються людьми, що використовують інформаційні технології для злочинних цілей. Серед основних видів кіберзлочинності виділяють поширення шкідливих програм, злом паролів, крадіжку номерів кредитних карт і інших банківських реквізитів, а також поширення протиправної інформації через Інтернет. Киберзлочинічтю прийнято вважати кримінально карані дії, що передбачають несанкціоноване проникнення в роботу комп'ютерних мереж, комп'ютерних систем та програм, з метою видозміни комп'ютерних даних.

При цьому комп'ютер виступає в якості предмета злочину, а інформаційна безпека об'єкта [60].

Для цілей основної криміналістичної класифікації злочинів, вчинених у кіберпросторі, на групи потрібно виходити саме з традиційних сфер суспільного життя суб'єктів кіберпростору, класифікуючи мотиви вчинення злочинів на такі групи:

1) корисливі мотиви, пов'язані з фінансово-економічною сферою відносин суб'єктів у кіберпросторі;
2) соціально-економічні мотиви, пов'язані з соціальною сферою відносин
3) суб'єктів у кіберпросторі;
4) антидержавно-політичні мотиви, пов'язані з державно-політичною сферою відносин суб'єктів у кіберпросторі;
5) ідейні мотиви, пов'язані зі світоглядною сферою життя суб'єктів відносин у кіберпросторі.

Тож, на підставі класифікації мотивів можна класифікувати злочини, вчинені у кіберпросторі, на відповідні чотири групи:

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

Звичайно ці групи злочинів характеризуються різноманітністю їх кримінально-правових ознак, тому виникає питання поділу на підгрупи в межах виділених груп злочинів, які традиційно утворюють визначену множину злочинів в одному акті розслідування. В цьому сенсі важливим є беззаперечне визнання в юридичній літературі наявності у суб'єкта вчинення злочину, крім основного мотиву, також й додаткових мотивів. З криміналістичної точки зору ці мотиви мають системоутворююче значення в технологіях вчинення злочинів, забезпечуючи досягення кінцевої злочинної мети, відповідно зумовлюють суб'єктний склад організованої групи, відповідний комплекс злочинів, обрання певного предмету посягання. Організовані злочинні групи вчиняють не окремі злочини, а їх комплекси, розробляючи цілі технології злочинної діяльності, які забезпечують їм систематичне одержання кримінального доходу [46, с.12].

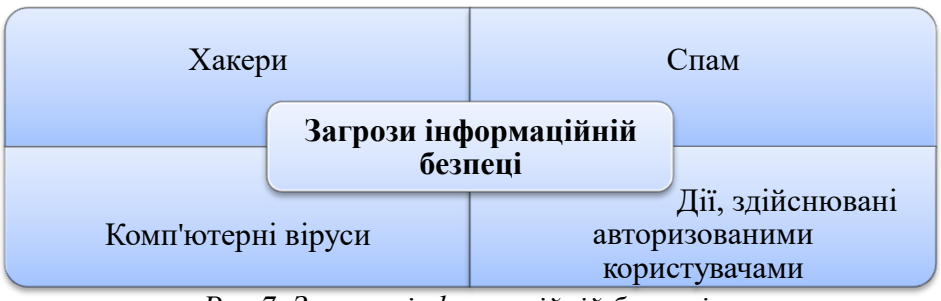


Рис.7. Загрози інформаційній безпеці

Для позначення різних категорій комп'ютерних злочинців використовуються різноманітні терміни: «хакери», «кракери», «пірати», «шкідники».

Хакери (хекери) – це узагальнююча назва людей, які зламують комп'ютерні системи. Часто цей термін застосовується і до «програмістів-маніяків» – за однією з легенд, слово «hack» уперше стало застосовуватись у Массачусетському технологічному інституті для позначення проекту, який не має видимого практичного значення і виконується виключно заради задоволення від самого процесу роботи. У більш вузькому розумінні слово «хакер» позначає тих, хто одержує неправомочний доступ до ресурсів 1С тільки для самоствердження. Останнє відрізняє хакерів від професійних зламувачів – кракерів, які є серйозними порушниками безпеки, оскільки не мають жодних моральних обмежень. Найбільш криміногенною групою є пірати – професіонали найвищого ґатунку, які спеціалізуються на крадіжках текстів нових комерційних програмних продуктів, технологічних ноу-хау тощо. Така робота, природно, виконується на замовлення або передбачає реального покупця. За відсутності замовлень пірат може зосередитися на кредитних картках, банківських рахунках, телефонному зв’язку. В усіх випадках мотивація – матеріальні інтереси, а не цікавість чи пустощі [1].

Протягом останнього десятиріччя значно розширилися масштаби протизаконного використання ЕОМ саме при вчиненні економічних злочинів. Організація інформаційно-технологічних систем на світовому рівні поряд з поліпшенням взаємодії ставить багато проблем. Організовані злочинні формування намагаються проникнути у виробництво програмного забезпечення і впливати на безпеку комп'ютерних мереж. Ці проблеми не можна не враховувати. Просте управління комп'ютерами та водночас недостатня захищеність комп'ютерних мереж від несанкціонованого доступу стає причиною розкрадання великої кількості коштів шляхом їх електронного переказу за вигадані послуги з міжнародних банків усього світу на поточні рахунки до тих країн, де уряди не особливо турбують себе запитами та іншими формами перевірки. Випадки крадіжок грошей за допомогою комп'ютерної техніки стають такими ж небезпечними злочинами, як викрадення дітей, вимагання, тероризм, торгівля наркотиками [36].

Під загрозою безпеки комп'ютерної системи розуміється подія (вплив), що у випадку своєї реалізації стане причиною порушення цілісності інформації, її втрати або заміни. Загрози можуть бути як випадковими, так і навмисними. До випадкових загроз відносять: помилки обслуговуючого персоналу і користувачів; втрата інформації, обумовлена неправильним збереженням архівних даних; випадкове знищення або зміна даних; збої устаткування і електроживлення; збої кабельної системи; перебої електроживлення; збої дискових систем; збої систем архівування даних; збої роботи серверів, робочих станцій, мережевих карт і т.д.; некоректна робота програмного забезпечення; зміна даних при помилках у програмному забезпеченні; зараження системи комп'ютерними вірусами;

несанкціонований доступ; випадкове ознайомлення з конфіденційною інформацією сторонніх осіб.

Найчастіше збиток спричиняється не через чийсь злий намір, а просто через елементарні помилки користувачів, що випадково псують або видаляють дані, життєво важливі для системи. У зв'язку з цим, крім контролю доступу, необхідним елементом захисту комп'ютерної інформації є розмежування повноважень користувачів [20, с.2].

Однією з важливих проблем безпеки мережевого середовища є зловмисні або, принаймні, небажані спроби вторгнення в мережу, що виконуються деякими користувачами або програмним забезпеченням. Такого роду порушення з боку користувачів можуть мати форму спроб несанкціонованого доступу до комп'ютера або спроб легального користувача одержати привілеї або виконати операції, які виходять за рамки наданих йому повноважень. Під порушеннями з боку програмного забезпечення мають на увазі роботу вірусу, «черв'яка» або «троянського коня».

Усі ці порушення належать до питань захисту мереж, оскільки вхід до системи може здійснюватися за допомогою мережі. Проте ці порушення не можна віднести до чисто мережевих. Користувач, що має доступ до локального терміналу, може спробувати проникнути до системи, не використовуючи мережевих засобів. Вірус або «троянський кінь» можуть потрапити до системи з дискети. У цьому сенсі тільки «черв'як» може вважатися чисто мережевим засобом вторгнення в систему. Таким чином, питання вторгнення до системи знаходяться на перетині галузей, що належать до захисту мереж і захисту комп'ютерних систем.

Однією з двох найпоширеніших загроз безпеки є *порушники*, яких називають хакерами (hacker) або зломщиками (cracker), другою загрозою є віруси. Класифікація порушників:

– *Імітатор (masquerader)* – це особа, що не має права користуватися комп'ютером, але подолала механізм керування доступом і використовує права доступу деякого легального користувача.

– *Правопорушник (misfeasor)* – це легальний користувач, що намагається дістати доступ до даних, програм або ресурсів, до яких він не має відповідних прав доступу, або користувач, який має в своєму розпорядженні відповідні права доступу, але використовує їх в зловмисних цілях.

– *Таємний користувач (clandestine user)* – це особа, що заволоділа правами керування системою і використовує ці права для обходу засобів аудиту і керування доступом або для створення перешкод у реєстрації системних подій [9, с.46].

Виявлення правопорушника (легального користувача, що виконує несанкціоновані операції) є складним завданням, оскільки в даному випадку нелегітимна поведінка може майже не відрізнятися від легітимної. Поведінку правопорушника можна виявити, якщо правильно визначити клас умов, за яких відбувається несанкціоноване використання ресурсів. Нарешті,

виявлення таємних користувачів, здається, взагалі виходить за рамки одних лише методів автоматичного виявлення [9, с. 57-58].

Найбільш поширеними є:

– виявлення аномалій**.** Розробляються правила, що дозволяють виявити відхилення від поведінки, які спостерігались раніше.

– ідентифікація вторгнення**.** Підхід на основі використання експертної системи, що виявляє підозрілу поведінку.

За останні п’ять років в Україні кількість інформаційних злочинів зросла щонайменше у 2,5 рази.

Про це повідомляє платформа відкритих даних Опендатабот. Як повідомляється, стрибок кількості всіх кіберзлочинів відбувся у 2017 році. Після цього кількість злочинів має тенденцію зростати. Так в 2017 було зафіксовано 1795 справ, в 2018 – 1023, за півроку 2019 – 1005.

Кіберзлочинці полюють на персональні дані, банківські рахунки, паролі та іншу інформацію, яка існує в електронному вигляді [8].

Потерпілими можуть стати як фізичні особи, так і бізнес та державний сектор. За даними платформи, найпопулярніша стаття кіберзлочинів – шахрайство, на другому та третьому місцях незаконне втручання в роботу комп’ютерів та розповсюдження порнографії.

Повідомлення про шахрайські дії в Інтернеті становлять 80 % від усіх звернень громадян. Найбільш розповсюдженими видами шахрайства у віртуальному просторі є продаж неіснуючих товарів, а також фішингові онлайн-магазини.

Загалом із початку цього року кіберполіція зареєструвала понад 32 тисячі звернень громадян.

Найчастіше злодії ошукують громадян, продаючи неіснуючі товари на майданчиках оголошень або у соцмережах. Як правило, у таких випадках головна умова купівлі – повна переплата за товар.

Ще одна поширена схема шахраїв – створення фішингових ресурсів, які ззовні схожі на популярні Інтернет-магазини. Сплачуючи на таких сайтах, покупець не лише залишається без бажаного товару, а й «передає» дані банківської картки аферисту [13].

Загрози під час роботи в Інтернеті:

– Комунікаційні ризики (кібербулінг, компрометувати, кібергрумінг та ін.);

– Контентні ризики – реклама, нецензурна лексика, сцени насилля, пропаганда расизму та ін.

– Споживчі ризики – реклама, втрата коштів, купівля підроблених товарів відомих брендів, викрадення персональних даних.

– Технічні ризики – спам, віруси, хробаки, трояни, боти, рекламні модулі.

Технології захисту інформації в комп’ютерних мережах

Для вирішення проблеми захисту інформації, основними засобами, використовуваними для створення механізмів захисту, прийнято вважати:

Технічні засоби

Технічні засоби – електричні, електромеханічні, електронні і ін. типу пристрою. Переваги технічних засобів пов'язані з їх надійністю, незалежністю від суб'єктивних факторів, високою стійкістю до модифікації. Слабкі сторони – недостатня гнучкість, відносно великі обсяг і маса, висока вартість. Технічні засоби поділяються на:

1) апаратні пристрої, що вбудовуються безпосередньо в апаратуру, або пристрої, що сполучаються з апаратурою локальних мереж по стандартному інтерфейсу (схеми контролю інформації з парності, схеми захисту полів пам'яті по ключу, спеціальні регістри);
2) фізичні – реалізуються у вигляді автономних пристроїв та систем (електронно-механічне обладнання охоронної сигналізації та спостереження. Замки на дверях, ґрати на вікнах).

Програмні засоби

Програмні засоби – програми, спеціально призначені для виконання функцій, пов'язаних з захистом інформації. А саме програми для ідентифікації користувачів, контролю доступу, шифрування інформації, видалення залишкової (робочої) інформації типу тимчасових файлів, тестового контролю системи захисту та ін. Переваги програмних засобів – універсальність, гнучкість, надійність, простота установки, здатність до модифікації і розвитку.

Недоліки – обмежена функціональність мережі, використання частини ресурсів файл-сервера і робочих станцій, висока чутливість до випадкових або навмисних змін, можлива залежність від типів комп'ютерів (їх апаратних засобів).

Змішані апаратно-програмні засоби

Змішані апаратно-програмні засоби, які реалізують ті ж функції, що й апаратні та програмні засоби окремо, і мають проміжні властивості.

Організаційні засоби

Організаційні засоби складаються з організаційно-технічних (підготовка приміщень з комп'ютерами, прокладка кабельної системи з урахуванням вимог обмеження доступу до неї та ін) і організаційно-правових (національні законодавства і правила роботи, що встановлюються керівництвом конкретного підприємства). Переваги організаційних засобів полягають у тому, що вони дозволяють вирішувати безліч різнорідних проблем, прості в реалізації, швидко реагують на небажані дії в мережі, мають необмежені можливості модифікації та розвитку. Недоліки – висока залежність від суб'єктивних чинників, у тому числі від спільної організації роботи в конкретному підрозділі [1].

В. Іванов, наводить наступні методи захисту інформації в комп’ютерних мережах:

Захист від віддаленого адміністрування. Ефективний захист від віддаленого адміністрування забезпечують два основні методи. Перший – встановлення на комп'ютері «жертви» програми (аналог сервера), з якого зловмисник може створити віддалене з'єднання в той час, коли "жертва" перебуває в мережі. Програми, що використовуються для цього, називаються троянськими. За своїми ознаками вони значною мірою нагадують комп'ютерні віруси. Другий метод віддаленого адміністрування оснований на використанні похибок (помилок), що є в програмному забезпеченні комп' ютерної системи – партнера по зв'язку. Мета цього методу – вийти за рамки спілкування з клієнтської (серверної) програми і прямо впливати на операційну систему, щоб через неї одержати доступ до інших програм і даних. Програми, що використовуються для експлуатації похибок комп'ютерних систем, називаються експлантами.

Захист від троянських програм. Для ураження комп'ютера троянською програмою хтось повинний її запустити на цьому комп'ютері. Тому варто обмежити доступ сторонніх осіб до мережних комп'ютерів звичайним адміністративним способом (фізичне обмеження доступу, пароль тощо). Звичайний метод установки троянських програм на чужих комп'ютерах пов'язаний із психологічним впливом на користувача. Треба умовити користувача зробити це самому. Найчастіше практикується розсилання шкідливих програм у вигляді додатків до повідомлень електронної пошти. У тексті повідомлення вказується, наскільки корисна і вигідна ця програма.

Рекомендації. Ніколи не запускайте нічого, що надходить разом з електронною поштою, незалежно від того, що написано в супровідному повідомленні (навіть від друзів).

Крім електронної пошти зловмисники використовують розповсюдження троянських програм через компакт-диски. Багато програм знаходяться в самому Інтернеті. Ніколи не встановлюйте неперевірених програм з компакт-дисків.

Захист від експлуатації помилок у програмному забезпеченні. Цей вид загроз майже безпечний для клієнтської сторони. Атакам програм-експлантів в основному піддаються сервери. Стратегія зловмисників реалізується в три етапи.

На першому етапі вони з'ясовують склад програм і устаткування в локальній мережі «жертви». На другому етапі розшукують інформацію про відомі помилки (похибки) в даних програмах. На третьому етапі готують програми-експланти (чи використовують раніше підготовлені кимось програми) для експлуатації виявлених похибок. Боротьба з цими загрозами може відбуватися на всіх трьох етапах.

Адміністрація серверів, насамперед, контролює звертання, мета яких полягає в з'ясуванні програмно-апаратної конфігурації сервера. Це дозволяє поставити порушника на облік задовго до того, як він зробить реальну атаку.

У найбільш відповідальних випадках використовують спеціально виділені комп'ютери чи програми, що виконують функції міжмережних екранів. Такі засоби також називають брандмауерами. Брандмауер займає положення між комп'ютерами, що захищаються, і зовнішнім світом. Він не дозволяє переглядати ззовні склад програмного забезпечення на сервері і не пропускає несанкціонованих даних і команд.

Захист від активного змісту. Сторона, яка захищається, повинна оцінити загрозу своєму комп' ютеру і, відповідно, настроїти браузер так, щоб небезпека була мінімальною. Якщо цінні дані чи конфіденційні відомості комп'ютер не містить, захист можна відключити і переглядати веб-сторінки в тому вигляді, який передбачив їх розробник. Якщо загроза небажана, необхідно виконати настроювання захисту в програмі Internet Explorer у діалоговому вікні Параметры безопасности.

Засоби захисту даних на шляхах транспортування. З проникненням комерції в Інтернет усе частіше виникає потреба проведення дистанційних ділових переговорів, купівлі через мережу програмного забезпечення та грошових розрахунків за поставлені товари й послуги, а отже, й захисту даних на шляхах транспортування. Одночасно з захистом даних необхідно забезпечити посвідчення (ідентифікацію) партнерів по зв'язку і підтвердження (аутентифікацію) цілісності даних. Сьогодні в електронній комерції захищають і аутентифікують дані, а також ідентифікують віддалених партнерів за допомогою криптографічних методів, технологічно реалізованих в ЕЦП.

Криптографічний захист інформації – вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо (Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»).

Усі програми кодування дозволяють привести початкову інформацію, що знаходиться в кодованому файлі, до вигляду, який не дозволяє використовувати закодовану інформацію за прямим призначенням. Для приведення закодованої інформації до початкового вигляду застосовують програми декодування. Програми кодування інформації переважно мають функції, що дозволяють декодувати дані, приведені до початкового вигляду [64, с. 70-77].

Для захисту даних і пристроїв комп’ютера від шкідливих програм використовується спеціальне програмне забезпечення – антивірусні програми.

Розрізняють такі антивірусні програми:

– *детектори (сканери)* – програми, що здатні проводити перевірку комп’ютера на наявність шкідливих програм і повідомляти користувача про їх наявність. У ході перевірки програми використовують дані з так званих антивірусних баз – сукупності даних про відомі на даний момент часу шкідливі програми і способи боротьби з ними;

– *лікарі* – програми, що здійснюють «лікування» комп'ютерів від виявлених шкідливих програм, тобто знешкоджують їх, а при неможливості знешкодження можуть видаляти заражені об'єкти або розташовувати їх у спеціальних папках. Як і детектори, лікарі використовують антивірусні бази для оновлення даних про способи боротьби зі шкідливими програмами;

– *монітори* – програми, що постійно (резидентно) знаходяться в оперативній пам'яті комп'ютера з моменту завантаження операційної системи і перевіряють усі файли і диски, до яких іде звертання, блокують дії, що можуть ідентифікуватись як дії шкідливої програми;

– *ревізори* – програми, які аналізують стан системних файлів і папок та порівнюють їх зі станом, що був на початку роботи антивірусної програми. При певних змінах, які характерні для діяльності шкідливих програм, програма-ревізор виводить повідомлення про можливість ураження шкідливою програмою;

– *блокувальники* – програми, які аналізують обмін даними комп'ютера користувача з іншими комп'ютерами в мережі. Програма блокує з'єднання з певним комп'ютером у мережі, якщо фіксує дії, які характерні для шкідливих комп'ютерних програм, і виводить повідомлення про намагання їх проникнення на комп'ютер користувача. Користувач може встановити певні правила обміну даними з іншими комп'ютерами в мережі, дозволити або заборонити певні дії.

