With the support of the Erasmus+ Programme of the European Union

EULIoT

National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"

Міністерство освіти і науки України

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

ПРОЕКТ ERASMUS +

«Європейська інтеграція: законодавство та Інтернет речей»

№620017-EPP-1-2020-1-UA- EPPJMO-MODULE

ЄВРОПЕЙСЬКА ІНТЕГРАЦІЯ: ЗАКОНОДАВСТВО ТА ІНТЕРНЕТ РЕЧЕЙ

Навчально-методичний посібник

КИЇВ
Вересень 2021

Упорядники посібника

Баранов О.А. – доктор юридичних наук, професор, факультет соціології і права, КПІ ім. Ігоря Сікорського. Академічний лідер проекту «Європейська інтеграція: законодавство та Інтернет речей»

Головко О.М. – кандидат юридичних наук, старший викладач, факультет соціології і права КПІ ім. Ігоря Сікорського. Координатор проекту «Європейська інтеграція: законодавство та Інтернет речей»

Дубняк М.В. – кандидат юридичних наук, старший викладач, факультет соціології і права КПІ ім. Ігоря Сікорського. Менеджер проекту «Європейська інтеграція: законодавство та Інтернет речей»

ПРОЕКТ ERASMUS +

«Європейська інтеграція: законодавство та Інтернет речей»

№ 620017-EPP-1–2020–1-UA-EPPJMO-MODULE

Європейська інтеграція: законодавство та Інтернет речей. Навчально-методичний посібник / Упорядн.: О. Баранов, О. Головко, М. Дубняк. - Київ, КПІ ім. Ігоря Сікорського, 2021 - 216 с.

Навчально-методичний посібник підготовлено для забезпечення слухачів курсу «Європейська інтеграція: законодавство та Інтернет речей» систематизованим конспектом лекцій, який забезпечує легке сприйняття та запам'ятовування матеріалу. Виклад тексту посібника враховує особливості сучасного сприйняття інформації. Посібник містить виклад основних тем курсу, інтерактивні елементи тестових завдань та контрольні питання для самостійної перевірки рівня знань.

Рекомендується студентам, аспірантам, викладачам, науковцям, державним службовцям, підприємцям, юристам, а також усім, хто цікавиться проблемами правового регулювання суспільних відносин у сфері застосування штучного інтелекту, робототехніки, криптовалют, технологій блокчейн, «хмарних» технологій, «великих даних» та інших складових Інтернету речей (IoT), правовим забезпеченням цифрової трансформації, дослідженням національного законодавства та законодавства Європейського Союзу з питань забезпечення кібербезпеки, вільного обігу даних, захисту персональних даних.

Посібник підготовлено в рамках реалізації міжнародного проекту у сфері освіти «Європейська інтеграція: законодавство та Інтернет речей» у межах напряму Жан Моне «Модуль» програми «Erasmus+».

№ 620017-EPP-1–2020–1-UA-EPPJMO-MODULE (спільний проект КПІ імені Ігоря Сікорського, Еразмус+ Жан Моне Фонду та Виконавчого агентства з питань освіти, аудіовізуальної діяльності та культури за підтримки ЄС)».

Зміст

РОЗДІЛ І.

ВСТУП ДО ПРЕДМЕТНОЇ СФЕРИ ІНТЕРНЕТУ РЕЧЕЙ

1. Загальні питання Інтернету речей

1. Визначення Інтернету речей, склад та особливості застосування
2. Політика Євросоюзу щодо розвитку Інтернету речей
3. Системні ризики та перешкоди впровадження Інтернету речей

1. Визначення Інтернету речей, склад та особливості застосування.

Перш ніж давати поняття явищу Інтернету речей необхідно з'ясувати передумови його появи. Для цього треба звернутись до питання соціальних змін, що відбувались за період відомої нам історії людства. Ці зміни частіше за все були спричинені реформами.

Реформи – це завжди соціальні трансформації. Соціальна трансформація – це перетворення, зміна або корекція мети функціонування, структури і функцій суспільства або його окремого сегменту, зокрема, методів, способів і механізмів реалізації цих функцій, для нейтралізації або сприяння дії зовнішніх і внутрішніх впливів на його подальший розвиток.

