**Виклики сучасності в сфері захисту персональних даних.**

1. Значення Big Data та блокчейн у захисті персональних даних.
2. Оцінка переваг та ризиків великих даних.
3. Кіберзлочинність як основна проблема захисту персональних даних.
4. Webs 2.0 та 3.0: соціальні мережі та інтернет речей
5. Вплив цифровізації та діджиталізації на захист персональних даних.

## Значення Big Data та блокчейн у захисті персональних даних.

У сучасному світі, де цифрові технології все більше проникають у всі сфери життя, захист персональних даних є однією з найважливіших проблем. З одного боку, цифровізація даних надає громадянам нові можливості, такі як доступ до інформації та послуг, які раніше були недоступні. З іншого боку, вона також створює нові ризики порушення прав громадян або ускладнення їх реалізації.

Одним із найпоширеніших ризиків є витік персональних даних. У 2018 році, наприклад, у результаті витоку даних з Facebook було скомпрометовано персональні дані понад 87 мільйонів користувачів. Ці дані були використані для цілей політичної пропаганди, що призвело до порушення права громадян на свободу висловлювань і право на приватне життя.

Іншим ризиком є використання персональних даних для злочинних цілей. Наприклад, персональні дані можуть використовуватися для шахрайства, вимагання або інших злочинів. Для захисту персональних даних існує ряд нормативно-правових актів, таких як Загальний регламент про захист даних (GDPR). Однак ці акти часто не є достатніми для запобігання порушенням прав громадян.

Одним із перспективних напрямів захисту персональних даних є використання технології блокчейн. Блокчейн - це децентралізована система зберігання інформації, яка забезпечує її безпеку та конфіденційність. Технологія блокчейн може бути використана для створення цифрових паспортів, які дозволять громадянам контролювати свої персональні дані.

Зберігання персональних даних на єдиному сервері є вразливим до кібератак і людського фактору. Технологія блокчейн може забезпечити більший захист даних, оскільки вона децентралізована і використовує криптографію. У традиційних системах зберігання персональних даних всі дані зберігаються на одному сервері. Цей сервер є єдиною точкою відмови, а також потенційною ціллю для кібератак. Якщо сервер буде зламний, то всі дані можуть бути втрачені або скомпрометовані.

Крім того, в традиційних системах важливу роль відіграє людський фактор. Недобросовісні працівники організації можуть незаконно поширювати конфіденційну інформацію. Технологія блокчейн децентралізована, що означає, що дані зберігаються на багатьох різних комп'ютерах. Це робить систему більш стійкою до кібератак, оскільки для успіху атаки необхідно зламати всі комп'ютери, на яких зберігаються дані.

Технологія блокчейн також використовує криптографію для захисту даних. Це означає, що дані можуть бути доступні лише тим користувачам, які мають правильний ключ розшифровки. У контексті захисту персональних даних технологія блокчейн може використовуватися для створення децентралізованих систем управління персональними даними. У таких системах користувачі зберігають свої персональні дані на своїх власних пристроях. Це забезпечує користувачам повний контроль над своїми даними.

В Україні діє понад 135 державних реєстрів з персональними даними громадян. Серед ключових проблем цих реєстрів виділяють дублювання

даних, низький рівень взаємодії та обміну інформацією між реєстрами, а також відсутність законодавства, що регулює порядок ведення реєстрів.

Ці проблеми призводять до збільшення фінансових витрат на утримання реєстрів, а також до незручностей для громадян, які повинні звертатися в різні органи державної влади для отримання адміністративних послуг. Для вирішення цих проблем в Україні розроблено проект закону про публічні електронні реєстри. Цей проект передбачає створення єдиного розподіленого державного реєстру персональних даних. Новий реєстр буде містити інформацію з усіх державних реєстрів в Україні. При цьому інформація, яка буде вноситись в реєстр із попередніх реєстрів, повинна перевірятися на достовірність.