Сучасні антивірусні програми – це комплексні програми, що мають властивості всіх перерахованих видів антивірусних програм. Такими є програми Dr.Web, Антивірус Касперського (AVP), Avast Free Antivirus, 360 Total Security, Zillya та інші.

Вони можуть виконувати такі дії:

– знаходячись резидентно в оперативній пам'яті, перевіряти на наявність шкідливих програм усі об'єкти, до яких звертається користувач;

– проводити евристичний аналіз (грец. еысзчб – знайшов) – здійснювати пошук нових шкідливих програм за стандартними діями вже відомих вірусів;

– перевіряти вхідну і вихідну електронну пошту, поштові бази даних;

– виконувати пошук шкідливих програм у архівах;

– виконувати лікування об'єктів – видаляти коди шкідливих програм із файлів, системних областей, відновлюючи їх функціональність;

– виконувати за встановленим розкладом повну перевірку комп'ютера, оновлення антивірусних баз та інше;

– створювати карантинну зону для підозрілих об'єктів;

– блокувати несанкціоновані користувачем дії по відправленню даних на віддалений комп'ютер, запуску програм, завантаженню з віддалених комп'ютерів різноманітних даних та інше.

Якщо антивірусна програма встановлена, то при включенні ПК вона буде однією з перших автоматично завантажуватись в оперативну

пам’ять комп’ютера і виконувати операції з перевірки наявності шкідливих програм та блокування їхніх дій. При цьому в Області сповіщень з’явиться значок антивірусної програми.

Для ефективної боротьби з новими вірусними загрозами потрібно постійно оновлювати антивірусні бази. За замовчуванням в антивірусній програмі встановлено автоматичне оновлення антивірусних баз кожного дня з сайту компанії-виробника. Якщо користувач хоче змінити цей розклад, то потрібно змінити налаштування програми.

Змінивши налаштування антивірусної програми, можна:

– здійснити перевірку всього комп’ютера;
– здійснити перевірку одного із зовнішніх запам’ятовуючих пристроїв;
– встановити типи файлів, які будуть перевірятися:
  - усі файли;
  - тільки файли документів і програм (враховується не розширення імені, а внутрішня структура файлу);
  - файли документів і програм (враховується тільки розширення їх імені і не аналізується внутрішня структура);
  - зменшити час на перевірку встановленням позначки прапорця
– перевіряти тільки нові і змінені файли;
– установити, чи перевіряти файли архівів, файли дистрибутивів (інсталяційних пакетів),
– відкласти або не здійснювати перевірку архівних файлів, якщо їх розмір перевищує введене користувачем значення тощо.

У ході перевірки у вікні програми відображається індикатор ходу перевірки та кількість перевірених файлів і знайдених шкідливих програм. Залежно від налаштувань програма може виводити в інформаційних або діалогових вікнах повідомлення про знайдені шкідливі програми та пропонувати виконати дії над ними.

Рекомендації щодо захисту персональних даних в комп’ютерних мережах

Щоб захистити свої персональні дані слід дотримуватися таких правил:

1. Зберігати ПІН-код кредитки, паролі, дані для входу в інтернет-банкінг у надійному місці, найкраще – у власній пам'яті.
2. У жодному разі не повідомляти третім особам паролі й реквізити картки.
3. Бути дуже обережними, здійснюючи інтернет-покупки. Користуватися лише офіційними й перевіреними сайтами.
4. Користуватися банкоматами, розміщеними у відділеннях банків або в місцях із відеонаглядом.
5. Не використовувати неліцензійне програмне забезпечення та не завантажувати його безкоштовно з підозрілих сайтів.

6. Не відкривати підозрілі листа та не переходити за незрозумілими посиланнями.
7. Обов'язково встановити антивірусні програми.
8. Здійснювати резервне копіювання важливих файлів і не надавати доступу стороннім особам до свого комп'ютера та/або телефону [28].

Захист доступу до ПК:

1) при щоденній роботі за комп’ютером використовуйте обліковий запис Windows без прав адміністратора;
2) під час листування конфеденційну інформацію можна захистити шляхом архівування та встановлення пароля на архів;
3) розділити жорсткий диск на кілька логічних розділів;
4) встановіть антивірус;
5) користуйтеся ліцензійними або з вільною ліцензією програмним забезпеченням;
6) не зберігайте дані на системному диску;
7) періодично робіть резервне копіювання важливої інформації;
8) до флеш-носіїв застосовуйте безпечне вилучення.
9) Брандмауер повинен бути увімкнений

Брандмауер – це технічний пристрій або програмний засіб для контролю даних, що надходять до комп’ютера через мережу (захищає від зловмисного проникнення або потрапляння шкідливих програм, але не запобігають витоку конфеденційної інформації користувача та завантаженню вірусів).

Заходи особистої безпеки в мережі Інтернет:

– не розміщуйте в Інтернеті особисті дані;
– не повідомляйте фінансову інформацію;
– створюйте складні паролі і часто їх змінюйте;
– не відкривайте вкладень до листів від незнайомих осіб;
– використовуйте окрему картку для інтернет-оплат;
– користуйтеся лише знайомими банкоматами;
– встановлюйте мобільні додатки лише з офіційних магазинів;
– періодично перевіряйте робочі екрани мобільних телефонів на предмет незнайомих додатків.

ТЕМА 3. ТЕХНІЧНЕ ТА ЮРИДИЧНЕ ЗАБЕЗПЕЧЕННЯ ЕЛЕКТРОННОГО ПІДПИСУ

1. Електроний бізнес та електронна комерція
2. Поняття про електронний підпис та кваліфікований електронний підпис. Правове регулювання електроного підпису
3. Симетричне і несиметричне шифрування інформації

Електроний бізнес та електронна комерція

Законодавство України у сфері електронного бізнесу та електронної комерції ґрунтується на Конституції України і складається із Цивільного і Господарського кодексів України, законів України «Про захист прав споживачів», «Про рекламу», «Про електронні документи та електронний документообіг», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про телекомунікації», «Про електронний цифровий підпис», «Про платіжні системи та переказ коштів в Україні», «Про фінансові послуги та державне регулювання ринків фінансових послуг», «Про захист персональних даних», «Про електронну комерцію».

Електронний бізнес – це вид економічної діяльності компаній через комп'ютерні мережі, зокрема, Internet, з метою отримання прибутку. Це електронна економічна діяльність, яка здійснюється за допомогою інформаційно-комунікаційних технологій з метою отримання прибутків [10, с.8].

Електронна комерція становить е-бізнес і є одиним зі способів його здійснення.

Проблема оплати за товар чи послугу вирішується масовим упровадженням електронних засобів платежу. Он-лайнові платіжні системи, що існують сьогодні, можна розділити на три види: пластикові (кредитні або дебетові) картки, електронні чеки та цифрові гроші («електронний гаманець»).

Згідно Закону України «Про електронну комерцію», «електронна комерція – відносини, спрямовані на отримання прибутку, що виникають під час вчинення правочинів щодо набуття, зміни або припинення цивільних прав та обов’язків, здійснені дистанційно з використанням інформаційно-телекомунікаційних систем, внаслідок чого в учасників таких відносин виникають права та обов’язки майнового характеру» [57].

Суб’єктом електронної комерції є суб’єкт господарювання будь-якої організаційно-правової форми, що реалізує товари, виконує роботи, надає послуги з використанням інформаційно-телекомунікаційних систем, або

особа, яка купує, замовляє, використовує зазначені товари, роботи, послуги шляхом вчинення електронного правочину.

Отже, електронна комерція, або e-commerce – це сфера економіки, коли торгові і фінансові операції проводяться в інтернеті, або іншими словами, транзакція, здійснена з електронного пристрою, підключеного до мережі, аналог торгового центру, але з великим асортиментом і комфортом: його можна відвідати, не виходячи з дому.

E-commerce в Україні – це поширення, продаж, реклама, просування послуг і товарів, тобто будь-які угоди у всесвітній мережі з використанням цифрових пристроїв.

Основні типи електронної комерції

E-commerce ділиться на кілька загальновизнаних категорій. Ось деякі, з якими ми найчастіше зустрічаємося в повсякденному житті:

- C2C (Consumer-to-Consumer). Схема «споживач-до-споживача». У приклад можна привести торговий майданчик OLX, eBay, і подібні до них, де людина, навіть якщо вона не підприємець, може виставити на продаж якусь річ.
- B2B (Business-to-Business). Схема «бізнес-до-бізнесу». Її характеризує продаж оптових партій товару від виробника дилера. Дилер віддає товар дрібним оптом інтернет-магазинам, звідки він надходить кінцевому споживачеві. Власне, це і є третя головна категорія e-trade.
- B2C (Business-to-Consumer), «бізнес-споживач». Розрахунки між онлайн-магазином і клієнтом, покупка навчальних курсів у зареєстрованих експертів, оренда програмного забезпечення – будь-яка роздрібна угода між юридичними і фізичними особами.
- E2E (Exchange-to-Exchange), «біржа-до-біржі». В Інтернеті термін E2E використовується для позначення обміну інформацією або угод між веб-сайтами, які самі виступають в якості бірж або брокерів для обміну товарами і послугами між підприємствами. Простий приклад: транзакція з електронного гаманця на банківську карту. E2E можна розглядати як форму B2B.
- G2C (Government-to-Citizens), «уряд-до-громадян». Сюди можна віднести сплату податків, комунальних послуг, ліцензій, і так далі. Також громадяни отримують необхідну державну інформацію, що вже не можна назвати електронною комерцією [70].

Поняття про електронний підпис та кваліфікований електронний підпис. Правове регулювання електроного підпису

Власноручний підпис під документом віддавна вважається доказом того, що людина, яка підписала цей документ, ознайомилася з ним і згодна з його змістом. Підпис заслужив довіру з таких причин: дійсність підпису можна перевірити (його наявність у документі дає змогу переконатися, чи справді він був підписаний людиною, що володіє правом ставити цей

підпис); підпис не можна підробити (справжній підпис – доказ того, що саме та людина, якій він належить, поставила цей підпис під документом); підпис, що вже стоїть під одним документом, не може бути використаний ще раз для підписання іншого документа (підпис — невід'ємна частина документа і його не можна перенести в інший документ); підписаний документ не підлягає ніяким змінам; від підпису неможливо відректися (той, хто поставив підпис, не може згодом заявити, що він не підписував цей документ).

У сучасному криміналізованому суспільстві підписи підробляють і копіюють, від них відрікаються, а в уже підписані документи вносять довільні зміни. Тобто застосування рукописного підпису не позбавлене недоліків.

Альтернативу рукописному підпису на сучасному етапі цифровізації та діджиталізації суспільства становить електроний підпис.

Питання надання електронного підпису (ЕЦП) та електронної ідентифікації регулюються Законом України «Про електроні довірчі послуги».

У ст.1 Закону України знаходимо поняття: «електроний підпис» та «кваліфікований електроний підпис».

Електронний підпис – електронні дані, які додаються підписувачем до інших електронних даних або логічно з ними пов’язуються і використовуються ним як підпис.

Кваліфікований електронний підпис – удосконалений електронний підпис, який створюється з використанням засобу кваліфікованого електронного підпису і базується на кваліфікованому сертифікаті відкритого ключа.

Відповідно до Закону України «Про електронні документи та електронний документообіг» ст. 6: «електронний підпис є обов'язковим реквізитом електронного документа, який використовується для ідентифікації автора та/або підписувача електронного документа іншими суб'єктами електронного документообігу. Накладанням електронного підпису завершується створення електронного документа» та ст.7: «оригіналом електронного документа вважається електронний примірник документа з обов'язковими реквізитами, у тому числі з електронним цифровим підписом автора. У разі надсилання електронного документа кільком адресатам або його зберігання на кількох електронних носіях інформації кожний з електронних примірників вважається оригіналом електронного документа» [39].

Електроний підпис отримується за результатом криптографічного перетворення набору електронних даних.

Отримати послуги ЕЦП фізична або юридична особа може в одному з Акредитованих центрів сертифікації ключів (АЦСК).

	Назва юридичної особи	*Назва кваліфікованого надавача електронних довірчих послуг*
1.	АКЦІОНЕРНЕ ТОВАРИСТВО КОМЕРЦІЙНИЙ БАНК "ПРИВАТБАНК"	Кваліфікований надавач електронних довірчих послуг АЦСК АТ КБ "ПРИВАТБАНК"
2.	Військова частина 2428	Кваліфікований надавач електронних довірчих послуг "Військова частина 2428" Державної прикордонної служби України
3.	Генеральний штаб Збройних Сил України	Кваліфікований надавач електронних довірчих послуг "Центр сертифікації ключів Збройних Сил України"
4.	Офіс Генерального прокурора	Кваліфікований надавач електронних довірчих послуг органів прокуратури України
5.	Державна казначейська служба України	Кваліфікований надавач електронних довірчих послуг Державної казначейської служби України
6.	Державне підприємство "Оператор ринку"	Кваліфікований надавач електронних довірчих послуг "АЦСК ринку електричної енергії"
7.	Державне підприємство "ДІЯ"	Кваліфікований надавач електроних довірчих послуг "ДІЯ"
8.	Державне підприємство "Український інститут інтелектуальної власності"	Кваліфікований надавач електронних довірчих послуг Укрпатенту
9.	Державне підприємство "Українські спеціальні системи"	Кваліфікований надавач електронних довірчих послуг Державного підприємства "Українські спеціальні системи"
10.	Інформаційно-довідковий департамент ДПС	Кваліфікований надавач електронних довірчих послуг Інформаційно-довідкового департаменту ДПС
11.	Міністерство внутрішніх справ України	Кваліфікований надавач електронних довірчих послуг – акредитований центр сертифікації ключів МВС України
12.	Національний банк України	Кваліфікований надавач електронних довірчих послуг "Акредитований центр сертифікації ключів Національного банку України"
13.	Акціонерне товариство "Державний ощадний банк України"	Кваліфікований надавач електронних довірчих послуг – центр сертифікації ключів акціонерного товариства «Державний ощадний банк України»
14.	Акціонерне товариство "УкрСиббанк"	Кваліфікований надавач електронних довірчих послуг АТ "УКРСИББАНК"
15.	Товариство з обмеженою відповідальністю "Алтерсайн"	Кваліфікований надавач електронних довірчих послуг АЦСК "eSign" ТОВ "Алтерсайн"
16.	Товариство з обмеженою відповідальністю "Арт-мастер"	Кваліфікований надавач електронних довірчих послуг "MASTERKEY"
17.	Товариство з обмеженою відповідальністю "Інтер-Метл"	Кваліфікований надавач електронних довірчих послуг "АЦСК ТОВ 'Інтер-Метл'"

18.	Товариство з обмеженою відповідальністю "Центр сертифікації ключів "Україна"	Кваліфікований надавач електронних довірчих послуг ТОВ "Центр сертифікації ключів "Україна"
19.	Філія "Головний інформаційно-обчислювальний центр" акціонерного товариства "Українська залізниця"	Кваліфікований надавач електронних довірчих послуг ЦСК АТ "УКРЗАЛІЗНИЦЯ"
20.	Товариство з обмеженою відповідальністю "ДЕПОЗИТ САЙН"	Кваліфікований надавач електронних довірчих послуг "ДЕПОЗИТ САЙН"

Симетричне і несиметричне шифрування інформації

Розрізняють шифрування двох типів:

– **симетричне** (із закритим ключем);
– **несиметричне** (з відкритим ключем).

При **симетричному** шифруванні створюється ключ, після чого через програму шифрування пропускається файл разом зі створеним ключем. Результат пересилається адресатові, йому ж передається і ключ, проте окремо, використовуючи захищений канал зв’язку. Адресат, отримавши файл з ключем, за допомогою програми шифрування може прочитати його.

Несиметричне шифрування складніше, але надійніше. Для його реалізації потрібні два взаємозалежних ключі: відкритий і закритий. Відкритий ключ може вільно розповсюджуватись. Закритий ключ зберігається у таємниці і відомий лише адресату. Відправник, якому треба надіслати зашифроване повідомлення адресату, виконую шифрування і при цьому використовує відкритий ключ. Після одержання повідомлення адресат розшифровує його за допомогою свого закритого ключа. Тобто у загальному випадку відритий ключ використовується для шифрування, а закритий – для розшифрування [35].

Закон України «Про електронні довірчі послуги» визначає поняття особистий ключ як параметр алгоритму асиметричного криптографічного перетворення, який використовується як унікальні електронні дані для створення електронного підпису чи печатки, доступний тільки підписувачу чи створювачу електронної печатки, а також у цілях, визначених стандартами для кваліфікованих сертифікатів відкритих ключів; відкритий ключ – параметр алгоритму асиметричного криптографічного перетворення, який використовується як електронні дані для перевірки електронного підпису чи печатки, а також у цілях, визначених стандартами для кваліфікованих сертифікатів відкритих ключів.

ТЕМА 4. КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ У ПІДГОТОВЦІ ЮРИДИЧНИХ ДОКУМЕНТІВ

1. Технологія підготовки юридичних документів засобами Microsoft Office Word
2. Технологія підготовки юридичних документів засобами Microsoft Office Excel

Технологія підготовки юридичних документів засобами Microsoft Office Word

Для роботи з текстом на комп'ютері використовують: текстові редактори і текстові процесори. У загальному їх називають системами обробки текстів – програми, які призначені для створення, редагування й друку текстових документів.

Текстовий редактор – це програма, що дозволяє вводити, редагувати, форматувати та зберігати текст (Блокнот, WordPad та ін.).

Текстовий процесор – це програма, що дозволяє вводити, редагувати й форматувати текст, вставляти малюнки й таблиці, перевіряти правопис, складати зміст, виконувати перенос слів та багато інших складних операцій (Microsoft Word, Word Prefect, OpenOffice, Word-Star).

Існує багато форматів файлів, в яких системи опрацювання текстів зберігають текстові документи. У кожній із програм один із форматів є стандартним і за замовчуванням. Так, наприклад, в текстовому редакторі Блокнот стандартним є формат .txt, а в текстовому процесорі Word – формат .docx. Для роботи з файлами інших форматів системи опрацювання текстів мають у своєму складі спеціальні програми-конвертори, які перетворюють файли текстового документа з одного формату в інший.