Один з панівних методів соціальної трансформації – це техніко-економічний метод, базовим критерієм якого є ефективність.

Техніко-економічні методи – реалізуються через промислові революції (технологічні революції).

Фундаментальний вплив на суспільні відносини мають особливості сучасного процесу розвитку цивілізації:

- швидке зростання темпів і масштабів глобалізації;
- глобалізуються – відносини: транснаціональних корпорацій, міждержавні, середнього та малого бізнесу різної юрисдикції, а також між окремими людьми;
- різке збільшення акторів, що приймають участь в певних суспільних процесах;
- світова логістична інфраструктура – в основному дозволяє швидко переміщувати товари, капітали, послуги та людей в будь-яку точку планети;
- високі темпи і масштаби проникнення ІКТ та інтернет-технологій в усі сфери людської активності;
- глобалізація інформаційних процесів стала необхідною та можливою завдяки використанню ІКТ та мережі Інтернет.

Через вищезгадані особливості значно зросли обсяги інформації.

Наприклад, землероб перед посівною має знати:

1. Кілька століть тому:
- відомості про тенденції погоди;
- температуру землі.

2. Сьогодні:
- кон'юнктуру конкретної сільськогосподарської продукції на внутрішньому та світовому ринках;
- інформація про агротехнології;
- інформація про насіння;
- інформацію про добрива та гербіциди;
- відомості про сільськогосподарську техніку;
- відомості про паливо;
- податкову та митну систему тощо.

На цьому прикладі можна зробити висновок, що сучасний процес прийняття рішень (останні 1,5 століття) характеризується наступним:

- потрібні великі обсяги інформації (даних);
- задіяна велика кількість суб'єктів та об'єктів;
- прийняття рішень здійснюється в режимі обмеженості часу (реального часу) тощо.

З цього можна зробити висновок, що

Людина внаслідок когнітивних обмежень не в змозі приймати обґрунтовані рішення в сучасних умовах.

В результаті, лавиноподібно наростають обсяги помилок, які допускає людство.

Зазначимо, що з середини XX століття почався процес широкого впровадження інформаційних комп'ютерних технологій (далі – ІКТ).

Це дозволяє вирішити окреслені вище проблеми:

- збору та обробки великих обсягів інформації (даних);
- збору та обробки даних про велику кількість суб'єктів та об'єктів;
- швидкого прийняття рішень, навіть, в режимі реального часу тощо.

Широке впровадження ІКТ в різні часи мало назви:

- комп'ютеризація
- інформатизація
- інформаційне суспільство
- цифровізація
- діджиталізація тощо

В кінцевому рахунку пропонуємо використовувати такий термін:
<u>інформаційне суспільство</u> *– це суспільство, в якому вся сукупність суспільних відносин з метою підвищення ефективності людської діяльності (ефективності прийняття рішень) в різних сферах реалізується на основі максимального використання ІКТ.*

Тож, в процесі цивілізаційного розвитку з'явились загрозливі цивілізаційні виклики, серед яких:

- виснаження планетарних ресурсів: чисте повітря; вуглеводи; корисні копалини, ліси, прісна вода; родючі землі.
- зниження стійкості екосистеми людства;
- перенасичені: міста, інфраструктури, виробництва, автомобілі тощо;
- глобальна нестача продовольства;
- погіршення екології та зміна клімату;
- надзвичайно високі темпи соціальних процесів;
- низька ймовірність достовірності прогнозування природних, соціальних, економічних, технічних і технологічних процесів і явищ;
- недостатність наявних обсягів інформації.

Сучасною реакцію на ці цивілізаційні виклики стала соціальна трансформація на базі цифрової трансформації.

Цифрова трансформація *– це соціальна трансформація, яка відбувається на основі максимального використання цифрових технологій таких як:*

- *Інтернет речей,*
- *Індустрія 4.0,*
- *штучний інтелект,*
- *робототехніка,*
- *обробка великих даних,*
- *хмарні обчислення,*
- *електронні комунікації,*
- *та багатьох інших.*

Інтернет речей (англ. Internet of Things, IoT) – це один з фундаментальних результатів 4-ї технологічної революції.