Будь-який орган державної влади відповідно до своїх повноважень буде мати доступ відповідного рівня до тих даних, які йому необхідні для реалізації поставлених завдань. Такий розподіл рівнів доступу дозволить уникнути дублювання інформації, а також захистити персональні дані громадян від несанкціонованого втручання.

Створення єдиного розподіленого державного реєстру персональних даних є важливою ініціативою, яка може суттєво покращити захист персональних даних в Україні.

Ризики порушень прав громадян у цифровому світі є серйозною проблемою, яка потребує вирішення. Для цього необхідно посилити нормативно-правове регулювання захисту персональних даних, а також розробити нові технологічні рішення, які допоможуть забезпечити безпеку даних.

Окрім зазначених зризиків, до числа інших ризиків порушень прав громадян у цифровому світі можна віднести такі:

1. Незаконне збирання персональних даних. Це може відбуватися без відома або згоди суб'єкта даних. Наприклад, дані можуть бути зібрані за допомогою веб-трекерів, які встановлюються на веб-сайтах.

2. Незаконне використання персональних даних. Персональні дані можуть бути використані для цілей, які не були погоджені суб'єктом даних. Наприклад, дані можуть бути використані для цілей прямого маркетингу.

3. Недостатній рівень захисту персональних даних. Це може призвести до їх витоку або злому.

Для зниження ризиків порушень прав громадян у цифровому світі необхідно дотримуватися таких заходів безпеки: 1) Уважно читайте умови використання веб-сайтів та додатків, перш ніж надавати персональні дані; 2) Використовуйте надійні паролі та методи аутентифікації; 3) Регулярно оновлюйте програмне забезпечення на своїх пристроях; 4) Будьте обережні при діленні персональними даними в Інтернеті.

***Big Data: можливості та ризики.***

Big Data – це технологія, яка дозволяє збирати та обробляти величезні обсяги інформації. Вона має широкий спектр застосувань, зокрема в бізнесі, медицині, охороні здоров'я, державному управлінні тощо.

Однак використання Big Data пов'язане з певними ризиками, зокрема з ризиком порушення захисту персональних даних.

Ключові моменти:

- Big Data має ряд переваг, зокрема дозволяє:
- Оптимізувати прибуток;
- Досліджувати онлайн поведінку потенційних клієнтів;
- Боротися з COVID-19;
- Запобігати природним катаклізмам.

Водночас використання Big Data пов'язане з певними ризиками, зокрема:

- Витоком персональних даних;
- Продажем персональних даних користувачів без їхньої згоди;
- Застосуванням дискримінаційних суджень до користувачів.

- Найчастіше такі проблеми виникають із двох причин:
- Недотримання законодавства про персональні дані;
- Нехтування правилами кібербезпеки.
- Захист персональних даних при використанні Big Data

Для зменшення ризиків, пов’язаних з використанням Big Data, компанії повинні дотримуватися таких заходів:

1. Перевірити, яке законодавство застосовується до їхньої діяльності та оновити політики щодо обробки персональних даних відповідно до цього законодавства.
2. Проводити регулярні аудити ефективності методів та систем кібербезпеки.
3. За можливості шифрувати/псевдомінізувати персональні дані.
4. Проводити регулярні тренінги з кібербезпеки та захисту персональних даних у межах компанії.
5. Законодавче регулювання захисту персональних даних

Більшість країн світу прийняли національні законодавчі акти щодо захисту персональних даних. Деякі з цих актів, як наприклад, GDPR та CIPP, застосовуються за принципом «екстратериторіальності». Це означає, що вони застосовуються до компаній, які обробляють персональні дані резидентів цих юрисдикцій, незалежно від того, де розташовані ці компанії.

Big Data – це потужна технологія, яка має великий потенціал для розвитку бізнесу та суспільства. Однак використання Big Data вимагає дотримання певних правил, зокрема правил захисту персональних даних. Важливо, щоб компанії, які використовують Big Data, були обізнані з цими правилами та дотримувалися їх.