Найпоширеніші формати текстових документів:

– .txt – у файлі зберігається тільки текст з розбиттям на абзаци і без форматування.
– .doc – у файлі зберігається текст, рисунки, вставлені об'єкти, значення їх властивостей.
– .RTF – у файлі зберігається текст, рисунки, вставлені об'єкти, значення їх властивостей.

Можливості текстового процесора:

– набір тексту (введення інформації) в пам'ять комп'ютера;
– можливість введення тексту декількома мовами;
– редагування (заміна, зміна, вставляння, видалення, копіювання, переміщення і т. ін.) фрагментів тексту;

– форматування (зміна параметрів шрифтів, абзаців, сторінок і т. ін.) фрагментів тексту;
– опрацювання декількох текстів одночасно;
– пошук потрібних фрагментів тексту;
– можливість вставляння в текст різних об’єктів (рисунків, схем, таблиць, графіків, формул, спеціальних знаків, яких немає на клавіатурі, тощо);
– перевірка правопису та автоматичне коригування помилок при введенні тексту;
– друкування всього тексту або його фрагментів;
– створення стандартних документів (листів, резюме, записок і т. ін.);
– друкування набраного тексту або його фрагментів;
– збереження набраного тексту на зовнішньому носієві.

Вікно програми Microsoft Word 2010

Після запуску програми Microsoft Word 2010 на екрані з'являється вікно програми є типовим вікном Windows (рис. 8).

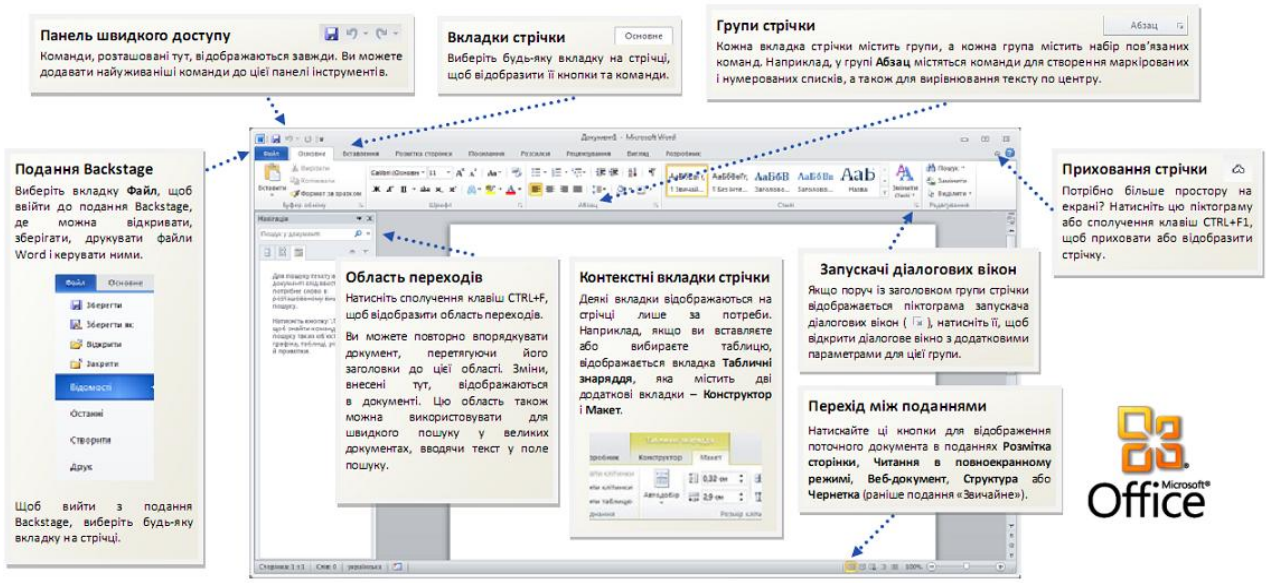


Рис.8. Інтерфейс програми MS Word

Багатофункціональний текстовий редактор Microsoft Word 2010 дозволяє створювати професійно оформлені документи, оскільки він володіє широкими можливостями форматування і оформлення текстів.

Microsoft Word дозволяє вводити, редагувати, форматувати, оформляти текст і грамотно розміщувати його на сторінці. За допомогою цієї програми можна вставляти в документ графіку, таблиці та діаграми, а також автоматично виправляти орфографічні та граматичні помилки. Текстовий редактор Word володіє і багатьма іншими можливостями, значно полегшують створення і редагування документів.

Найчастіше використовувані функції:

– якщо при введенні тексту ви упираєтеся в кінець рядка, Word автоматично робить перехід на наступний рядок;
– якщо при введенні тексту робиться помилка, функція автокорекції автоматично її виправляє. А функція автоматичної перевірки орфографії підкреслює неправильно написані слова червоною хвилястою лінією, щоб їх було легше побачити і виправити;
– якщо користуватися рисками для виділення елементів списку, вживати дробу, знак торгової марки або інші спеціальні символи, функція Автоматичне буде сама їх коригувати;
– режим попереднього перегляду дозволяє побачити документ у тому вигляді, в якому він вийде з друку. Крім того, він дає можливість відобразити відразу всі сторінки, що зручно для внесення змін перед друкуванням.

Програма пропонує також ряд функцій, вельми корисних і які заощаджують час і зусилля. Серед них:
– авто текст – служить одним з інструментів зберігання та швидкої вставки тексту, малюнків, полів, таблиць, закладок та інших часто використовуваних елементів, призначений для зберігання й автоматичного вставки часто вживаних слів, фраз або графіки;
– стилі – дозволяють однією дією застосувати відразу всю групу атрибутів форматування, полегшують роботу тим, що дозволяють зберігати і ставити відразу цілі набори форматів;
– макроси – служать для виконання послідовності команд, необхідні тим, хто часто здійснює одні й ті ж дії. Макрос – це серія команд, згрупованих разом для спрощення повсякденної роботи. Замість того, щоб вручну робити забирають багато часу і повторювані дії, можна створити і запускати один макрос, який буде виконувати це завдання;
– шаблони – шаблони дозволяють заощаджувати час при оформленні типових документів. За допомогою шаблонів Word можна швидко створювати листи, факси, написи на конвертах і т. п., вони призначені для створення професійно оформлених документів. Існують вже готові шаблони, але Microsoft Word дозволяє також створювати власні шаблони;
– колонтитули – використовуються в друкованих документах, колонтитул – це текст та/або малюнок (номер сторінки, дата друку документа, емблема організації, назва документа, ім'я файлу, прізвище автора і т. п.), що друкується унизу або угорі кожної сторінки документа;
– виноски – використовуються в друкованих документах для оформлення різноманітних уточнюючих відомостей та посилань, один документ може містити і звичайні, і кінцеві виноски. Звичайні виноски друкуються внизу кожної сторінки документа. Кінцеві виноски зазвичай містяться в кінець документа.
– Об'єкти – Microsoft Word дозволяє використовувати цю команду для додавання всього або частини файлу, створеного однією з програм Office чи будь-якою програмою, що підтримує зв'язані і впроваджені об'єкти, в інший файл.

Правила введення тексту. Увімкнувши панелі інструментів та лінійку (якщо вони були вимкнені), задавши та перевіривши значення параметрів, можна вводити текст. Головні правила введення текстів:

− не натискайте на клавішу вводу для переходу на новий рядок, оскільки такий перехід відбувається автоматично;

− не натискайте на клавішу пропуск для створення абзацних відступів і центрування тексту, оскільки для цього є спеціальні засоби;

− робіть лише, один пропуск між словами, не забувайте робити пропуск після коми і крапки;

− не натискайте на клавішу Backspace, щоб перевести курсор до позиції з помилкою, користуйтесь для цього клавішами-стрілками;

− щоб отримати велику букву, натисніть на клавішу Shift;

− стежте, щоб не був постійно ввімкненим режим Caps Lock, інакше всі букви будуть великими;

− пам'ятайте, що наступний абзац утворюється після натискання на клавішу вводу; він успадкує вигляд (кажуть також стиль) попереднього абзацу;

– службові документи завжди друкують шрифтом Times New Roman № 14, абзацний відступ -1,25, міжрядковий інтервал – одинарний або полуторний (в залежності від виду документу).

Технологія підготовки юридичних документів засобами Microsoft Office Excel

Електронні таблиці на відміну від текстових процесорів призначені для обробки інформації нетекстового характеру. Основною особливістю електронних таблиць є використання формул і можливість автоматичного перерахунку таблиць у разі зміни даних у таблиці, якщо ці дані використовуються у формулах. У зв’язку з цим електронні таблиці часто називають електронними процесорами.

Термін *«електронна таблиця»* використовується для позначення простої у використанні комп’ютерної програми, яка призначена для обробки даних. Обробка включає в себе:

1) проведення різних обчислень з використанням потужного набору функцій і формул;
2) дослідження впливу різних факторів на дані;
3) вирішення задач оптимізації;
4) отримання вибірки даних, які відповідають заданим критеріям;
5) побудова графіків і діаграм;
6) статичний аналіз даних.

Запуск *Excel* можна здійснити двома способами:

– за допомогою меню *Пуск*: *Пуск – Microsoft Office – Microsoft Excel;*

– якщо на екрані знаходиться Microsoft Office, то для запуску достатньо натиснути кнопку, відповідну Excel.

Microsoft Excel – засіб для роботи з електронними таблицями, що набагато перевищує за своїми можливостями існуючі редактори таблиць. Microsoft Excel – це простий і зручний засіб, що дає можливість проаналізувати дані і за необхідності поінформувати про результат зацікавлену аудиторію, використовуючи Internet.

Під час запуску Excel на екрані з'явиться робоча книга «Книга 1», яка містить декілька робочих листів. Кожний лист є таблицею, яка складається з рядків і стовпців. У цих таблицях зберігаються дані, які необхідно обробляти.

ЕТ складається з клітинок (комірок, чарунок), що утворюють рядки і стовпці. Стовпці таблиці позначені буквами (A,B,C…), а рядки цифрами (1,2,3…). Кожна клітинка має адресу, наприклад A1– адреса лівої верхньої клітинки. Стовпців може бути до 256, а рядків до 65536.

У таблиці можна вводити інформацію різного типу: текст, числа, дати й час, формули, малюнки, діаграми, графіки. Вся введена інформація може бути оброблена за допомогою спеціальних функцій.

Щоб виконати якусь дію над клітинкою чи її даним, клітинку потрібно виокремити (вибрати, активізувати). Це роблять за допомогою клавіш зі стрілками або миші. Активна клітинка має рамку з маркером, який є в правому нижньому куті. З нею можна виконувати дії, визначені в основному чи контекстному меню: ввести чи вилучити дане, скопіювати чи перемістити дане в буфер обміну, очистити клітинку, відформатувати дане чи клітинку, вставити примітку.

Над таблицею є *рядок формул* (якщо він увімкнений). У ньому висвітлюється дане чи формула, які вводять або які вже є в клітинці.

Формули призначені для виконання дій над вмістом клітинок (над даними) згідно з умовою конкретної задачі.

Статистична обробка даних – це збір, упорядкування, узагальнення та аналіз інформації з можливістю визначення тенденції і прогнозу щодо досліджуваного явища. В Excel є величезна кількість інструментів, які допомагають проводити дослідження в даній області. Останні версії цієї програми в плані можливостей практично нічим не поступаються спеціалізованим програмам в області статистики. Головними інструментами для виконання розрахунків й аналізу є функції.

Як і будь-які інші функції в Excel, статистичні функції оперують аргументами, які можуть мати вигляд постійних чисел, посилань на осередки або масиви.

Вирази можна вводити вручну в певну комірку або в рядок формул, якщо добре знати синтаксис конкретного з них. Але набагато зручніше скористатися спеціальним вікном аргументів, яке містить підказки та вже готові поля для введення даних. Перейти у вікно аргументу статистичних виразів можна через *Майстер функцій* або за допомогою кнопок *Бібліотеки функцій* на стрічці.

Запустити Майстер функцій можна трьома способами:

1. Натиснути на піктограму *Вставити функцію* зліва від рядка формул.
2. Перебуваючи у вкладці *Формули,* натиснути на стрічці на кнопку *Вставити функцію* в блоці інструментів *Бібліотека функцій.*
3. Набрати на клавіатурі поєднання клавіш *Shift + F3*.
4. Під час виконання будь-якого з перерахованих вище варіантів відкриється вікно *Майстра функцій*.
5. Потім потрібно натиснути на поле *Категорія* і вибрати значення *Статистичні.*

Статистичні функції Excel

Функція	Опис
СРЗНАЧ (число1; число2; ...)	Повертає середнє (арифметичне) своїх аргументів. Число1, число2 ... - це від 1 до 30 аргументів, для яких обчислюється середнє. Аргументи мають бути або числами, або іменами, масивами або посиланнями, що містять числа.
СЧЁТЗ (значення1; значення2; ...)	Підраховує кількість не порожніх значень в списку аргументів. Функція СЧЁТЗ використовується для підрахунку кількості комірок з даними в інтервалі або масиві.
МАКС (число1;число2; ...)	Повертає найбільше значення з набору значень. Число1, число2... - від 1 до 30 чисел, серед яких потрібно знайти найбільше. Якщо аргументи не містять чисел, то функція МАКС повертає 0 (нуль).
МИН (число1;число2; ...)	Повертає найменше значення в списку аргументів. Якщо аргументи не містять чисел, то функція МИН повертає 0.
НАИБОЛЬШИЙ (масив;k)	Повертає k-ое по величині значення з безлічі даних. Ця функція дозволяє вибрати значення по його відносному місцю розташування. Наприклад, функцію НАИБОЛЬШИЙ можна використовувати для визначення найкращого, другого або третього результатів тестування в балах.
НАИМЕНЬШИЙ (масив;k)	Повертає k-ое найменше значення в безлічі даних. Ця функція використовується для визначення значення, що займає певне відносне положення в безлічі даних.
СЧЁТЕСЛИ (діапазон; критерій)	Підраховує кількість комірок усередині діапазону, що задовольняють заданому критерію. Діапазон - діапазон, у якому потрібно підрахувати комірки. Критерій - критерій у формі числа, вираження або тексту, який визначає, які комірки треба підраховувати. Наприклад, критерій може бути виражений таким чином: 32, "32", ">32", "яблука".
РАНГ (число; посилання; порядок)	Повертає ранг числа в списку чисел. Ранг числа - це його величина відносно інших значень у списку. (Якщо список відсортувати, то ранг числа буде його позицією). Число - число, для якого визначається ранг. Посилання - масив або посилання на список чисел. Нечислові значення в посилання ігноруються. Порядок - число, що визначає спосіб впорядкування.

ТЕМА 5. МЕРЕЖНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

1. Класифікація комп'ютерних мереж
2. Пошук інформації в мережі Інтернет
3. Структура та принципи створення хмарних сховищ даних. Хмарні технології
4. Засоби для інтерактивного спілкування в Інтернеті
5. Сучасні системи авторизації (цифрові, графічні та інші)
6. Електронна пошта

Класифікація комп'ютерних мереж

Комп'ютерна мережа – це група з декількох комп'ютерів, з'єднаних між собою за допомогою мереженого обладнання.

Комп'ютерна мережа забезпечує:

- колективну обробку даних користувачами;
- обмін даними між користувачами;
- спільне використання програм;
- спільне використання периферії (принтерів, модемів та ін.).

Класифікація комп'ютерних мереж:

- за географічною площею: глобальні, регіональні, корпоративні, локальні;
- за сферою застосування: побутові, офісні, промислові;
- за топологією: шина, кільцева, зіркоподібна, деревоподібна;
- за середовищем передачі: симетричний кабель, коаксіальний кабель, вита пара, волоконно-оптичний кабель, інфрачервоне, мікрохвильове випромінювання;
- за набором протоколів.

Локальні мережі – мережі з максимальною відстанню між вузлами не більше декількох км.

Глобальні мережі – мережі, що охоплюють територію країни, кількох країн з відстанню між окремими вузлами в тисячі кілометрів.

Регіональні мережі – мережі масштабу міста, району, області і т.п.

Корпоративні мережі фірми – об'єднання кількох локальних мереж за допомогою телефонних, супутникових, чи інших каналів глобальної мережі у єдину мережу фірми.

Топологія мережі визначає фізичне розташування комп'ютерів, кабелів та інших компонентів мережі.

Основні топології: пряме кабельне з'єднання, шина, зірка, кільце.

Пряме кабельне з'єднання – так можна з'єднати лише два комп'ютери, при цьому існує багато обмежень, тому такий тип з'єднання використовується лише для тимчасового об'єднання двох ПК.

Шинна топологія – всі комп'ютери приєднуються до головного кабелю за допомогою мережевих адаптерів. Всі вони мають рівноправний доступ до магістрального кабелю. Чим більше комп'ютерів на шині, тим повільніше працює мережа. Основний недолік: при пошкодженні магістрального кабелю уся мережа перестає працювати. Перевага: простота організації, легке під'єднання нових робочих станцій. Прикладом такої мережі є локальні мережі побудовані на товстих чи тонких коаксіальних кабелях, які служать магістральним кабелем, до якого підключаються усі ПК.

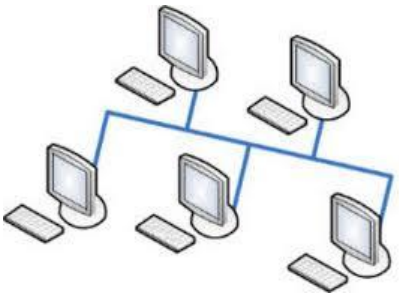


Рис.8. Шинна топологія

Зіркоподібна топологія – усі комп'ютери під'єднується за допомогою сегментів кабелю до центрального компоненту (хабу, світчеру) . З точки зору надійності цей тип топології є найкращим. Вся мережа вийде з ладу лише у випадку виходу з ладу центрального компоненту. Прикладом такої мережі служить будь-яка сучасна локальна мережа з застосуванням хабу як центрального елементу, сегментними кабелями при цьому виступає вита пара.

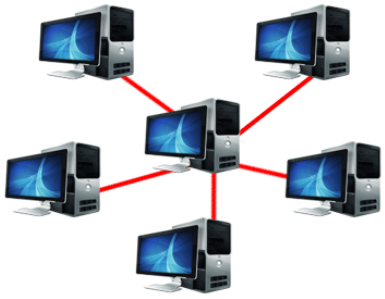


Рис.9. Зіркоподібна топологія

Кільцеподібна топологія – усі комп'ютери об'єднуються в кільце один за одним парою кабелів. Інформація передається послідовно між адаптерами робочих станцій. Якщо з ладу вийде хоч один комп'ютер, уся мережа перестане функціонувати (хоча існують мережі в яких цей недолік усунено). Це є основним недоліком цієї мережі.