Технологічні революції – це відгук на концептуальний соціальний запит.

З огляду на принципи роботи технологій IoT дамо наступне визначення:
Інтернет речей *– це взаємодіючі комплекси і системи, що складаються з сенсорів, мікропроцесорів, виконавчих пристроїв, обчислювальних ресурсів програмних засобів, зокрема, програм штучного інтелекту передача даних між якими здійснюється за допомогою мережі Інтернет, які призначені для надання послуг і проведення робіт за участі або без участі людини в інтересах суб'єктів (юридичних або фізичних осіб).*

Таким чином, Інтернет речей – це взаємодіючі технологічні комплекси і системи, передача даних між якими здійснюється за допомогою мережі Інтернет та які призначені для надання послуг і проведення робіт за участі або без участі людини в інтересах суб'єктів (юридичних або фізичних осіб).

Що дає впровадження технологій Інтернету речей?
Наприклад в системі охорони здоров'я це:

- витрати на лікування хронічних захворювань – 60% від загальних витрат на медицину;
- дистанційний моніторинг для груп ризику зменшує витрати на медицину на 10–20%;
- зменшення хронічних захворювань за рахунок переходу до стратегії попередження та ранньої діагностики захворювань;
- збільшення тривалості життя – 10–15 років.

Що очікується від впровадження технологій Інтернету речей:

- 10–15% – економія на охорону здоров'я;
- 10–15 років – збільшення тривалості життя;
- 40–50% – збільшення врожайності;
- 15–20% збільшення пропускної здатності доріг у містах;
- 85–90% зменшення кількості автомобілів.

Що буде у майбутньому у сфері впровадження технологій Інтернету речей?

- 80–100 мільярдів підключень до мережі Інтернет (сьогодні – біля 16 млрд.);
- $7–19 трильйонів буде складати світовий ринок IoT;
- ($21,4 трлн. – США; $14,7 – Китай);
- 1 трлн. євро – буде складати ринок технологій IoT у Європі;
- Індустрія 4.0 – додатковий дохід:
- 30 млрд. євро (Німеччина);
- 110 млрд. євро (Євросоюз).

Іноземний досвід у сфері впровадження технологій Інтернету речей

США

- національна стратегія Інтернету речей – 2016 р.
- закон «Розвиток інновацій и сприяння Інтернету речей» – січень 2017 р.

Велика Британія

- «Цифрова стратегія Великої Британії 2017».

Японія

- «Стратегії росту Японії – 2020» (Індустрія 4.0, розвиток IoT, великих даних, робототехніки).

Китай

- $127,5 млрд. державна програма до 2020 року.
- 500 розумних міст – з 2017 р.

2. Політика Євросоюзу щодо розвитку Інтернету речей

В стратегії «Цифровий порядок денний для Європи» один з найперспективніших за потенціалом розвитку визначено напрям **технологій Інтернету речей (Internet of Things)**.

З початку 2000-х років спостерігалась динамічна поява великої кількості інформаційного матеріалу щодо вражаючих результатів застосування технологій IP в самих різноманітних сферах соціальної активності. В результаті, у 2010-2020 р. національні уряди і Європейське співтовариство в цілому:

- починають розглядати розвиток IP як пріоритетний напрямок внутрішньої політики;

- починають створювати альянси, загальноєвропейські та національні програми з розвитку впровадження Інтернету речей.

Наприклад, в Резолюції Європейського Парламенту від 17.02.2017 року зазначалось: «Існує нагальна потреба провести оцінки впливу на майбутнє цивільне законодавство створення в довгостроковій перспективі особливого юридичного статусу для роботів, наприклад, для найскладніших автономних роботів (роботів зі ШІ)».