## Оцінка переваг та ризиків великих даних.

Сучасні технології обробки даних можуть ефективно впоратися з великими обсягами інформації, швидко імпортувати нові дані та забезпечувати обробку в режимі реального часу зі швидким наданням відповідей, навіть на складні запитання. Вони також здатні обробляти багато запитань одночасно та забезпечувати аналіз різних типів інформації, таких як фотографії, текст чи цифри. Ці інновації у технологіях дозволяють ефективно структурувати, обробляти та оцінювати великі обсяги даних в режимі реального часу.

Завдяки зростанню доступних для аналізу даних, які можна обробляти, тепер можна досягти результатів, які раніше були недосяжними. Великі дані сприяли створенню нових галузей бізнесу, де з'являються нові послуги як для підприємств, так і для споживачів. Вартість персональних даних громадян ЄС може потенційно зрости до майже 1 трильйона євро на рік до 2020 року. Таким чином, великі дані можуть створити нові можливості, розвиваючи соціальні, економічні та наукові концепції, які приносять вигоду фізичним особам, бізнесу та державним органам.

Аналітика великих даних може розкривати закономірності між різними джерелами та наборами даних, призводячи до корисних відкриттів у науці та медицині. Наприклад, у галузі охорони здоров'я, харчової безпеки, інтелектуальних транспортних систем, енергоефективності та містобудування. Аналіз інформації в реальному часі може бути використаний для вдосконалення впроваджуваних систем. Можна отримати нові знання в дослідницькій роботі, поєднуючи велику кількість даних і статистичні оцінки, особливо в областях, де оцінка великої частини даних раніше виконувалася вручну. Розробка нових методів лікування, спеціально адаптованих до потреб окремих пацієнтів, можлива на основі порівняння з великою кількістю доступної інформації.

Компанії сподіваються отримати конкурентну перевагу, заощадити кошти та створити нові сфери бізнесу за допомогою аналізу великих даних

для надання індивідуалізованих послуг споживачам. Державні органи розраховують на вдосконалення в кримінальному правосудді. Стратегія Єдиного цифрового ринку Європи визнає потенціал технологій, послуг і великих даних на основі даних як каталізатори економічного зростання, інновацій та цифровізації в ЄС. Однак великі дані також несуть ризики, особливо пов'язані з обсягом, швидкістю та різноманіттю оброблюваних даних, що викликає конкретні питання щодо захисту персональних даних та приватності. Ці ризики були визначені в висновках ЄІЗПД, резолюціях Європейського Парламенту та програмних документах Ради Європи.

## Кіберзлочинність як основна проблема захисту персональних даних.

У наші дні використання інформаційних технологій не має меж. Віртуальний простір переймає від реального все підряд, у тому числі й злочинність у її нових формах і проявах. Поняття кіберпростору, введеного письменником Вільямом Гібсоном у п'єсі «Le Neuromancer», описує віртуальний простір як такий, в якому циркулюють електронні дані всіх комп'ютерів світу.

Практично кожен чув про кіберзлочинність і, можливо, навіть особисто з нею зіштовхувався. Кіберзлочинність включає в себе різні види злочинів, що здійснюються за допомогою комп’ютера і в мережі Інтернет. Об’єктом кіберзлочинів є персональні дані, банківські рахунки, паролі та інша особиста інформація як фізичних осіб, так і бізнесу та державного сектору. Кіберзлочинність є загрозою не тільки на національному, а й на глобальному рівні.

Кіберзлочинність - це вид злочинності, який використовує комп'ютери або інші електронні пристрої для вчинення злочинів. Об'єктом

кіберзлочинів може стати будь-який користувач інтернету, незалежно від його віку, статі, професії чи місця проживання.

**Найпоширенішими видами кіберзлочинів є:**

Кардинг - це використання реквізитів платіжних карт, отриманих зі зламаних серверів інтернет-магазинів, платіжних і розрахункових систем, а також із персональних комп'ютерів. Зловмисники можуть отримати ці дані за допомогою різних методів, таких як хакерство, фішинг, вішинг або соціальна інженерія.