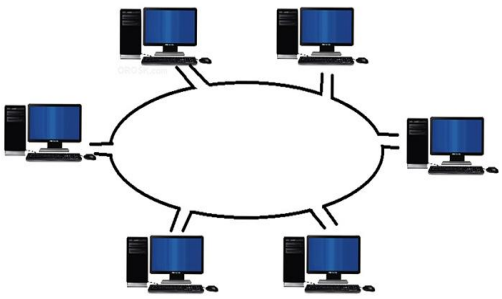


Рис 10. Кільцеподібна топологія

Пошук інформації в мережі Інтернет

Internet – це глобальна інформаційна мережа, яка об'єднує велику кількість регіональних мереж і водночас мільйони комп'ютерів в усіх кінцях планети з метою обміну даними та доступу до інформаційних і технологічних ресурсів.

Інформаційний пошук – це процес пошуку інформації з певної теми. Основним його завданням є швидке і точне знаходження необхідної інформації.

Пошук інформації – завдання, яке найчастіше доводиться виконувати користувачу глобальної мережі. Але знайти у великій кількості сайтів і веб-сторінок потрібне джерело – дуже непросто. Для цього потрібно вміти використовувати різні способи пошуку інформації, правильно формулювати запити й критично оцінювати знайдену інформацію.

Основні способи пошуку у глобальній мережі такі:

1. *Вказання адреси веб-сторінки.* Це найшвидший спосіб пошуку. Його використовують, якщо точно відома адреса сторінки.
2. *Переміщення за допомогою гіперпосилань:* можна переходити зі сторінки на сторінку, шукаючи потрібну інформацію. Недолік очевидний: так можна довго і безрезультатно подорожувати мільйонами сторінок Інтернету.
3. *Використання спеціальних інструментів пошуку:* добірок посилань, пошукових каталогів та систем метапошуку. Ці інструменти мають спеціальні засоби організації пошуку, що забезпечує ефективний пошук потрібної інформації в Інтернеті.

Принцип роботи пошукових покажчиків заснований на *ключових словах*. Ключові слова (Keywords), або *пошуковий запит*, – це слова, фрази або набір символів, що відображають основну думку, які користувач Інтернету вводить у спеціальне поле (рядок) пошуку з метою одержання інформації, що його цікавить. Запит обробляється пошуковою машиною, що знаходить у своїх базах дані адреси Web-ресурсів, у яких присутні ключові слова і клієнтові видаються результати пошуку [61].

Пошук за зображенням у Google допоможе дізнатися більше про об'єкти поруч. Наприклад, ви можете завантажити фото людини та знайти інформацію про неї чи подібні зображення.

Інформацію, яку можна знайти**:**

- результати пошуку, пов'язані з об'єктами на зображенні;
- подібні зображення;
- веб-сайти, де розміщено це або схожі зображення

Структура та принципи створення хмарних сховищ даних. Хмарні технології

Хмарне сховище – це онлайн-сховище, всі дані якого зберігаються на серверах. В хмарних сховищах дані зберігаються і обробляються в так званій «хмарі»: для клієнта це виглядає як один великий віртуальний сервер, куди він може завантажити інформацію.

Після завантаження будь-якого файлу в Інтернет, цей файл може існувати там протягом довгого часу, тобто зберігатися у хмарному сховищі.

Хмарні сховища захищають файли від сторонніх, і вимагають або спеціального посилання, або введення пароля для доступу до них.

Більшість сервісів хмарного зберігання дозволяють завантажувати всі типи файлів: відео, зображення, документи, музику і все, що завгодно.

Переваги хмарного сховища: доступ до файлів з будь-якого пристрою, будь це комп'ютер або смартфон; спільна робота компаній і користувачів з документами і файлами; ймовірність втрати файлів через збої обладнанні зводиться до нуля; високий захист файлів і створення резервних компаній з боку провайдера.

Недоліки хмарного сховища: **з**а статистикою деякі компанії відмовляються використовувати хмарні сховища через недостатній рівень безпеки.

Виділимо найбільш популярні хмарні сховища:

- Dropbox.
- SkyDrive.
- E-disk.
- Google Drive (Google Disk).
- Apple iCloud і iCloud Drive.
- OneDrive і т.д.

Хмарні технології – це технології розподіленої обробки цифрових даних, за допомогою яких комп'ютерні ресурси надаються інтернет-користувачеві як онлайн-сервіс.

Засоби для інтерактивного спілкування в Інтернеті

Інтерактивне спілкування – це обмін повідомленнями в режимі реального часу. В залежності від програм спілкування може виконуватися шляхом передавання голосу, відео зображення чи тексту. Для участі в голосовій конференції необхідно мати мікрофон, динаміки, для відео конференції – відеокамеру.

Форми спілкування в Інтернеті:

- відеоконференції (Zoom, ;
- чат;
- форуми;
- миттєві повідомлення (наприклад, Skype);
- листування електронною поштою (e-mail);
- листування в соціальних мережах.

Основні риси Інтернет-спілкування:

1. Анонімність, яка може призвести до безкарності, розкутості, і безвідповідальності поведінки учасників спілкування.
2. Відсутність невербальної інформації. Як правило, спостерігається установка на бажані риси партнера.
3. Добровільність контактів. Користувач добровільно зав'язує контакти чи може перервати їх у будь-який момент.
4. Стійке прагнення до емоційного наповнення тексту, що виражається у створенні спеціальних знаків для позначення емоцій.

5. Прагнення до нетипової, ненормативної поведінки. Найчастіше користувач презентує себе по-іншому, ніж у реальному житті, програє не реалізовані в діяльності поза мережею ролі, сценарії, і, не знаючи співрозмовника, створює його образ, відмінний від реального.
6. Більша, ніж у реальному світі, залежність від співрозмовника у спілкуванні. Наслідком є порушення безпосереднього живого спілкування.
7. Відсутність єдності простору і часу, тобто Інтернет дає можливість бути одночасно у різних місцях, а також спілкуватися з людьми з інших годинних поясів.
8. Характер спілкування – майже завжди письмовий.

Альтернативою спілкування в режимі реального часу є спілкування за допомогою форумів. *Форум* – це довготривалі і постійно діючі телеконференції, в ході яких співрозмовники надсилають і читають текстові повідомлення в зручний для них час. У дискусіях може брати участь безліч користувачів, не обов'язково одночасно підключених до Інтернету, що, безсумнівно, є перевагою цього способу спілкування. Проте процес обговорення відбувається повільніше, ніж в інтерактивному чаті. *Чат* – інтерактивне спілкування декількох осіб. Чат відносять до відкритих груп спілкування в Інтернеті, де ви можете розмовляти з іншими користувачами в режимі реального часу, використовуючи нік (псевдонім).

Електронна пошта

Електронна пошта (англ. *e-mail*, або *email*, скорочення від *electronic mail*) − спосіб обміну цифровими повідомленнями між людьми з використанням цифрових пристроїв, таких як комп'ютери та мобільні телефони, що робить можливим пересилання даних будь-якого змісту (текстові документи, аудіо-, відеофайли, архіви, програми).

Поштові системи мають подібні основні меню, що значно полегшує роботу з ними. Принципи роботи такі. Запустивши програму і відкривши новий файл, можна в основному вікні написати лист, відповідні поля заповнити адресою адресата, адресами, кому висилати копії, а також темою листа. Щоб відправити лист, треба натиснути кнопку Віправити. На панелях інструментів є кнопки для редагування тексту і роботи з файлами, а також кнопки для задавання таких параметрів:

– приєднання до листа ще одного файлу;
– підтвердження про отримання листа адресатом;
– підтвердження факту прочитання листа адресатом;
– перевірка граматики;
– вибір адреси з бази адрес;
– отримання довідки про програму тощо.

Електронні скриньки розміщуються на спеціальних комп’ютерах – поштових серверах. Для кожної скриньки на поштовому сервері відводиться спеціальне місце. На одному поштовому сервері не може бути двох скриньок

з однаковими назвами. Електронна адреса складається з двох частин, розділених знаком @.

Електронна пошта – засіб спілкування людей, тому вона передбачає дотримання певного етикету:

– починайте текст листа з привітання, завершуйте підписом;

– якщо звертаєтеся до людини, з якою ви особисто не знайомі, назвіть себе;не забудьте вжити слова «будь ласка», якщо звертаєтеся до кого-небудь з проханням;

– подякуйте, якщо хтось допомагає вам;

– слідкуйте за тоном вашого листа, намагайтеся уникати фраз, що можуть стати причиною конфлікту на релігійній, расовій, політичній та іншій основі; не надсилайте в листах неперевірені дані без посилання на їхнє джерело; намагайтеся не допускати граматичних помилок, використовуйте засоби перевірки орфографії, надані поштовою службою.

МОДУЛЬ 2. Інформаційне забезпечення юридичної та правоохоронної діяльності в Україні

Тема 6. Бази даних правової інформації

1. Бази даних правової інформації Верховної Ради України.
2. ІПС «ЛІГА:ЗАКОН».
3. Єдиний державний реєстр нормативно-правових актів.
4. Єдиний реєстр досудових розслідувань.
5. Єдиний державний реєстр судових рішень.
6. Інформаційно-телекомунікаційна система «Інформаційний портал Національної поліції України».

Бази даних правової інформації Верховної Ради України

Бази даних правової інформації орієнтовані на забезпечення правовою інформацією широкого кола користувачів за допомогою інформаційно-пошукових систем «Право», «Законодавство», «Картотека» і «Закони та підзаконні акти України в Інтернет», які дають змогу швидко шукати та аналізувати нормативно-правові документи.

Бази даних систем містять нормативно-правові документи в остаточній редакції із внесеними змінами (у системі «Законодавство» є попередні редакції), зокрема:

- закони, постанови Верховної Ради України, постанови та укази Президії Верховної Ради України, починаючи з 1990 року;
- кодекси;
- укази та розпорядження Президента України;
- постанови та розпорядження Кабінету Міністрів України, починаючи з 1992 року;
- декрети Кабінету Міністрів України;
- документи міністерств і відомств України, зареєстровані в Міністерстві юстиції відповідно до Указу Президента України № 493/92 від 03.10.1992 р. та постанови Кабінету Міністрів України № 731 від 28.12.1992 р.;
- міжнародні угоди;
- документи міністерств і відомств України, які не підлягають реєстрації в Міністерстві юстиції (листи, роз'яснення Національного банку, Державної податкової адміністрації, рішення Конституційного Суду України, постанови Верховного Суду та Вищого господарського суду України тощо).

Системи «Право», «Законодавство», «Картотека» забезпечують:

- пошук документів за реквізитами (назва, номер, дата прийняття, орган видання та тип документа), за ключовими словами та темами (пенсії, боротьба зі злочинністю, податки тощо);
- перегляд, сортування, друкування або виведення у файл переліку знайдених документів;
- перегляд текстів документів у багатовіконному режимі з підсвічуванням ключових слів;
- друкування цілого тексту або будь-яких його частин на принтері;
- контекстний пошук за двома словами (відстань між словами визначається користувачем);
- ведення списків (тематичних папок) користувачів;
- перегляд нормативних актів, пов'язаних з документом (що вносять зміни, вводять у дію, ратифікують, посилаються на даний документ тощо);
- переключення перегляду з одного документа на інший за посиланням у тексті (динамічний гіпертекст);
- перегляд додаткових реквізитів документа (дати набуття або втрати чинності, дати публікації у пресі), перегляд як чинних, так і нечинних документів;
- перегляд структури документа, створення закладок у текстах, власних приміток користувача до документів;
- перегляд статистики бази даних;
- актуалізація бази даних за допомогою спеціальних файлів (блоків поновлення), які передаються користувачам на дискетах або засобами телекомунікацій (електронною поштою, через ftp-сервер мережі Інтернет тощо);
- перегляд результатів попередніх пошуків за різними критеріями, перегляд списків документів, що додавались до бази даних з окремих блоків поновлень;

– одержання довідок про стан системи (обсяг вільного дискового простору, версію системи, обсяг бази даних, номер останнього блока поновлення тощо).

На офіційному порталі Верховної Ради України (ВРУ) за Інтернет-адресою http://www.rada.gov.ua розміщено найповнішу базу даних по законодавству України, включно з усіма законами та постановами Парламенту. Крім того, офіційний портал «Верховна Рада України» подає вичерпну інформацію про поточний склад і структуру ВРУ, зокрема депутатські фракції і групи, комітети й тимчасові комісії, апарат ВРУ, стислі дані про всіх народних депутатів ВРУ від першого до останнього скликання. Правова ІПС «Законодавство України» надає електронні послуги інформаційно-аналітичного забезпечення законотворчої діяльності безкоштовно. Вона дозволяє здійснювати швидкий пошук необхідної інформації і зорієнтована на широке коло користувачів глобальної мережі Інтернет. Офіційний портал доступний українською та англійською мовами.

Інформаційно-пошукова система «ЛІГА: ЗАКОН»

Правовий портал України «ЛІГА: ЗАКОН» є лідером на ринку комерційних правових ІПС. Популярність «Ліга: Закон» зумовлена тим, що вона пропонує широкий вибір систем інформаційно-правового забезпечення: «Ліга: Закон Класик», «Ліга: Закон Юрист», «Ліга: Еліт», «Ліга: Бізнес», «Ліга: Бухгалтер» та ін.

Перевагою системи ЛІГА: ЗАКОН у порівнянні з її аналогами є можливість забезпечення своїм користувачам наступних можливостей:

− допомога в прийнятті ефективних рішень, швидко реагуючи на зміни законодавчої бази, що регламентує їхню діяльність;

− економія часу, засобів і ресурсів при здійсненні пошуку необхідної нормативної інформації, відстеженні не тільки всіх змін і доповнень у чинних правових актах, але і поточної ділової преси;

− зручна, інтуїтивно зрозуміла робота з великими масивами інформації – як нормативноправової, так і довідково-консультаційної;

− широкі можливості для ведення аналітичної роботи з документами (створення і ведення власних добірок документів, рубрикаторів і класифікаторів; установлення характерних позначок у текстах документів і створення власних коментарів до них; установлення зв'язків між документами, створення власних оглядів тощо);

− можливість роботи з оглядами економічної преси з питань оподаткування, бухгалтерського обліку, підприємницької діяльності та ознайомлення з різноманітними довідковими матеріалами;

− можливість створення власних статистичних оглядів і звітів у будь-якому тематичному розрізі й на будь-яку часову глибину;

− робота з актуальною нормативною базою (тексти документів підтримуються щодня в контрольному стані, зберігаючи історію їх зміни і розвитку; динамічно генеруються редакції документа на задану дату);
− можливість створювати й вести свої власні бази даних і здійснювати доступ до сервера системи з територіально віддалених філій і мобільних робочих місць [65].

Системи «ЛІГА: ЗАКОН» – найбільш повне джерело систематизованої і достовірної правової інформації із зручними інструментами для пошуку інформації. Дозволяють швидко знайти і проаналізувати правову інформацію на будь-який момент часу, оцінити ситуацію і прийняти вірне рішення.

Єдиний державний реєстр нормативно-правових актів

Єдиний державний реєстр нормативно-правових актів – це автоматизована система збирання, накопичення та опрацювання актів законодавства, яка складається з еталонного, страхового, робочого, інформаційного фондів та окремого розділу [46].

Користувачами Реєстру є будь-які фізичні, юридичні особи та об’єднання громадян без статусу юридичної особи, які мають доступ до інформації з інформаційного фонду Реєстру через веб-сайт www.reestrnpa.gov.ua, а також які звернулись до Міністерства юстиції України із запитом відповідно до Закону України «Про доступ до публічної інформації» за одержанням інформації з інформаційного фонду Реєстру на паперових носіях.

Структура реєстру:
− *Еталонний фонд Реєстру* – комп'ютерна інформаційна система, призначена для зберігання та обліку еталонних текстів нормативно-правових актів у контрольному стані. Еталонний фонд формується та зберігається в Мін'юсті.
− *Робочий фонд Реєстру* – комп'ютерна інформаційна система, яка підтримує технологію ведення Реєстру і використовується для підготовки та опрацювання текстів нормативно-правових актів при внесенні їх до еталонного фонду Реєстру.
− *Страховий фонд Реєстру* – архівні копії еталонного фонду Реєстру, які зберігаються в Мін'юсті на електронних носіях і призначені для відновлення в автентичній формі еталонного фонду Реєстру у разі його повної або часткової втрати.
− спеціально створена для надання широкому колу користувачів інформації з Реєстру комп'ютерна інформаційна система у формі окремої бази даних, в якій зберігаються копії еталонних текстів нормативно-правових актів.

Переліки нормативно-правових актів, включених до Реєстру, які підлягають опублікуванню в чергових номерах інформаційного бюлетеня «Офіційний вісник України», формуються програмно.

Переліки нормативно-правових актів, включених до Реєстру, які підлягають опублікуванню в інформаційному бюлетені «Офіційний вісник України», передаються до державного підприємства, що належить до сфери управління Міністерства юстиції України, яке забезпечує видання інформаційного бюлетеня «Офіційний вісник України», листами Міністерства юстиції України за підписом заступника Міністра (відповідно до розподілу повноважень між Міністром, першим заступником Міністра, заступниками Міністра).

Єдиний реєстр досудових розслідувань

Єдиний реєстр досудових розслідувань (ЄРДР) – це створена за допомогою автоматизованої системи електронна база даних, відповідно до якої здійснюється збирання, зберігання, захист, облік, пошук, узагальнення даних про кримінальні правопорушення та хід досудового розслідування у кримінальних провадженнях.

ЄРДР запрацював одночасно з набранням чинності КПК – 20 листопада 2012 року.

Досудове розслідування розпочинається з моменту внесення відомостей до Єдиного реєстру досудових розслідувань.

Відомості з реєстру надаються у вигляді витягу.

Реєстр утворений та ведеться відповідно до вимог Кримінального процесуального кодексу України з метою забезпечення:

− реєстрації кримінальних правопорушень (проваджень) та обліку прийнятих під час досудового розслідування рішень, осіб, які їх учинили, та результатів судового провадження;

− оперативного контролю за додержанням законів під час проведення досудового розслідування;

− аналізу стану та структури кримінальних правопорушень, вчинених у державі;

− інформаційно-аналітичного забезпечення правоохоронних органів.

Користувачами Реєстру є:

− керівники органів прокуратури, органів досудового розслідування та органів дізнання;

− прокурори;

− слідчі органів поліції, безпеки, органів, що здійснюють контроль за додержанням податкового законодавства, та Державного бюро розслідувань, детективи Національного бюро;

− дізнавачі підрозділів дізнання органів поліції, безпеки, органів, що здійснюють контроль за додержанням податкового законодавства, та органів

Державного бюро розслідувань, а також уповноважені особи інших підрозділів зазначених органів;

– інші уповноважені особи органів прокуратури, поліції, безпеки, органів, що здійснюють контроль за додержанням податкового законодавства, Державного бюро розслідувань та Національного бюро, які виконують функції з інформаційно-аналітичного забезпечення правоохоронних органів та ведення спеціальних обліків (оперативних, оперативно-облікових, дактилоскопічних тощо) відповідно до чинного законодавства.

До Реєстру вносяться відомості про:

– час та дату надходження заяви, повідомлення про кримінальне правопорушення або виявлення з іншого джерела обставин, що можуть свідчити про вчинення кримінального правопорушення;

– прізвище, ім'я, по батькові (найменування) потерпілого або заявника;

– інше джерело, з якого виявлені обставини, що можуть свідчити про вчинення кримінального правопорушення;

– короткий виклад обставин, що можуть свідчити про вчинення кримінального правопорушення, наведених потерпілим, заявником чи виявлених з іншого джерела;

– попередню правову кваліфікацію кримінального правопорушення із зазначенням статті (частини статті) закону України про кримінальну відповідальність;

– передачу матеріалів та відомостей іншому органу досудового розслідування, дізнання або за місцем проведення досудового розслідування;

– прізвище, ім'я, по батькові керівника органу прокуратури, прокурора, керівника органу досудового розслідування, слідчого, детектива, керівника органу дізнання, дізнавача (уповноваженої особи інших підрозділів), який вніс відомості до Реєстру та/або розпочав досудове розслідування та/або здійснює досудове розслідування чи процесуальне керівництво;

– дату та час затримання особи (звільнення);

– обрання, зміну та скасування запобіжного заходу;

– час та дату повідомлення про підозру, зміну, скасування повідомлення про підозру, особу, яку повідомлено про підозру, правову кваліфікацію кримінального правопорушення, у вчиненні якого підозрюється особа, із зазначенням статті (частини статті) закону України про кримінальну відповідальність;

– час та дату складання повідомлення про підозру, особу, стосовно якої складено повідомлення про підозру, правову кваліфікацію кримінального правопорушення, у вчиненні якого підозрюється особа, із зазначенням статті (частини статті) закону України про кримінальну відповідальність у разі неможливості повідомлення такій особі про підозру з об'єктивних причин;

– юридичну особу, щодо якої можуть застосовуватися заходи кримінально-правового характеру;

– дату та підставу здійснення (скасування) спеціального досудового розслідування;
– зупинення та відновлення досудового розслідування;
– оголошення розшуку підозрюваного;
– об'єднання та виділення матеріалів досудових розслідувань;
– продовження строків тримання під вартою та досудового розслідування;
– встановлені, відшкодовані матеріальні збитки, суми пред'явлених позовів у кримінальному провадженні, вартість арештованого майна;
– закінчення досудового розслідування;
– інші відомості, передбачені в електронних картках.

Єдиний державний реєстр судових рішень

Єдиний державний реєстр судових рішень (*ЄДРСР*) – автоматизована система збирання, зберігання, захисту, обліку, пошуку та надання електронних копій судових рішень. До реєстру вносяться усі рішення судів України у цивільних, адміністративних, господарських справах, справах про адміністративні правопорушення та кримінальних провадженнях.

Внесення судових документів до реєстру складається з трьох етапів:
1. збір судових документів штатним працівником суду і передача їх оператору реєстру;
2. обробка документів оператором;
3. внесення документів до реєстру.

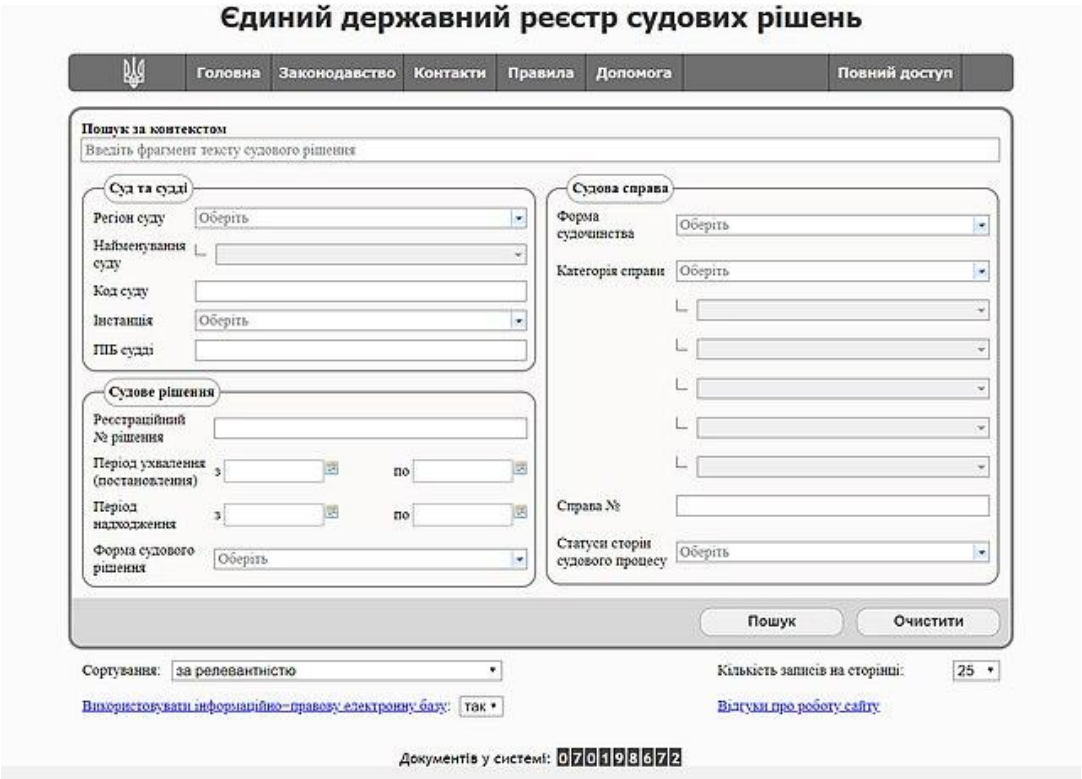


Рис 11. Інтерфейс Єдиного держаного реєстру судових рішень

Обов'язковими для внесення в базу даних є такі реквізити:

1. найменування суду, який ухвалив (постановив) судове рішення;
2. код суду згідно з Довідником статистичних кодів, затвердженим Державною судовою адміністрацією;
3. інстанція, у якій розглядалася справа;
4. форма судочинства (цивільне, кримінальне, господарське, адміністративне);
5. форма судового рішення;
6. дата ухвалення (постановлення) судового рішення;
7. номер та дата судової справи (якщо номер судової справи змінено, додатково зазначається попередній номер та дата судової справи);
8. номер та дата судової справи, рішення у якій переглядається;
9. дата ухвалення (постановлення) судового рішення, що переглядається;
10. найменування та код суду, що ухвалив (постановив) судове рішення, що переглядається, згідно із зазначеним Довідником статистичних кодів;
11. склад суду із зазначенням прізвища та ініціалів судді (суддів);
12. найменування сторін судового процесу (з урахуванням режиму доступу до судових рішень);
13. статус сторін судового процесу (фізична особа, юридична особа, зокрема державний орган, державне підприємство, установа, організація).

Інформаційно-телекомунікаційна система «Інформаційний портал Національної поліції України»

Інформаційно-телекомунікаційна система «Інформаційний портал Національної поліції України» (далі – система ІПНП) – сукупність технічних і програмних засобів, призначених для обробки відомостей, що утворюються у процесі діяльності Національної поліції України та її інформаційно-аналітичного забезпечення. Система ІПНП є складовою частиною єдиної інформаційної системи МВС (далі – ЄІС МВС).

Основними завданнями системи ІПНП є:

1. інформаційно-аналітичне забезпечення діяльності Національної поліції України;
2. забезпечення наповнення та підтримки в актуальному стані інформаційних ресурсів баз (банків) даних, що входять до ЄІС МВС;
3. забезпечення щоденної діяльності органів (закладів, установ) поліції у сфері трудових, фінансових, управлінських відносин, відносин документообігу;
4. забезпечення електронної взаємодії з МВС та іншими органами державної влади.

Система ІПНП призначена для:

- формування інформаційних ресурсів ЄІС МВС;
- обробки інформації, яка утворена в процесі діяльності поліції;

− надання безпосереднього оперативного доступу до інформаційних ресурсів ЄІС МВС;
− генерації інтерфейсів та оброблення тимчасових наборів даних для здійснення інформаційної взаємодії органів (підрозділів) поліції з іншими органами державної влади, органами правопорядку іноземних держав, міжнародними організаціями;
− здійснення пошукових та аналітичних функцій для використання інформації з інформаційних ресурсів (баз даних) поліції, МВС та інших органів державної влади в межах службової діяльності відповідно до рівня доступу і повноважень за запитом або регламентом;
− використання програмних компонентів геоінформаційних підсистем для візуалізації інформації у вигляді електронних карт, автоматичної зміни зображеного образу об'єкта в залежності від зміни його характеристик, зміни масштабу та деталізації картографічної інформації в інформаційних ресурсах;
− забезпечення автоматизації процесів управління силами та засобами поліції;
− забезпечення електронного документообігу в органах (підрозділах) поліції, обміну електронними документами з МВС;
− комплексного захисту інформації та розмежування доступу до інформації, що зберігається в базах даних системи ІПНП.

Складовими системи ІПНП є:

− центральний програмно-технічний комплекс;
− автоматизовані робочі місця користувачів;
− телекомунікаційна мережа доступу;
− комплексна система захисту інформації.

ТЕМА 7. ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ЮРИДИЧНОЇ ТА ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ

1. Інформаційно-аналітична робота в правоохоронних органах
2. Система централізованого управління нарядами поліції «ЦУНАМІ»
3. Поняття «штучний інтелект», як технологія майбутнього
4. Міжнародний досвід використання ШІ правоохоронними органами
5. Можливості використання штучного інтелекту правоохоронними органами України.
6. Особливості використання працівниками Національної поліції України нагрудних відеокамер

Аналітична робота в правоохоронних органах

Інформація в сучасному світі відіграє надзвичайно важливу роль, нею може в окремих випадках може впливати на різноманітні процеси як локального, так і загальнодержавного значення.

Інформація та володіння нею виступає серйозним чинником у системі протидії та запобігання злочинності, оскільки наявність та достовірність її прямо пов’язана із досягненням позитивного результату. В свою чергу, в умовах глобального інформування постає і необхідність здійснення аналітичних операцій, оскільки інформація може бути надана не достовірна або не об’єктивна і саме через це потребує співставлення з іншими фактами, іншими джерелами тощо [31, с.251].

Інформаційно-аналітичне забезпечення посідає дуже важливе місце та є комплексом організаційних, правових і технологічних засобів, які забезпечують процес збирання, отримання, обробки, поширення, аналізу та використання інформаційних ресурсів, необхідних для виконання визначених чинним законодавством завдань і функцій правоохоронних органів.

Органи поліції у своїй роботі використовують інформацію, пов’язану не лише з відомостями про стан публічного порядку і рівня злочинності на певній території, але також і про самі органи та підрозділи, їх сили і засоби.

Поліція в рамках інформаційно-аналітичної діяльності: формує бази (банки) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України; користується базами (банками) даних Міністерства внутрішніх справ України та інших органів державної влади; здійснює інформаційно-пошукову та інформаційно-аналітичну роботу; здійснює інформаційну взаємодію з іншими органами державної влади.

Інформаційна-аналітична робота є елементом організації розслідування злочинів, тобто передбачає пошук, збирання, оцінку, аналіз, узагальнення даних, необхідних для прийняття управлінського чи оперативного рішення та є засобом отримання інформації під час розслідування злочинів.

Основними інформаційними ресурсами, що використовуються в процесі інформаційно-аналітичної роботи у розслідуванні злочинів, є: оперативні обліки, які складаються із оперативно-розшукових, оперативно-профілактичних та оперативно-довідкових обліків; криміналістичні обліки, які складаються з оперативно-пошукових та інформаційно-довідкових колекцій; банки даних кримінологічної, адміністративної, статистичної інформації; банки даних інших міністерств, відомств, підприємств, установ та організацій, які не стосуються безпосередньо боротьби зі злочинністю; банки даних міських і обласних органів влади; об'єкти надання та отримання охоронних послуг; оператори мобільного зв'язку; звернення та заяви громадян, депутатські запити; засоби масової інформації, зокрема Інтернет [3,с.194].

Система централізованого управління нарядами поліції «ЦУНАМІ»

Система централізованого управління нарядами поліції (скорочено – система «ЦУНАМІ») являє собою комплекс апаратних та програмних засобів, а також персоналу, призначений для управління силами й засобами Національної поліції.

Основні компоненти системи "ЦУНАМІ":

Організаційно-управлінський рівень

1.) Центр прийняття повідомлень – служба «102»
1.1. Служба «102»
1.2. Онлайн-сервіс 102kiev.com.ua
1.3. Чергова служба (чергові частини Головних управлінь, аппарату Національної поліції)
2.) Диспетчерський центр управління
3.) Інформаційно-технічний супровід системи.
3.1. Геоінформаційна система (електронна карта міста).
3.2. Система супутникового GPS-позиціювання та мобільного комунікаційного обладнання.
3.3. Система відеоспостереження.
3.4. Система колективного відображення.

Виконавчий рівень

1.) Наряди управління патрульної поліції.
2.) Групи реагування патрульної поліції (ГРПП).
3.) Слідчо-оперативні групи.
4.) Наряди управління поліції охорони.

5.) Чергові частини управлінь, відділів поліції (а також УПО, УПП).
6.) Додаткові сили (дільничні офіцери поліції, працівники управління захисту економіки, кіберполіції, вибухотехнічної служби, кінологічного центру, спеціалісти НДЕКЦ тощо).

Дана система забезпечує користувачів необхідними інформаційними, технічними та аналітичними ресурсами для виконання функціональних обов'язків та прийняття ефективних управлінських рішень. Система фіксує, зберігає та робить доступними для аналізу та контролю повідомлення до ОВС і результати реагування на них. Мета впровадження системи «ЦУНАМІ» обумовлена необхідністю вдосконалення процесу організації діяльності з управління силами й засобами ОВС для ефективного реагування на повідомлення про злочини та події. Досягнення зазначеної мети забезпечується виконанням таких завдань:

1. оптимізація роботи нарядів патрульної поліції, задіяних для охорони громадського порядку в системі єдиної дислокації, слідчо-оперативних груп чергових частин;
2. скорочення часу реагування на повідомлення громадян про злочини та події, попередженню правопорушень й затримання злочинців по «гарячих слідах»;
3. здійснення оперативного контролю за своєчасністю й якістю реагування нарядами патрульної поліції на злочини та правопорушення, дотриманню законності під час виконання службових обов'язків працівниками поліції.

Диспетчер системи «ЦУНАМІ» є оперативним черговим і куратором кожного конкретного райуправління поліції, відповідальним за організацію реагування на злочини та пригоди в районах. До функцій чергових-диспетчерів входить:

1. управління нарядами поліції;
2. отримання інформації з служби «102» та відстеження на електронній карті місць учинення правопорушень;
3. передача даних про правопорушення на планшет конкретного патруля поліції;
4. забезпечення відповідного патруля всією наявною інформацією, що знаходиться у відомчих інформаційних масивах, про заявника та адресу виїзду;
5. координація роботи найближчих вільних нарядів поліції, які залучаються до розкриття злочину по «гарячих слідах», виїзду до заявника, на місце пригоди або в напрямку вірогідного переховування злочинця;
6. контроль часу виїзду наряд)' та відстеження результатів реагування на заяви та повідомлення громадян про злочини, прийняті рішення тощо.

Патруль одержує від диспетчера у формі електронного повідомлення основні дані із заяви, у тому числі номер заявника.

За результатами реагування диспетчер ставить відповідні відмітки. Інформаційна електронна картка залишається у диспетчера на контролі, поки не буде отриманий повний звіт про результати реагування на звернення.

Рис 12. Схема інформаційних потоків системи «ЦУНАМІ»

Автоматизація служби «102» дозволяє операторові одержувати інформацію про абонента ще до моменту підняття трубки:

1. дані про власника телефонного номера;
2. кількість дзвінків, які раніше надходили із цього номера та щодо яких подій;
3. відстеження повторних викликів вже зареєстрованої події;
4. географічне місце (адресу) на електронній карті міста тієї події, про яку було раніше повідомлено;
5. попередження про дзвінки абонементів, які внесені до окермого списку: психічно хворі; телефонні хулігани тощо.

Поняття «штучний інтелект», як технологія майбутнього

Штучний інтелект сьогодні викликає найбільшу кількість багатогранних, підчас дуже суперечливих емоцій, починаючи від активного просування технологій, пов’язаних з його подальшим розвитком, закінчуючи його практично повним запереченням. Як зазначає Джон Маркофф, поштовхом для появи штучного інтелекту стала ера технічного прогресу (1950-ті роки) та персональних комп’ютерів (1970-ті роки) минулого століття. Саме суцільна комп’ютеризація та світ «big data» фактично стали тими, що визначає сьогодні наш розвиток. Він вважає, що саме зараз той переломний момент в світлі розвитку інформатики, програмування, робототехніки, нейробіології та ін., після якого нас

очікує світ машин, які замінюють або перевершують людину за певними якостями [10].

Термін «інтелект» (intelligence) походить від латинського поняття intellectus – «розум». Штучний інтелект (artificial intelligence) розуміється як здатність автоматичних систем брати на себе функції людини, вибирати і приймати оптимальні рішення на основі раніше отриманого життєвого досвіду і аналізу зовнішніх впливів. Будь-який інтелект спирається на діяльність. У свою чергу, діяльність мозку – це мислення. Інтелект і мислення пов'язані багатьма цілями і завданнями: розпізнавання ситуацій, логічний аналіз, планування поведінки. Характерними особливостями інтелекту є здатність до навчання, узагальнення, накопичення досвіду, адаптація до умов, що змінюються в процесі вирішення завдань. Виходячи з самого визначення штучного інтелекту випливає основна проблема у створенні інтелекту: можливість або неможливість моделювання мислення людини [37]. У сучасному розумінні термін «штучний інтелект» – це науковий напрям, в рамках якого ставляться і розв'язуються завдання апаратного і програмного моделювання тих видів людської діяльності, які традиційно вважаються інтелектуальними, тобто потребують певних розумових зусиль.

Вперше термін ШІ використав американський інформатик Джон Маккарті в 1956-му. Його команда є розробником першого ШІ – програми для англійського комп'ютера Ferranti Mark 1, яка могла грати в шахи. Сьогодні ШІ набув набагато ширшого поняття, і ми вже не називаємо гру в шахи на бабусиній кнопковій Nokia ШІ-програмою.

Таким чином, ШІ – надзвичайно узагальнене поняття, і, в ідеалі, – це штучно розроблена система, яка має людські або близькі до людських інтелектуальні здібності і може виконати будь-яке завдання з можливих для homo sapiens.

Поняття ШІ часто вживають у розрізі машинного навчання і штучних нейронних мереж. Тут вже простіше і побільше конкретики. Нейромережі – це форма ШІ, реалізована через програмне забезпечення, яке симулює принципи обміну інформацією між нейронами в мозку людини. Простіше кажучи, штучна нейромережа використовує мережу вузлів для обробки інформації, схожу на нейронну мережу в організмі людини [69].

Отже, штучний інтелект – це штучно створена система, здатна знаходити рішення поставлених перед нею задач не за допомогою наперед заданого алгоритму, а за допомогою власного досвіду, тобто може сама знаходити алгоритм рішення [36].