Фішинг - це вид шахрайства, відповідно до якого клієнтам платіжних систем надсилають повідомлення електронною поштою нібито від адміністрації або служби безпеки цієї системи з проханням вказати свої рахунки та паролі. Зловмисники використовують такі повідомлення, щоб отримати конфіденційну інформацію про жертв, яку потім можуть використовувати для крадіжки грошей або здійснення інших злочинів.

Вішинг - це вид кіберзлочинів, у якому в повідомленнях міститься прохання зателефонувати на певний міський номер, а при розмові запитуються конфіденційні дані власника картки. Зловмисники використовують такі повідомлення, щоб отримати конфіденційну інформацію про жертв, яку потім можуть використовувати для крадіжки грошей або здійснення інших злочинів.

Онлайн-шахрайство - це різноманітні схеми шахрайства, які здійснюються в Інтернеті. До таких схем відносяться, наприклад, несправжні інтернет-аукціони, інтернет-магазини, сайти та телекомунікаційні засоби зв'язку, які використовують для залучення жертв і отримання від них грошей або іншої цінної інформації.

Піратство - це незаконне розповсюдження інтелектуальної власності в Інтернеті. До таких дій відносяться, наприклад, скачування музики,

фільмів, програмного забезпечення та інших творів без дозволу правовласника.

Кард-шарінг - це надання незаконного доступу до перегляду супутникового та кабельного TV. Зловмисники отримують доступ до даних абонентів і використовують їх для перегляду телевізійних каналів безкоштовно.

Соціальна інженерія - це технологія управління людьми в Інтернет-просторі. Зловмисники використовують соціальну інженерію для того, щоб змусити жертви надати їм конфіденційну інформацію або здійснити інші дії, які можуть завдати їм шкоди.

Мальваре - це шкідливе програмне забезпечення, яке може завдати шкоди комп'ютерам або іншим електронним пристроям. До шкідливого програмного забезпечення відносяться, наприклад, віруси, трояни, боти, шпигунське програмне забезпечення та інші програми, які можуть використовуватися для крадіжки даних, блокування роботи комп'ютера або здійснення інших шкідливих дій.

Протиправний контент - це контент, який пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості і насильства. Такий контент може завдати шкоди суспільству і спричинити негативні соціальні наслідки.

Наслідки кіберзлочинності можуть бути дуже серйозними. Вони можуть включати в себе:

Фінансова шкода - крадіжка грошей, даних кредитних карт або інших фінансових ресурсів.

Порушення конфіденційності - отримання злочинцями конфіденційної інформації про жертву, наприклад, її імені, адреси, номера телефону, паролів тощо.

Шкідливий вплив на репутацію - поширення в Інтернеті неправдивої інформації про жертву, яка може завдати їй шкоди.

Психологічний вплив - стрес, тривога, депресія тощо.

Існує декілька порад щодо того, як вберегти себе від кіберзлочинів:

- створення надійних паролів, захист інформації та періодична їх зміна;
- поінформованість про розповсюджені прийоми, які використовують злочинці для того, щоб розпізнавати їх;
- захист пристроїв, встановлення антивірусних програм;
- використання захищених мереж;
- перевірка своїх облікових записів;
- використання інструментів конфіденційності та безпеки Google чи інших браузерів.

Узагальнюючи матеріали, можна впевнено сказати, що проблема кіберзлочинності є однією з найважливіших сьогодні, та такою що потребує негайного втручання в її вирішення. Історичний аспект, а також сучасний стан цього питання свідчать про те, що явище кіберзлочинності активно розвивається. Як кримінальна категорія, злочини в кіберпросторі є джерелом високого рівня суспільної небезпеки, що напряму пов'язано з їх особливостями, різноманітністю та проблемами боротьби з ними. Про глобальність проблеми свідчить і той факт, що сьогодні весь світ об'єднує зусилля для протидії кіберзлочинам.