Міжнародний досвід використання штучного інтелекту правоохоронними органами

Цифрова трансформація суспільства передбачає упровадження комп'ютерних технологій у всі сфери суспільного життя. Сьогодні дуже

актуальним стає залучення інформаційних технологій та технологій штучного інтелекту працівниками органів Національної поліції України до виявлення та розслідування злочинів та робить діяльність правоохоронних органів ефективнішими в їх попередженні.

Основний принцип роботи штучного інтелекту (ШІ) – вивчення наявної інформації з масивів даних. Спеціально написані програми «проганяють» дані, виділяють певні закономірності і на їхній основі роблять висновки, які потім можуть використовуватися людьми для ухвалення рішень [5].

Дослідження, підтримувані ШІ, допомагають бути лідерами в застосуванні штучного інтелекту для задоволення потреб кримінального правосуддя, таких як ідентифікація осіб та їх дій у відеозаписах, пов'язаних зі злочинною діяльністю або громадською безпекою, аналіз ДНК, виявлення вогнепальних поранень і прогнозування злочинності [70].

Відповідно до дослідження, проведеного за замовленням американської Національної довідкової служби з кримінального правосуддя, використання штучного інтелекту допоможе не тільки в затриманні злочинців (наприклад, на підставі систем розпізнавання облич на фото і відео), але і в попередженні злочинів. Зазвичай ця робота лягає на плечі поліції і служб пробації.

Група дослідників проаналізувала понад 340 тисяч ордерів, щоб обчислити ризики повторного порушення, в який проміжок часу це може статися і яка ймовірність того, що злочинець сховається від правоохоронців (якщо він не перебуває під наглядом). Вони сформували алгоритми, які мають допомогти правоохоронним органам у виконанні ордерів та оптимізації ресурсів.

Алгоритми також можуть виявляти злочини проти літніх людей і допомагати припиняти їх. А також – вираховувати потенційних жертв насильницьких злочинів на підставі асоціацій і поведінки. Програмне забезпечення використовує алгоритми в трьох основних напрямках – для оцінки ризику загального рецидивізму, насильницького рецидивізму або можливості сховатися від суду [68].

У Лондоні створена своя система профілактичних заходів проти використання мобільних телефонів за кермом. Щоб зрозуміти, чому дорожній безпеці приділяється так багато уваги в усьому світі, звернемося до офіційних даних: наприклад, у США мобільні телефони стають причиною 70 тисяч ДТП на рік, а у Великобританії розмова по телефону за кермом призводить до одного летального випадку кожні 10 днів. Профілактика ДТП приносить свої плоди, і велике значення тут мають сучасні технології, системи штучного інтелекту.

В Австралії, наприклад, поліція впроваджує нові дорожні камери, призначені для відстеження водіїв, які розмовляють по телефону під час руху. Після успішного тестового періоду, що завершився у жовтні 2018 року, штрафи отримали понад 11 тисяч водіїв. Працює така технологія на основі сенсорних радарних систем, що роблять фотографії водіїв через вітрове скло. Потім фото передаються до нейронної мережі, яка аналізує знімок людини на

предмет наявності мобільного телефону. Неправомірність дій водія можна легко довести на підставі фотографії [36].

З появою iOS 11 користувачам iPhone стала доступною нова вбудована функція «Не турбувати під час водіння». У цьому режимі блокуються вхідні дзвінки і будь-які повідомлення. Ця технологія також доступна на смартфонах з ОС Android.

Компанія Evolv Technology розробила машину безпеки на базі штучного інтелекту, що працює через додаток Evolv Pinpoint і використовує функцію розпізнавання осіб. Ця технологія дозволяє запобігти заворушенням, терактам, забезпеченню безпеки на концертах або у інших місцях масового скупчення людей.

Конструкцію можна встановити на вході у комерційні установи, школи, торгові центри, аеропорти, нічні клуби, ресторани і т.д. Для перевірки людині досить пройти через конструкцію, як через звичайний металошукач. Пропускна можливість такого детектора становить 600-900 осіб на годину. Перевірка проводиться вбудованою камерою, алгоритми Evolv Pinpoint зіставляють особи відвідувачів з особами в списку спостереження, завантаженому у базу даних системи. Якщо з'ясовується, що відвідувач представляє інтерес для поліції або інших служб, його зображення і особисті дані відображаються на планшеті співробітника служби безпеки і підсвічуються червоним. Жовте підсвічування говорить про неперевірену загрозу, тоді профіль перевіряється у реальному часі протягом декількох секунд.

У середньому рівень злочинності при використанні систем безпеки на базі ШІ знижується на 27% протягом першого року їх функціонування. Застосування таких систем економить кошти міського бюджету, дисциплінує суспільство і підвищує рівень комфорту городян [68].

Перспективним для оперативно-розшукової ідентифікації вважається використання відеоінформації з камер спостереження, встановлених на вулицях, камер банкоматів, автомобільних відео реєстраторів тощо.

У нинішніх умовах протидії злочинності та тероризму біометрична ідентифікація за зображенням обличчя опинилася на першому місці серед технологій розпізнавання осіб. Розпізнавання обличчя часто застосовується у поєднанні з іншими біометричними технологіями, як розпізнавання за відбитками пальців. Розпізнавання також застосовується в аеропортах за проходженням митного контролю шляхом порівняння портрета у біометричному паспорті з обличчям особи власника.

Упродовж останнього десятиліття алгоритмами автоматичного розпізнавання обличчя цікавилися фахівці у галузі біометрії. Наприклад OpenFace – це інструментарій з відкритим кодом, що базується на алгоритмі FaceNet для автоматичної ідентифікації обличчя створеної Google. Він був створений та розповсюджений як програмне забезпечення з відкритим кодом Брендоном Амосом у дослідницькій групі Satya в університеті Карнегі Меллона. Головні переваги OpenFace полягають у тому, що він, не

потребуючи значних людських ресурсів, продемонстрував високі показники на еталоні LFW.

OpenFace можна використовувати для ідентифікації злочинців та підозрюваних, для пошуку осіб, які зникли безвісти та для ідентифікації трупів.

Однак жоден із запропонованих проектів поки що не зміг надати результати, які можна порівняти з ручним розпізнаванням обличчя людини.

Біометричну ідентифікацію за формою обличчя часто використовує поліція. У країнах Євросоюзу суворо контролюється правомірність їх застосування.

Як приклад, «Людину в капелюсі», яку було звинувачено в серії терактів у 2016 році, викрили завдяки програмному забезпеченню з інтегрованою системою розпізнавання осіб ФБР.

У 2019 році ФБР США оголосило про успішний запуск в експлуатацію системи розпізнавання нового покоління Next Generation Identification (NGI), яка збирає, обробляє, і ідентифікує зображення обличчя, райдужну оболонку очей, татуювання та відбитки пальців.

Цифрових рішень з безпеки безліч, як приклад можна привести розробку компанії Digital Barriers – додаток EdgeVis Shield. Він об'єднує сейсмічні, бездротові і оптичні давачі з телевізійними камерами і відеоаналітикою, надаючи максимально повний огляд території, яка охороняється. Система спрацьовує при виявленні проникнення, вторгнення фіксується відеокамерами в реальному часі. Робота системи підпорядковується алгоритму: якщо транспортний засіб або людина потрапляє у заборонену зону або залишається там довше, ніж дозволено, спрацьовує сигнал тривоги.

Сучасні глобальні системи безпеки реагують на погодні умови, тремтіння камери, тіні і навіть ворушіння листя, використовують технологію розпізнавання осіб. Сейсмічні давачі вміють розрізняти транспортні засоби або людей. Інформацію з камер можна прослуховувати і переглядати у декількох режимах: по мережі бездротового зв'язку, по військовій мережі, у вигляді радіосигналу або по Satcom.

У Китаї з поліцією в напрямку застосування і розвитку штучного інтелекту у сфері безпеки співпрацює низка передових компаній зі світовим ім'ям, які займаються розробками в галузі штучного інтелекту.

Однією з таких компаній є китайська компанія «Cloudwalk» з Гуанчжоу.

Завдяки технології розпізнавання облич від «Cloudwalk» правоохоронним органам Китаю за останні 4 роки вдалось затримати 10 тис. підозрюваних. Система накопичила понад 100 млрд зразків зображень облич для ідентифікації. Щодня проводиться понад 1 млрд порівнянь. «Cloudwalk» змогла досягти точності в розпізнаванні облич у натовпі 99,8 % з 91 ракурсу.

Вона ідентифікує загримованих і дуже щільно вдягнутих людей за частки секунди. Фірма IHS Markit прогнозує, що до кінця 2020 р. в Китаї

буде встановлено 450 млн нових камер. Завдяки розгортанню нової мережі масового спостереження в Ічжуані під назвою Sharp Eyes у разі виникнення нестандартної обстановки система автоматично надішле сигнал тривоги [73].

Подія буде відображена на великому екрані, і працівники поліції негайно прибудуть на місце події. На території у 18 км^2 встановлено більше двох тисяч камер високої роздільної здатності, які мають можливість ідентифікувати державні знаки й типи автомобілів і розпізнавати обличчя людей. Нагрудні камери патрульних передають потік відеоінформації на центральний пункт управління для його миттєвого аналізу.

Кожен охочий може встановити мобільний додаток на смартфоні, з якого інформація може бути передана в центр управління. Також смартфон можна підключити до потоку інформації з відеокамер або з центрального пункту управління. Кількість крадіжок зі зломом і викрадень автомобілів, за словами влади міста, зменшилася порівняно з періодом до установки системи на 76 %.

Кількість кримінальних справ скоротилася на 39 %. Система здатна розпізнавати поведінкові ознаки людей і прогнозувати можливі їх дії, заздалегідь підготувати патрульного до можливої реакції підозрюваного. Для забезпечення безпеки кордону Євросоюз також запроваджує нові системи інтелектуального відеоконтролю. Розробляється проєкт IBORDERCTRL.

Система інтелектуального відеоконтролю покликана полегшити роботу прикордонників щодо виявлення нелегальних мігрантів, терористів, контрабандистів, наркокур'єрів тощо. Мандрівникові необхідно за допомогою онлайн-додатку відповісти на питання комп'ютерної програми, використовуючи веб-камеру. Система автоматично визначає етнічну належність, мову і стать мандрівника. Далі програма аналізує його мікрорухи, щоб з'ясувати, чи бреше він. На мандрівників, які намагаються обдурити систему, чекає більш ретельний контроль. Решта пройде кордон за спрощеною програмою.

У США вогнепальна зброя перебуває у вільному доступі. У цій країні є дуже великим відсоток злочинів із використанням вогнепальної зброї. Тому в США застосовується система ShotSpotter [38].

Система має фіксувати постріли. У населених пунктах розміщено акустичні датчики та камери. За допомогою штучного інтелекту й акустичних датчиків, розташованих на деякій відстані та пов'язаних між собою через мережу Інтернет, ShotSpotter визначає координати місця події. Крім того, за характером пострілу встановлюється тип вогнепальної зброї.

Після фіксації пострілу система визначає місце події, яке відображається на інтерактивній мапі. Запускаються камери відеоспостереження, розташовані в місці, де були зафіксовані звуки пострілів. Проводиться зйомка з камер відеоспостереження, які перемішують напрям спостереження у бік місця стрільби. Інформація про події зберігається в електронному журналі для проведення розслідування.

Штучний інтелект все ширше розповсюджується у правоохоронних системах різних держав. Наразі рано передбачати чи замінять повністю алгоритми більшість повноважень правоохоронців, проте окремі переваги штучного інтелекту вже були підтверджені. Зокрема, це можливість аналізу та обробки даних із сотень справ за короткий проміжок часу. Скоріш за все, цю властивість використовуватимуть і надалі перш за все у Сполучених Штатах та державах Європейського союзу з умовою дискреційних повноважень правоохоронців щодо застосування такого аналізу. Важливим аспектом є також прийняття нормативних актів, що регулюють використання штучних технологій та легітимізацію такого використання.

Можливості використання штучного інтелекту правоохоронними органами України

Застосування нових інформаційних технологій і розвинених засобів комунікацій різнопланове і має тенденцію до зростання. У свою чергу концептуальним етапом у розвитку інформаційних технологій є створення і використання інтелектуальних систем в державному управлінні, будівництві, економіці, навчальному процесі та багатьох інших галузях життєдіяльності людини.

Не винятком є діяльність правоохоронних органів України у сфері протидії злочинності. Розглянемо окремі особливості інтелектуальних систем, що використовуються в правоохоронних органах, а саме:

1) прикладом інтелектуальної системи може бути Інтегрована інформаційно-пошукова систему органів внутрішніх справ України (ІІПС), що призначена для підтримки оперативно-службової діяльності органів і підрозділів внутрішніх справ, інших взаємодіючих підрозділів правоохоронних органів, суттєвого зміцнення їх спроможності у протидії та профілактиці злочинності, яка потребує розвинення та удосконалення в Єдину комп'ютерну інформаційну систему правоохоронних органів з питань боротьби зі злочинністю;

2) інформаційно-довідкове забезпечення правоохоронної діяльності. Цей напрямок розвинення ІС пов'язаний з появою геоінформаційних систем (ГІС), які надають інформацію про просторове розміщення об'єктів з використанням карт або планів;

3) створення спеціалізованих інформаційних інтелектуальних систем оперативно-розшукового призначення. У цьому напрямку використання ІС ефективним вважається розробка автоматизованої системи проведення оперативно-розшукових заходів та негласних слідчих (розшукових) дій у телекомунікаційних мережах загального користування за аналогією до американських «ЕШЕЛОН» («Eche1оп») та «DCS-1000», європейської системи «RES»;

4) розвинення інтелектуальних систем відео спостереження; Функціональність всього об'єктного програмного забезпечення інтелектуальних систем відеоспостереження поділяється на дві великі групи: розпізнавання та класифікація об'єктів відеоспостереження; відстеження шляху об'єкта відеоспостереження;

5) охорона об’єктів. До цього виду ІС можна віднести системи централізовооі охорони об'єктів «Орлан», «КРОНОС», «АІ-Грифон» тощо, які по суті представляють комплекс технічних засобів і програмного забезпечення для централізованого спостереження за станом пристроїв охоронної та пожежної сигналізація з використанням стільникової мережі GSM-900/1800 та проводових ліній АТС;

6) створення відомчих спеціалізованих інтелектуальних інформаційних систем. Прикладами можуть бути: для поліції – автоматизовані дактилоскопічні інформаційні системи (АДІС «Сонда», «Дакто-2000», «Морфо» – Франція, «Принтрак» – США, «NEX» – Японія тощо); для прикордонної служби – Інтегровані інформаційні системи «Аркан» та «Гарт»; для міністерства доходів і зборів – багатофункціональна комплексна інформаційна система «Електронна митниця»;

7) впровадження та розробка інтелектуальних інформаційних освітніх систем: моделювання знань, комунікації, інтерпретації, самовдосконалення; взаємодії [19].

Сьогодні правоохоронні органи України для виконання різних завдань широко застосовують системи відеоспостереження, які належать силовим структурам, а також ті, що перебувають у приватній власності. Застосування відеоспостереження в діяльності поліції регламентується законами України, наказами та інструкціями Міністерства внутрішніх справ і НП України.

Відеоспостереження ведеться спираючись на:

− Закон України «Про Національну поліцію»;

− Про затвердження Інструкції із застосування органами та підрозділами поліції технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, засобів фото- і кінозйомки, відеозапису;

Алгоритм першочергових дій оператора відділу служби 102, диспетчера, оперативних чергових ГУНП та територіальних підрозділів поліції, а також нарядів поліції у разі отримання повідомлення про правопорушення метою попередження, виявлення і фіксації правопорушень, а також для забезпечення громадського порядку, безпеки громадян, охорони власності та дотримання правил дорожнього руху.

Упровадження систем відеоспостереження – це вагомий чинник, який суттєво впливає на рівень злочинності в країні та створює безпечні умови життя громадян, значною мірою сприяє організації безпечного середовища, профілактиці правопорушень та їх розкриттю. Наявність і використання систем відеоспостереження сприяє позитивній динаміці розкриття злочинів і запобіганню правопорушенням за всіма напрямками.

Протягом 2019 р. лише в м. Київ за допомогою відеокамер розкрито понад 3500 правопорушень. Використання системи відеоспостереження сприяло зниженню загального рівня злочинності в публічних місцях.

Сьогодні в Україні не створено єдиної системи відеоспостереження. У різних областях нашої держави і в різних структурних підрозділах Національної поліції України існують самостійні системи відеоспостереження, які поряд із сучасними використовують досить застарілі технології та обладнання. Національна поліція України застосовує портативні відеореєстратори, системи відеоспостереження, встановлені на службових транспортних засобах, автомобільні системи, стаціонарні системи, а також засоби відеозапису на безпілотних літальних апаратах (БпЛА). Патрульна поліція України використовує нагрудні відеокамери (відеореєстратори), системи відеоспостереження, встановлені на службових транспортних засобах, і стаціонарні системи відеоспостереження.

Найбільш сучасною системою відеоспостереження, із запроваджених в Україні, вважається UASC, що належить до Єдиного аналітичного сервісного центру Головного управління Національної поліції в Донецькій області [32].

В UASC уже використовують інтелектуальні відеокамери, які являють собою окремий апаратно-програмний комплекс. Вона може діяти самостійно або в межах внутрішньої підмережі з такими ж комплексами. Камера має самостійні аналітичні функції, які спираються на програмні датчики руху, функції інфрачервоного спостереження, вимірювання швидкості та інші детектори, які можуть подавати сигнал тривоги. Крім того, камера передає потокову інформацію до основного центру UASC, де проводиться більш глибокий аналітичний аналіз.

Однією з функцій UASC є розпізнавання та пошук номерів автомобілів, які перебувають у розшуку. Система проводить ідентифікацію автомобіля, на який встановлено державний номер, і виявляє відповідність його номера згідно з реєстрацією.

Система має можливість не лише розпізнавати державні номери автомобілів, а й визначати тип і марку автомобіля та його колір. Використовуючи вказані ознаки, можна перевірити, чи перебує автомобіль у розшуку та чи відповідає державний номер автомобіля, подивитись його реєстраційні документи, ідентифікувати осіб, які знаходяться на передньому сидінні.

Система також виявляє скупчення людей, може фіксувати їх неадекватну поведінку, розпізнає заборонений або нетиповий рух автотранспорту, фіксує перетин забороненої зони або перетинання візуальної лінії, реагує на прохід людей у заданому напрямі, ідентифікує події в умовах дорожнього руху, виявляє щільність потоку, затори, масове скупчення автотранспорту, реагує на появу людей у зоні спостереження, може виявляти залишення або зникнення предметів [42].

У Харкові міська влада спільно з усіма силовими структурами розпочала створення єдиної системи відеоспостереження в межах

масштабного проєкту «Безпечне місто». Система повинна об'єднати кілька тисяч відеокамер на базі програмної платформи для системи відеоспостереження «Milestone». До створення системи долучають китайську компанію Huawei.