## Webs 2.0 та 3.0: соціальні мережі та інтернет речей

Спочатку інтернет був задуманий як мережа для взаємозв'язку комп'ютерів та передачі повідомлень. В еру Web 2.0 інтернет був трансформований у форум, на якому користувачі взаємодіють, співпрацюють та генерують дані. Ця ера характеризується надзвичайним успіхом та широким використанням служб соціальних мереж.

Служби соціальних мереж (ССМ) або «соціальні медіа» в широкому розумінні визначаються як «онлайн-платформи комунікацій, які надають людям можливість приєднуватись або створювати мережі однодумців». Щоб приєднатися до мережі або створити її, особам пропонується надати персональні дані та створити свій обліковий запис.

ССМ дозволяють користувачам створювати цифровий «контент», від фотографій та відеозаписів до посилань на газети та особистих нотаток, щоб висловити свою думку. За допомогою таких онлайн-платформ комунікацій користувачі можуть взаємодіяти та спілкуватися з кількома іншими користувачами.

Важливо, що більшість популярних ССМ не вимагають жодних реєстраційних внесків. Замість того, щоб вимагати від користувачів плату за приєднання до мережі, провайдери ССМ отримують більшу частину своїх доходів від цільової реклами. Рекламодавці можуть отримати значну користь від особистої інформації, яка щодня розкривається на цих сайтах. Володіння інформацією про вік, стать, місцезнаходження та інтереси користувача допомагає їм доводити свою рекламу до відома «потрібних» людей.

Розвиток ССМ має важливі наслідки для прав людини. З одного боку, ССМ забезпечують нові можливості для свободи вираження поглядів, свободи асоціацій та свободи інформації. Користувачі ССМ можуть вільно висловлювати свої думки та ідеї, спілкуватися з іншими людьми та отримувати доступ до інформації.

З іншого боку, ССМ також можуть призвести до порушень прав людини. Наприклад, ССМ можуть використовуватися для поширення неправдивої інформації або мови ненависті. Крім того, використання ССМ може призвести до порушення приватності та конфіденційності користувачів.

Комітетом міністрів Ради Європи було прийнято Рекомендацію про захист прав людини в контексті служб соціальних мереж, в окремому розділі якої йдеться про захист персональних даних. Ця рекомендація закликає держави-члени Ради Європи вжити заходів для захисту прав людини в контексті ССМ, зокрема шляхом забезпечення захисту персональних даних користувачів.

У 2018 році Комітетом міністрів Ради Європи було прийнято Рекомендацію про роль та обов’язки інтернет-посередників. Ця рекомендація закликає інтернет-посередників, зокрема провайдерів ССМ, вжити заходів для захисту прав людини в Інтернеті, зокрема шляхом боротьби з поширенням неправдивої інформації та мови ненависті.

Соціальні мережі (ССМ) стали невід'ємною частиною сучасного суспільства. Вони дозволяють людям спілкуватися, взаємодіяти, отримувати доступ до інформації та формувати громадську думку. Однак ССМ також мають потенціал для порушення приватності та захисту персональних даних. З одного боку, ССМ можуть використовуватися для цільової реклами. Цей підхід дозволяє компаніям охопити свою аудиторію, пропонуючи їй більш конкретні товари. Споживачі також можуть бути зацікавлені в тому, щоб презентована їм реклама була більш доцільною та цікавою. З іншого боку, ССМ можуть використовуватися для поширення неправдивої інформації та мови ненависті. Це може призводити до дестабілізації суспільства та порушення прав людини.

Ще одна проблема, пов'язана з ССМ, полягає в тому, що вони можуть становити загрозу для приватності користувачів. СМС збирають величезний обсяг особистої інформації про своїх користувачів, включаючи їхні імена, дати народження, місцезнаходження, інтереси та зв'язки. Ця інформація може бути використана для цілей маркетингу, розслідування або навіть злочинів. Європейське законодавство щодо захисту персональних даних намагається відповісти на виклики ССМ стосовно

захисту приватності та персональних даних. Такі принципи, як згода, захист приватного життя та персональних даних за призначенням і замовчуванням, а також права фізичних осіб, є особливо важливими в контексті ССМ та мережевих служб.