Позитивним досвідом у розробленні цього проєкту є уникнення традиційних проблем під час створення схожих систем. Зазвичай, у разі розвитку системи безпеки у великих містах нарощують кількість серверів, кожен з яких охоплює групу з кількох десятків або сотень відеокамер, створюються розподілені системи відеоспостереження. У результаті експлуатації таких систем виникають проблеми синхронізації та часті відмови, а їх обслуговування багато коштує. Для виключення таких проблем складові системи «Безпечне місто» будуть розгортатися на базі централізованих систем із використанням хмарної інфраструктури в дата-центрах.

Система «Безпечне місто» повинна відіграти позитивну роль у профілактиці і розслідуваннях ДТП, підтриманні правопорядку в громадських місцях та розвантаженні транспортних магістралей, стати потужним стримуючим фактором для зловмисників. У структурі апарату НП України створено Управління організації діяльності підрозділів поліції на воді та повітряної підтримки (УПВП). Його запроваджено для організації, координації та контролю службової діяльності підрозділів поліції на воді та забезпечення повітряної підтримки підрозділів НП України.

Стрімкий розвиток безпілотних літальних апаратів (БпЛА) призвів до появи специфічних злочинів, пов'язаних із використанням цієї техніки, від вторгнення у приватне життя громадян до використання дронів, оснащених вибуховими пристроями та вогнепальною зброєю. Створення УПВП було викликано такими новими, нетрадиційними вимогами до безпеки громадян. Розвиток і використання нових сил і засобів такого типу повинні забезпечувати виконання завдань, покладених на НП України, зокрема протидії злочинності, підтримання публічної безпеки і порядку, сприяння в ліквідації надзвичайних ситуацій, захисту державного кордону.

Підрозділи поліції застосовують БпЛА для:

- висотного спостереження під час проведення масових святкувань, політичних демонстрацій, спортивних заходів, а також під час припинення масових заворушень;
- висотного спостереження в разі загрози нападу на стратегічні об'єкти та об'єкти, які перебувають під охороною;
- виявлення злочинів та адміністративних правопорушень;
- організації відеодокументування;
- забезпечення зв'язку й управління наземними нарядами поліції;
- організації взаємодії підрозділів поліції з іншими силовими структурами;
- забезпечення та контролю безпеки дорожнього руху;

– проведення спостереження під час здійснення оперативних заходів, відстеження оперативної обстановки під час виконання службових завдань;
– пошуку підозрюваних, які намагаються сховатись;
– пошуку зниклих людей.

Особливості використання працівниками національної поліції України нагрудних відеокамер

Працівників патрульної поліції оснащено нагрудними камерами (відеореєстраторами), наявність яких розглядається ними як засіб захистити себе від упереджених заяв щодо їхньої неправомірної поведінки.

Персональний відеореєстратор є важливим елементом діяльності патрульного поліцейського. Використання нагрудних відеокамер (персональних відеореєстраторів) є превентивним поліцейським заходом та одним з елементів, що дозволяє продемонструвати чесність, відкритість і антикорупційну спрямованість діяльності патрульної поліції. Крім того відеореєстратор виконує профілактичну функцію. Його наявність стримує громадян (за винятком особливо зухвалих і цілком неадекватних осіб) від учинення деяких протиправних дій. Ведення відеозапису працює як психологічний стримуючий фактор відносно більшості правопорушників. Відеореєстратор є засобом об'єктивного контролю за місцем подій, відеозапис з місця події – це рівною мірою контроль дій патрульного та документальне підтвердження правомірності його вимог і вжитих заходів.

Метою використання персональних відеореєстраторів працівниками патрульної поліції є:
– підвищення відповідальності працівників патрульної поліції під час виконання службових обов'язків;
– підвищення рівня довіри суспільства до працівників патрульної поліції;
– підвищення рівня захисту прав і свобод людини та громадянина;
– попередження випадків невиправданого застосування фізичної сили, спеціальних засобів і вогнепальної зброї працівниками патрульної поліції та/або щодо працівників патрульної поліції;
– забезпечення об'єктивного розгляду справ уповноваженими органами шляхом створення додаткових належних доказів;
– підвищення відкритості патрульної поліції;

– забезпечення об’єктивного розгляду скарг на рішення, дії чи бездіяльність працівників патрульної поліції, зменшення кількості безпідставних скарг;
– запобігання конфліктним ситуаціям [19, с.6-7].

Використання нагрудних відеореєстраторів відбувається згідно «Інструкції із застосування органами та підрозділами поліції технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, засобів фото- і кінозйомки, відеозапису». Портативні відеореєстратори та карти пам’яті зберігаються в приміщеннях органів, підрозділів поліції та видаються поліцейському під підпис у журналі обліку видачі, повернення портативного відеореєстратора та карт пам’яті, копіювання цифрової інформації, який зберігається в органі, підрозділі поліції.

Під час здійснення повноважень поліцейськими портативний відеореєстратор закріплюється на його форменому одязі на грудях (ближче до плечового суглоба) так, щоб не створювати перешкод діям поліцейського. У випадках, пов’язаних з необхідністю якісної фіксації подій, поліцейські можуть тримати портативний відеореєстратор у руках. Дозволяється закріплення портативного відеореєстратора на екіпіруванні (шоломі) або зброї, якщо їх конструкцією передбачені відповідні кріплення.

Включення портативного відеореєстратора відбувається з моменту початку виконання службових обов’язків та/або спеціальної поліцейської операції, а відеозйомка ведеться безперервно до її завершення, крім випадків, пов’язаних з виникненням у поліцейського особистого приватного становища (відвідування вбиральні, перерви для приймання їжі тощо). У процесі включення портативного відеореєстратора поліцейський переконується в точності встановлених на пристрої дати та часу.

Під час здійснення повноважень поліцейський забезпечує збереження та належні умови експлуатації виданого йому портативного відеореєстратора та не допускає його розряджання.

У разі пошкодження портативного відеореєстратора поліцейський негайно доповідає про це відповідальній особі та керівнику органу, підрозділу поліції.

Після прибуття до місця постійної дислокації портативний відеореєстратор або карта пам’яті передається відповідальній особі.

Під час приймання портативного відеореєстратора відповідальна особа проводить його візуальний огляд та за відсутності видимих пошкоджень приймає під підпис зазначений портативний відеореєстратор або карту пам’яті [45].

Плани семінарських занять

Семінарське заняття № 1

Тема: Правова інформатика і правова інформація. Правові інформаційні системи і підсистеми

ПЛАН

1. Поняття правової інформації та правової інформатики
2. Інформаційні технології та інформаційні системи.
3. Правові інформаційні системи та підсистеми:
    1) ІПС «Законодавство України (сайт Верховної Ради України)»
    2) Інформаційно-пошукова система LIGA: Закон
    3) Інформаційний портал Національної поліції України

РЕКОМЕДОВАНА ЛІТЕРАТУРА

1. Благута Р.І., Мовчан А.В. Новітні технології у розслідуванні злочинів: сучасний стан і проблеми використання: монографія. Львів: ЛьвДУВС, 2020. 256 с.
2. Використання інформаційно-пошукових систем в діяльності поліції. Правові інформаційно-пошукові системи.
URL. https://arm.naiau.kiev.ua/books/inform_tekhnolohii/lection/lec3.html
3. Закон України «Про інформацію».
URL. https://zakon.rada.gov.ua/laws/show/2657-12#Text
4. Закон України «Про Національну поліцію».
URL. https://zakon.rada.gov.ua/laws/show/580-19#Text
5. Косиченко О.О. Правові інформаційні ресурси Інтернет: довідник. – Дніпро: ДДУВС, 2017. – 92 с.
6. Правова інформація та комп'ютерні технології в юридичній діяльності: навч. посібник. / В.Г. Іванов, С.М. Іванов, В.В. Карасюк та ін.; за заг.ред. В.Г. Іванова. – 4-те вид., змін. І доп. Х.: Право, 2014. 240 с.
7. Сезонова І. К. Інформатика для правоохоронців: навч. посіб./ І. К. Сезонова; МВС України, Харк. нац. ун-т внутр. справ, 2015. 182 с.
8. О.В. Співаковський, М.І. Шерман, В.М. Стратонов, В.В. Лапінський Інформаційні технології в юридичній діяльності: базовий курс: [навчальний посібник]. Херсон: ХДУ, 2012. 220 с.

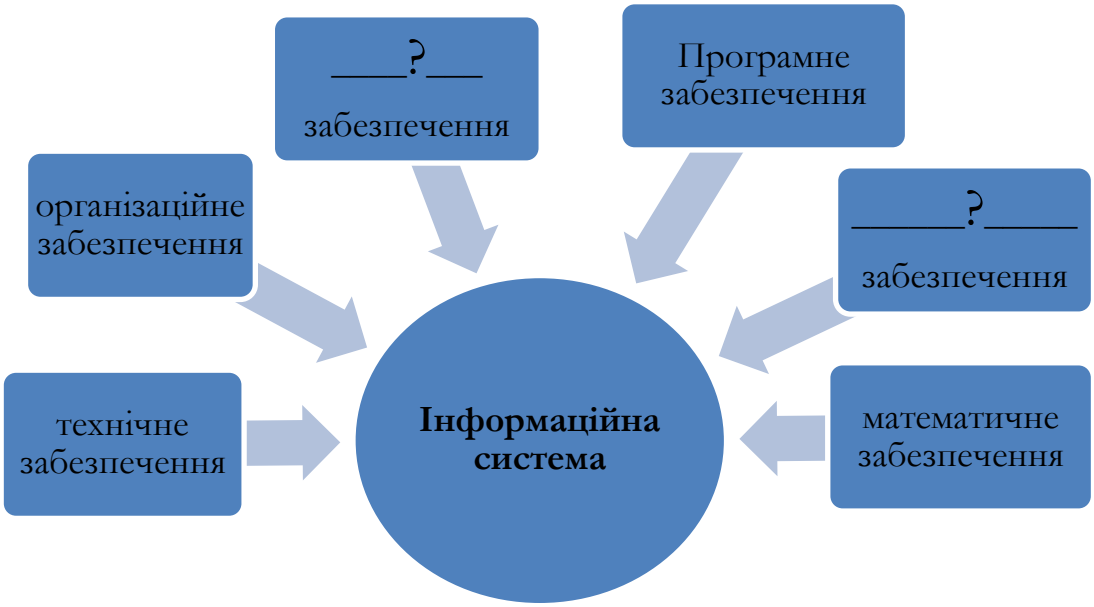
Завдання до семінарського заняття

Завдання № 1. Завантажте ІПС «Законодавство України (сайт Верховної Ради України) https://zakon.rada.gov.ua/laws, занотуйте:

ст.17. Правова інформація – це……..

Ст.18. Статистична інформація – ……

Ст.21. Види інформації з обмеженим доступом:
Конфіденційна інформація – це …….
Завдання № 2. Як ви розумієте поняття «інформаційна система»?
Завдання № 3. Яких підсистем інформаційної системи не вистачає? Вкажіть їх у прямокутниках



Завдання № 4. Завантажте Інформаційно-пошукову систему LIGA: Закон https://ips.ligazakon.net/resource/main_documents?q=*. Знайдіть у пошуку Наказ № 676 «Про затвердження Положення про інформаційно-телекомунікаційну систему «Інформаційний портал Національної поліції України».
Завдання № 5. З якою метою створена Інформаційно-телекомунікаційна система "Інформаційний портал Національної поліції України"? Дайте визначення поняттю.
ІПНП – це ……..
Завдання № 6. Вкажіть призначення та структуру ІПНП
Призначення ІПНП _____
*Складовими системи ІПНП є:*_____

Семінарське заняття № 2
Тема: Захист правової комп'ютерної інформації

ПЛАН

1. Загальне уявлення про інформаційну безпеку
2. Види загроз для комп'ютерної інформації
3. Поняття комп'ютерні злочини. Визначення, класифікація, аналіз та фіксація слідів комп'ютерних злочинів
4. Технологічні, організаційні, правові заходи захисту даних
5. Кримінальна відповідальність щодо злочинів у сфері використання комп'ютерів
6. Засоби протидії загрозам для комп'ютерної інформації

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Іванов В. Г. Основи інформатики та обчислювальної техніки: підручник/ В. Г. Іванов, В. В. Карасюк, М. В. Гвозденко; за заг. ред. В.Г. Іванова. Х.: Право, 2015. 312 с.
2. О.В. Співаковський, М.І. Шерман, В.М. Стратонов, В.В. Лапінський Інформаційні технології в юридичній діяльності: базовий курс: [навчальний посібник]. Херсон: ХДУ, 2012. 220 с.
3. Правова інформація та комп'ютерні технології в юридичній діяльності: навч. посібник/ В.Г. Іванов, С.М. Іванов, В.В. Карасюк та ін.; за заг.ред. В.Г. Іванова. – 4-те вид., змін. І доп. Х.: Право, 2014. 240 с.
4. Сезонова І. К. Інформатика для правоохоронців: навч. посіб/ І. К. Сезонова; МВС України, Харк. нац. ун-т внутр. справ, 2015. 182 с.
5. Загальне уявлення про інформаційну безпеку. URL. http://mego.info/матеріал/41-загальне-уявлення-про-інформаційну-безпеку

Завдання до семінарського заняття

1. Завантажте ІПС «Законодавство України (сайт Верховної ради України), знайдіть Закон України «Про інформацію». Із ст. 1. занотуйте поняття захист інформації.
2. Завантажте ІПС «Законодавство України (сайт Верховної ради України), Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». Із ст. 1 занотуйте поняття «захист інформації в системі», «криптографічний захист інформації», «технічний захист інформації».
3. Які існують види загроз для комп'ютерної інформації?
4. У чому полягає негативний вплив програм вірусів на комп'ютерні дані з точки зору інформаційної безпеки?
5. Які основні заходи вживаються для протидії загрозам комп'ютерної інформації?

6. Сформулюйте поняття «комп'ютерний злочин».
7. Розгляньте систему та класифікацію кіберзлочинів.
8. Кримінальна відповідальність щодо злочинів у сфері використання комп'ютерів.

Семінарське заняття № 3

Тема: Захист правової комп'ютерної інформації. Технічний захист інформації. Криптографічні методи захисту інформації

ПЛАН

1. Засоби та методи захисту інформації
2. Правовий захист інформації
3. Технічний захист інформації
4. Види шифрування інформації: симетричні і асиметричні
5. Поняття «криптографічний захист інформації».
6. Методи криптографічного захисту інформації

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Вакалюк Т.А. Захист інформації в комп'ютерних системах. Навчально-методичний посібник для студентів напряму 6.040302 Інформатика. Житомир: Вид-во ЖДУ, 2013. 136 с.
2. Ємець В., Мельник А., Попович Р. Сучасна криптографія. Основні поняття. Львів, БаК, 2003. 144 с.
3. Електронне урядування та електронна демократія: навч. посіб.: у 15 ч./ за заг. ред. А.І. Семенченка, В.М. Дрешпака. К., 2017. Частина 13: Захист інформації в системах електронного урядування/ [О.М. Хошаба]. К.: ФОП Москаленко О. М., 2017. 72 с.
4. Остапов С.Е. Технології захисту інформації: навч. посіб. /С.Е. Остапов, С.П. Євсеєв, О.Г. Король. Х.: ХНЕУ, 2013. 476 с.
5. Технології захисту інформації. URL. https://www.uzhnu.edu.ua/uk/infocentre/get/4186

Семінарське заняття № 4

Тема: технічне та юридичне забезпечення електронного підпису

ПЛАН

1. Поняття про електронні документи та електронний документообіг (Закон України «Про електронні документи та електронний документообіг»)
2. Поняття «електронного підпису та електронної печатки» (Закон України «Про електронні довірчі послуги»)
3. Електронний підпис та електронний цифровий підпис

4. Електронний бізнес та електронна комерція
5. Симетричні й несиметричні методи шифрування
6. Вимоги до створення і впровадження єдиної системи електронного документообігу в Міністерстві внутрішніх справ України та центральних органах виконавчої влади, діяльність яких спрямовується і координується Кабінетом Міністрів України через Міністра внутрішніх справ України (СЕД системи МВС)

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Роз’яснення щодо скасування дії ЕЦП. URL. https://dp.tax.gov.ua/media-ark/news-ark/439706.html
2. Про Кваліфікований електронний підпис (КЕП) на захищених носіях: роз'яснення та відповіді. URL. https://intelserv.net.ua/news/material/id/650
3. Що таке електронні довірчі послуги? – роз'яснення від Мін'юсту. URL. https://news.dtkt.ua/accounting/automation/51478
4. Вимоги до створення і впровадження єдиної системи електронного документообігу в Міністерстві внутрішніх справ України та центральних органах виконавчої влади, діяльність яких спрямовується і координується Кабінетом Міністрів України через Міністра внутрішніх справ України (Шифр – СЕД системи МВС).
URL. https://mvs.gov.ua/upload/file/vimogi_do_sed_sistemi_mvs_363.pdf

Семінарське заняття № 5
Тема: Мережні інформаційні технології

ПЛАН

1. Основні принципи, методи і властивості інформаційних та комунікаційних технологій
2. Класифікація комп’ютерних мереж
3. Пошук інформації в мережі Інтернет
4. Структура та принципи створення хмарних сховищ даних. Хмарні технології
5. Засоби для інтерактивного спілкування в Інтернеті
6. Сучасні системи авторизації (цифрові, графічні та інші)
7. Електронна пошта

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Г.Г. Швачич, В.В. Толстой, Л.М. Петречук, Ю.С. Іващенко, О.А. Гуляєва, О.В. Соболенко. Сучасні інформаційно-комунікаційні технології: Навчальний посібник. Дніпро: НМетАУ, 2017. 230 с. URL. file:///C:/Users/test/Desktop/ikt_tutor.pdf

2. Електронна пошта та інтерактивне спілкування. URL. http://elektronapochtacpilkyv.blogspot.com/p/blog-page_80.html
3. Інтерактивне спілкування. URL. http://stud-msk.ho.ua/inf/72.htm
4. Інформаційні й комунікаційні технології. URL. https://www.ua5.org/svit/281-nformacjjn-jj-komunkacjjn-tekhnolog.html
5. Класифікація комп'ютерних мереж. URL. https://comp-net.at.ua/index/klasifikacija_komp_juternikh_merezh/0-4
6. Комп'ютерні мережі. Основні терміни класифікації. URL. https://sites.google.com/site/mijsajtmerezainternet/komputerni-merezi-osnovni-termini-klasifikaciie
7. Поняття інтерактивного спілкування.
URL. http://shmedu.at.ua/MM/Inform/IS.pdf
8. Пошук інформації у мережі. URL. http://mego.info/матеріал/84-пошук-інформації-у-мережі
9. Технологія пошуку інформації засобами мережі Інтернет: основні способи пошуку інформації в Інтернеті. URL. https://disted.edu.vn.ua/courses/learn/3121
10. Хмарні технології.
URL. https://sites.google.com/site/navcalnapraktikakitvoin/lekciie/lekcia-hmarni-tehnologiie

Семінарське заняття № 6

Тема: Бази даних правової інформації

ПЛАН

1. Бази даних правової інформації Верховної Ради України.
2. ІПС «ЛІГА:ЗАКОН».
3. Єдиний державний реєстр нормативно-правових актів.
4. Єдиний реєстр досудових розслідувань.
5. Єдиний державний реєстр судових рішень.
6. Інформаційно-телекомунікаційна система «Інформаційний портал Національної поліції України».

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Єдиний реєстр досудових розслідувань.
URL. https://uk.wikipedia.org/wiki/Єдиний_реєстр_досудових_розслідувань
2. Єдиний державний реєстр нормативно-правових актів. URL. https://uk.wikipedia.org/wiki/Єдиний_державний_реєстр_нормативно-правових_актів
3. Інформаційно-аналітичне забезпечення законотворчої та правозастосовної діяльності. URL. http://mego.info/матеріал/глава-6-

інформаційно-аналітичне-забезпечення-законотворчої-та-правозастосовної-діяльності.
4. Інформаційне забезпечення професійної діяльності: навч. посібник/ І.В. Краснобрижий, С.О. Прокопов, Е.В. Рижков. Дніпро: ДДУВС, 2018. 220 с.
5. Кримінальний процесуальний Кодекс України. URL. http://search.ligazakon.ua/l_doc2.nsf/link1/T124651.html.
6. Правова інформація та комп'ютерні технології в юридичній діяльності: навч. посібник / В.Г. Іванов, С.М. Іванов, В.В. Карасюк та ін.; за заг.ред. В.Г. Іванова. – 4-те вид., змін. І доп. Х.: Право, 2014. 240 с.
7. Про затвердження Інструкції з формування та ведення інформаційної підсистеми «Єдиний облік» інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України». URL. http://search.ligazakon.ua/l_doc2.nsf/link1/RE33710.html

Семінарське заняття № 7

Тема: Інформаційно-аналітичне забезпечення юридичної та правозастосовної діяльності

ПЛАН

1. Комп'ютерна мережа Верховної Ради України
2. Загальноправові бази даних
3. Автоматизована інформаційно-пошукова система «Нормативні акти України»
4. Всесвітня електронна мережа правових документів
5. Організація пошуку працівниками Національної поліції у відкритих джерелах мережі Інтернет

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Аналітична робота в органах внутрішніх справ. URL.https://libroos.io.ua/s30219/analitichna_robota_v_organah_vnutrishnih_sprav
2. Інформаційне забезпечення професійної діяльності : навч. посібник / І.В. Краснобрижий, С.О. Прокопов, Е.В. Рижков. Дніпро: ДДУВС, 2018. 220 с.
3. Правова інформація та комп'ютерні технології в юридичній діяльності: навч. посібник. / В.Г. Іванов, С.М. Іванов, В.В. Карасюк та ін.; за заг.ред. В.Г. Іванова. – 4-те вид., змін. І доп. Х.: Право, 2014. 240 с.

Семінарське заняття № 8

Тема: Інформаційно-аналітичне забезпечення юридичної та правоохоронної діяльності

ПЛАН

1. Аналітична робота в органах внутрішніх справ
2. Призначення та основні завдання інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України»
3. Система централізованого управління нарядами поліції «ЦУНАМІ»
4. Інформаційно-аналітичні технології в оперативно-розшуковій діяльності

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Аналітична робота в органах внутрішніх справ.
URL.https://libroos.io.ua/s30219/analitichna_robota_v_organah_vnutrishnih_sprav
2. Інформаційне забезпечення професійної діяльності: навч. посібник/ І.В. Краснобрижий, С.О. Прокопов, Е.В. Рижков. Дніпро : ДДУВС, 2018. 220 с.
3. Мовчан А. В. Інформаційно-аналітична робота в оперативно-розшуковій діяльності Національної поліції: навч. посібник / А. В. Мовчан. Львів: ЛьвДУВС, 2017. С.90-143.

Семінарське заняття № 9

Тема: Інформаційно-аналітичне забезпечення юридичної та правоохоронної діяльності. Застосування штучного інтелекту у боротьбі зі злочинами

ПЛАН

1. Поняття «штучний інтелект», як технологія майбутнього
2. Міжнародний досвід використання ШІ правоохоронними органами
3. Можливості використання штучного інтелекту правоохоронними органами України
4. Використання повітряних дронів у вирішенні задач правоохоронної діяльності
5. Особливості використання працівниками Національної поліції України нагрудних відеокамер

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Погореленко А.К. Штучний інтелект: сутність, аналіз застосування, перспективи розвитку.
URL. http://ej.journal.kspu.edu/index.php/ej/article/view/405/401
2. Штучний Інтелект. URL. http://referat-ok.com.ua/informatika/shtuchnii-intelekt
3. Можливості ШІ у правоохоронній системі міста. URL. https://www.everest.ua/mozhlyvosti-shi-u-pravoohoronnij-systemi-mista/
4. Використання штучного інтелекту в кримінальній юстиції. URL. https://ua.112.ua/statji/maliuska-khoche-vykorystovuvaty-shtuchnyi-intelekt-u-kryminalnii-iustytsii-naskilky-tse-mozhlyvo-535538.html
5. Благута Р.І., Мовчан А.В. Новітні технології у розслідуванні злочинів: сучасний стан і проблеми використання: монографія. Львів: ЛьвДУВС, 2020. 256 с.
6. Застосування органами та підрозділами поліції технічних приладів і технічних засобів фото- і кінозйомки, відеозапису. Аналіз закордонного досвіду: метод. матеріали для працівників підрозділів поліції МВС України/ В. А. Коршенко, М. В. Мордвинцев, Ю. В. Гнусов та ін. Харків: Харків. нац. ун-т внутр. справ, 2020. 44 с.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бараненко Р.В. Дослідження особливостей функціонування програмного забезпечення системи централізованого управління нарядами патрульної служби «ЦУНАМІ». Юридичний бюлетень : наук. журн. / редкол.: О. Г. Предместніков та ін. Випуск 2. Одеса, ОДУВС, 2016.
2. Безпечний онлайн шопінг – поради кіберполіції. URL. https://cyberpolice.gov.ua/article/bezpechnyj-onlajn-shoping---porady-kiberpolicziyi-5967/
3. Благута Р.І., Мовчан А.В. Новітні технології у розслідуванні злочинів: сучасний стан і проблеми використання: монографія. Львів: ЛьвДУВС, 2020. 256 с.
4. Використання інформаційно-пошукових систем в діяльності поліції. Правові інформаційно-пошукові системи. URL. https://arm.naiau.kiev.ua/books/inform_tekhnolohii/lection/lec3.html.
5. Використання штучного інтелекту в кримінальній юстиції. URL. https://ua.112.ua/statji/maliuska-khoche-vykorystovuvaty-shtuchnyi-intelekt-u-kryminalnii-iustytsii-naskilky-tse-mozhlyvo-535538.html
6. Голубєв В.О. Інформаційна безпека: проблеми боротьби з кіберзлочинами: Монографія. Запоріжжя: ГУ «ЗІДМУ», 2003. 250 с.
7. Давидюк В.М. Інтернет, як соціальне середовище роботи з конфідентами. *Актуальні питання протидії кіберзлочинності та торгівлі людьми*: збірник матеріалів Всеукр. наук.-практ. конф. (23 листоп. 2018 р., м. Харків). МВС України, Харків. нац. ун-т внутр. справ; Координатор проектів ОБСЄ в Україні. Харків: ХНУВС, 2018. – 436 с.
8. Денисова О.О. Інформаційні системи і технології в юридичній діяльності / О.О. Денисова. – К.: КНЕУ, 2003. – 315 с.
9. Державна служба фінансового моніторингу України [Електронний ресурс]: Кіберзлочинність та відмивання коштів Режим доступу: www.minfin.gov.ua/file/link/396800/file/tipolog2013.pdf
10. Джон Маркофф. Homo Roboticus? Люди и машини у пошуках взаэморозуміння URL. http://testlib.meta.ua/book/302060/read/
11. Електронний реєстр чинних, блокованих та скасованих сертифікатів відкритих ключів. URL. https://czo.gov.ua/ca-registry
12. За п'ять років кіберзлочинність в Україні виросла вдвічі. URL. https://www.epravda.com.ua/news/2019/10/21/652782
13. Закон України «Про інформацію». URL. https://zakon.rada.gov.ua/laws/show/2657-12#Text
14. Закон України «Про доступ до судових рішень». URL. https://ips.ligazakon.net/document/T053262.
15. Закон України «Про електронні документи та електронний документообіг» URL. https://zakon.rada.gov.ua/laws/show/851-15/ed20140419#Text

16. Закон України «Про електронну комерцію». URL. https://zakon.rada.gov.ua/laws/show/675-19#Text
17. Закон України «Про захист персональних даних». URL. https://zakon.rada.gov.ua/laws/show/2297-17#Text
18. Закон України «Про Національну поліцію». URL. https://zakon.rada.gov.ua/laws/show/580-19#Text
19. Застосування органами та підрозділами поліції технічних приладів і технічних засобів фото- і кінозйомки, відеозапису. Аналіз закордонного досвіду : метод. матеріали для працівників підрозділів поліції МВС України/ В. А. Коршенко, М. В. Мордвинцев, Ю. В. Гнусов та ін. Харків: Харків. нац. ун-т внутр. справ, 2020. 44 с.
20. Захист інформації в комп'ютерних системах та мережах : навч. посіб./ С.Г.Семенов, А.О.Подорожняк, О.І.Баленко, С.Ю.Гавриленко – Х.: НТУ «ХПІ», 2014.– 251 с.
21. Інформаційна безпека особистості. URL. https://sites.google.com/site/infobezpekaosobu/informacijna-bezpeka
22. Інформаційна безпека. URL. http://jure.in.ua/tema-9-informatsijna-bezpeka/
23. Інформаційна безпека. URL. http://pmf.uad.lviv.ua/storage/uploads
24. Інформаційна безпека. URL. https://uk.wikipedia.org/wiki
25. Інформаційна система. URL. http://іт.словник.укр/index.php/Інформаційна_система
26. Інформаційне забезпечення органів Національної поліції: основні поняття, завдання, структура системи, характеристика інформаційних підсистем.URL.https://arm.naiau.kiev.ua/books/inform_zabezpechennia/matherials/rozdil1.html
27. Інформаційні процеси. URL. https://uk.wikipedia.org/wiki
28. Карачка А.Ф. Технології захисту інформації. URL. http://dspace.wunu.edu.ua/bitstream/316497/26564/1/lekzii.pdf
29. Кіберзлочинність в Україні. Ера цифрових технологій – ера нових злочинів. URL. https://uz.ligazakon.ua/ua/magazine_article/EA013606
30. Кіберполіція надала рекомендації щодо захисту персональних даних під час використання мобільних додатків. URL. https://cyberpolice.gov.ua/article/kiberpolicziya-nadala-rekomendacziyi-shhodo-zaxystu-personalnyx-danyx-pid-chas-vykorystannya-mobilnyx-dodatkiv-8506/
31. Коваленко А.В. Інформаційно-аналітичне забезпечення діяльності Національної поліції: теоретичний і практичний підхід. URL. file:///c:/users/test/downloads/1616756398540493.pdf
32. Конвенція про кіберзлочинність. URL. https://zakon.rada.gov.ua/laws/show/994_575#Text
33. Концепція інформаційної безпеки України [Електронний ресурс]. – Режим доступу : https://www.osce.org/uk/fom/175056?download=true
34. Косиченко О.О. Правові інформаційні ресурси Інтернет: довідник. – Дніпро: ДДУВС, 2017. – 92 с.

35. Криптографія: загальні визначення, класифікація. асиметричні та симетричні криптоалгоритми, їх порівняння. URL. https://mozolevska09.wordpress.com/2014/03/14/криптографія-загальні-визначення-кл/
36. Можливості ШІ у правоохоронній системі міста. URL. https://www.everest.ua/mozhlyvosti-shi-u-pravoohoronnij-systemi-mista/
37. Навіщо ми розробляємо штучний інтелект і чим нам це загрожує. URL. https://nv.ua/ukr/techno/popscience/shtuchniy-intelekt-shcho-ce-take-i-navishcho-vin-nam-potriben-50053922.html
38. Наказ МВС України від 13.06.2018 № 497 // БД «Законодавство України» / ВР України. URL. https://zakon.rada.gov.ua/laws/show/z0787-18
39. Наливайко Н. Я. Інформатика. Навч.посібник. К.: Центр учбової літератури, 2019. 576 с.
40. О.В. Співаковський, М.І. Шерман, В.М. Стратонов, В.В. Лапінський Інформаційні технології в юридичній діяльності: базовий курс: [навчальний посібник]. Херсон: ХДУ, 2012. 220 с.
41. Ольшанська О.В. Основні положення інформаційної безпеки та її стан в сучасних умовах розвитку в Україні. URL. https://knutd.edu.ua/publications/pdf/Visnyk/2015-2/62-68.pdf
42. Пефтієв О. В. Єдиний аналітичний сервісний центр Головного управління Національної поліції в Донецькій області // Актуальні питання забезпечення публічної безпеки, порядку в сучасних умовах: поліція та суспільство – стратегії розвитку і взаємодії : тези доп. Всеукр. наук.-практ. конф. (м. Маріуполь, 12 трав. 2018 р.) / МВС України, ДВНЗ «Приазовський державний технічний університет». Маріуполь, 2018. С. 345–351.
43. Поняття та зміст кіберзлочинності. URL. https://goal-int.org/ponyattya-ta-zmist-kiberzlochinnosti/
44. Правова інформація та комп'ютерні технології в юридичній діяльності: навч. посібник. / В.Г. Іванов, С.М. Іванов, В.В. Карасюк та ін.; за заг.ред. В.Г. Іванова. – 4-те вид., змін. І доп. Х.: Право, 2014. 240 с.
45. Про затвердження Інструкції із застосування органами та підрозділами поліції технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, засобів фото- і кінозйомки, відеозапису. URL. https://zakon.rada.gov.ua/laws/show/z0028-19#Text
46. Про затвердження Інструкції про порядок включення нормативно-правових актів до Єдиного державного реєстру нормативно-правових актів та надання інформації з нього. URL. https://zakon.rada.gov.ua/laws/show/z0546-02#Text
47. Про затвердження Положення про Єдиний реєстр досудових розслідувань, порядок його формування та ведення. URL. https://zakon.rada.gov.ua/laws/show/v0298905-20#Text
48. Про затвердження Положення про Інтегровану інформаційно-пошукову систему органів внутрішніх справ України: наказ МВС України від 12.10.2009 р., № 436. Pro zatverdzhennya Polozhennya pro Integrovany

informatciyno-poshukovu sistemu organiv vnutrishnikh sprav Ukrainy vid 12.10.2009 p., № 436.
49. Про затвердження Положення про інформаційно-телекомунікаційну систему «Інформаційний портал Національної поліції України». URL. https://zakon.rada.gov.ua/laws/show/z1059-17#Text
50. Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки: Закон України від 09.01.07 р. № 537-V// Відомості Верховної Ради України. – 2007. – № 12. – Ст. 102.
51. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України». URL. https://zakon.rada.gov.ua/laws/show/96/2016#n11
52. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». URL. https://zakon.rada.gov.ua/laws/show/47/2017#Text
53. Рибальський О.В., Хахановський В.Г., Кудінов В.А. Основи інформаційної безпеки та технічного захисту інформації. Посібник для курсантів ВНЗ МВС України. К.: Вид. Національної академії внутріш. справ, 2012. 104 с.
54. Самойленко О. А. Виявлення та розслідування кіберзлочинів: навчально-методичний посібник. Одеса, 2020. 112 с.
55. Сащук Г. Інформаційна безпека в системі забезпечення національної безпеки. URL. http://journ.univ.kiev.ua/trk/publikacii/satshuk_publ.php
56. Сезонова І. К. Інформатика для правоохоронців: навч. посіб./ І. К. Сезонова; МВС України, Харк. нац. ун-т внутр. справ, 2015. – 182 с.
57. Сіренко О.В. Поняття кіберзлочинів та особливості методики їх розслідування.URL.http://dspace.oduvs.edu.ua/bitstream/123456789/486/1/ilovepdf_com-48-49%5B1%5D.pdf
58. Сугоняко Н.В. Поняття правової інформації та її особливості. Юридичний науковий електронний журнал. URL. http://www.lsej.org.ua/1_2019/42.pdf
59. Термін «Інформаційна безпека». Термінологія законодавства. *Верховна Рада України*: [сайт]. URL. https://zakon.rada.gov.ua/laws/term/11458.
60. Технології захисту інформації. URL. https://www.uzhnu.edu.ua/uk/infocentre/get/4186
61. Технологія пошуку інформації засобами мережі Інтернет: основні способи пошуку інформації в Інтернеті. URL. https://disted.edu.vn.ua/courses/learn/3121
62. Тлумачний словник з інформатики / Г.Г. Півняк, Б.С. Бусигін, М.М. Дівізінюк та ін. Д., Нац. гірнич. ун-т, 2010. 600 с.
63. Федишин І.Б. Електронний бізнес та електронна комерція (опорний конспект лекцій для студентів напрямку «Менеджмент» усіх форм навчання)/ І.Б. Федишин. Тернопіль, ТНТУ імені Івана Пулюя, 2016. 97 с.
64. Фурашев В.М. Сутність та визначення понять «інформаційна безпека» і «безпека інформації». URL. http://ippi.org.ua/furashev-vm-sutnist-ta-

viznachennya-ponyat-%E2%80%9Cinformatsiina-bezpeka%E2%80%9D-i-%E2%80%9Cbezpeka-informatsii%E2%80%9D
65. Шерман М. І. Правова інформаційно-пошукова система «ЛІГА: ЗАКОН. Юрист» як засіб комп'ютерної підтримки навчання правових дисциплін / М. І. Шерман // Науковий часопис НПУ імені М. П. Драгоманова. Серія 2: Комп'ютерно-орієнтовані системи навчання.–2011.–№. 11.–С. 46-51.– Режим доступу: http://nbuv.gov.ua/UJRN/Nchnpu_2_2011_11_9
66. Школьний В.Б. Деякі причини виникнення і розвитку злочинності у сфері використання ЕОМ.
URL. http://pravoisuspilstvo.org.ua/archive/2012/2_2012/48.pdf
67. Що таке електронна комерція? E-commerce для початківців. URL. https://www.interkassa.com/ua/blog/chto-takoe-elektronnaya-kommerciya-e-commerce-dlya-nachinayushchih/
68. Deng I. This state-backed AI unicorn has helped Chinese police arrest 10,000 criminals. URL. https://www.scmp.com/tech/start-ups/article/3003686/state-backed-ai-unicorn-has-helped-chinese-police-arrest-10000
69. Practitioner's Guide to COMPAS Core. URL. https://assets.documentcloud.org/documents/2840784/Practitioner-s-Guide-to-COMPAS-Core.pdf
70. Using Artificial Intelligence to Address Criminal Justice Needs (NIJ Journal280). URL. https://www.ncjrs.gov/pdffiles1/nij/252038.pdf
71. Xuanzun L. Ubiquitous surveillance cameras in a Beijing district reduce crimes by nearly 40 %. URL. http://www.globaltimes.cn/content/1113386.shtml