Однак ці принципи не завжди можуть бути ефективно реалізовані в контексті ССМ. Наприклад, може бути важко забезпечити прозорість у тому, хто здатний збирати, мати доступ та використовувати дані, зібрані з пристроїв ССМ. Крім того, люди часто не розуміють технічного процесу обробки даних і, відповідно, наслідків своєї згоди.

Резолюція Європейського Парламенту від 14 березня 2017 року розглядає важливість великих даних для основних прав, таких як приватність, захист персональних даних, недискримінація, безпека та правозастосування (2016/2225 (INI)). Рада Європи, Консультативний Комітет Конвенції 108, в своїй рекомендації від 23 січня 2017 року наголошує на захисті фізичних осіб у світі великих даних. Деякі інші документи, такі як Висновок 7/2015 та Висновок 8/2016 ЄІЗПД, розглядають виклики та забезпечення основних прав в ері великих даних.

Також варто відзначити резолюцію Європейського Парламенту від 14 березня 2017 року, що акцентує значення великих даних для основних прав, таких як приватність, захист персональних даних, недискримінація, безпека та правозастосування, яка була прийнята під номером P8_TA(2017)0076. Рекомендації Консультативного Комітету Конвенції 108 з питань захисту фізичних осіб в світі великих даних (T-PD(2017)01 від 23 січня 2017 року) також звертають увагу на ці аспекти.

Міжнародна конференція Уповноважених із захисту даних та приватності в 2014 році ухвалила резолюцію щодо великих даних. Важливо враховувати, що обробка великих обсягів даних може мати значні наслідки як для публічного, так і приватного сектору.

Огляд регуляторних аспектів включає Загальний регламент захисту персональних даних, який встановлює положення щодо права не бути об'єктом автоматизованих рішень, включаючи профайлінг. Питання приватності стає актуальним, коли реалізація права на відмову вимагає людського втручання, що дає суб'єктам даних можливість висловлювати свою думку та оскаржувати рішення. Це може викликати труднощі у забезпеченні належного рівня захисту персональних даних, особливо коли людське втручання неможливе або коли алгоритми стають занадто складними, а обсяг залучених даних занадто великий, щоб забезпечити фізичним особам роз'ясування певних рішень та/або попередню інформацію для отримання їхньої згоди. Наприклад, застосування штучного інтелекту та автоматизованого прийняття рішень можна спостерігати в останніх розробках іпотечних додатків або під час процесу підбору персоналу, коли заявки можуть бути відхилені або не задовольнені на підставі незадовільного відповідання певним параметрам чи факторам.

**Література.**

Яковлєв Р. В. Принципи мінімізації та точності персональних даних під час використання технології розподіленого реєстру (адміністративно-правовий аспект). ScienceRise: Juridical Science. 2019. № 4 (10). С. 16–24.

Адамов О. С., Хаханов В. І., Чумаченко С. В., Абдуллаєв В. Г. Блокчейн інфраструктура для захисту кіберсистем. Радиоэлектроника и информатика. 2018. № 4. С. 64–85.

Проект Закону про публічні електронні реєстри : від 10.09.2019 № 2110 / ініціатори: М. В. Крячко, Р. В. Соха, О. П. Федієнко, Є. В. Чернєв // База даних «Законодавство України» / Верховна Рада України. URL: https:// w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=66772.

Резолюція Європейського Парламенту від 14 березня 2017 р. про значення великих даних для основних прав: приватності, захисту персональних даних, недискримінації, безпеки та правозастосування (2016/2225 (INI)).

Рада Європи, Консультативний Комітет Конвенції 108, Рекомендації щодо захисту фізичних осіб стосовно обробки персональних даних у світі Великих даних, від 23 січня 2017 р.

Міжнародна конференція Уповноважених із захисту даних та приватності (2014), Резолюція щодо Великих даних.

М. Бем, І. Городський. Захист персональних даних: правове регулювання та практичні аспекти: науково-практичний посібник. – «К.І.С.»., 2021. С. 161.