3. Системні ризики та перешкоди впровадження Інтернету речей

Системні бар'єри

- відсутність державної стратегії та лідерів змін
- недостатнє розуміння цінностей Інтернету речей політичною елітою країни, керівниками галузей та бізнес-структур
- політичні
- освітянські та мотиваційні
- фінансово-економічні
- техніко-технологічні
- правового регулювання
- конфіденційності
- сумісності
- безпекові.

Проблеми безпеки

Основний принцип: безпека технологій IP (від англ. Internet Protocol) – забезпечення надійності, стійкості і якості здійснення тієї чи іншої людської діяльності.

Основні бар'єри та ризики на шляху розвитку IoT:
1. Інфраструктурна безпека (надійність, стійкість, резервування).
2. Технологічна безпека
3. Кібернетична безпека
4. Багаторівнева безпека
5. Безперервність безпеки
6. Інтеграція і взаємодія систем безпеки
7. Спеціальний менеджмент безпеки.

Правові проблеми застосування Інтернету речей

Базовий принцип – правове регулювання має сприяти використанню технологій IoT в інтересах людей.

Правові бар'єри та фактори ризику

Необхідна побудова прогнозів щодо:
- адміністративних, цивільних, кримінальних, фінансових, інформаційних відносин тощо;
- встановлення юридичної відповідальності;
- телекомунікацій та використання радіоспектра;
- забезпечення конкуренції;
- використання штучного інтелекту та роботів;
- застосування технологій блокчейну та криптовалют
- використання смарт контрактів;
- захисту інтелектуальної власності;
- захисту приватності;
- забезпечення безпеки і конфіденційності.

Концептуальна проблема правового регулювання

Традиційна правова доктрина права регулює суспільні відносини між людьми.

Традиційно система права формувалось після встановлення усталеної практики здійснення суспільних відносин, тобто після ретроспективного аналізу.

Терміни формування:
1. До кінця XIX сторіччя – це сотні років, іноді десятки років.
2. XX сторіччя – це десятки років, іноді декілька років.
3. XXI сторіччя – це декілька років.

Початок XXI сторіччя

Нагальна потреба у правовому регулюванні нових видів суспільних відносин, які:
- тільки почали з'являтись або
- будуть в майбутньому з'являтись.

ШІ сприймається як базова умова застосування технологій IoT, тому протягом останніх 1,5–2 років:

Національні стратегії розвитку штучного інтелекту
- біля 20 держав світу мають затверджені Національні стратегії;
- майже 10 з них визначили мету – стати державою №1 у світі у розвитку штучного інтелекту.

З'являється правова невизначеність при застосуванні.

Яке правове регулювання?
- технологій Інтернету речей;
- штучного інтелекту;
- роботів;
- робомобілей;
- технологій блокчейн;
- «хмарних» технологій;
- «великих даних»

Протягом наступних 20–30 років
Інформаційне право – це необхідна та важлива складова правового забезпечення будь-якої суспільної діяльності.

Однак, розвиток галузей права, насамперед, інформаційного права потребує *прогностичного підходу*.

Приклади ідентифікації правових проблем

Окремі галузі (медицина)
- Законодавче регулювання надання послуг е-медицини, зокрема, надання в дистанційному режимі.
- Встановлення меж та змісту юридичної відповідальності для медичного персоналу, операторів телекомунікацій, виробників обладнання та розробників програмного забезпечення.
- Правовий режим допуску на ринок медичних послуг автономного програмного забезпечення для мобільних засобів, дистанційній діагностики, інвазійних засобів, що керуються дистанційно тощо.
- Правовий режим допуску на ринок медичних послуг медичних приборів и діагностичних медичних приборів.
- Законодавчі вимоги щодо прозорості інформування населення про всі особливості надання медичних послуг з використання технологій IoT.
- Правове регулювання збору інформації та дистанційного доступу до е-картки пацієнта.

Телекомунікації:
- відміна ліцензування діяльності, лібералізація ринку, та введення економічних санкцій для порушників законодавства;
- створення прозорих умов для конкуренції;
- посилення регуляторної влади НКРЗІ;
- ЦОВЗ у формуванні державної та технічної політики.

Радіочастотний ресурс (далі - РЧР):
- режим Sharing, можливість створення віртуальних операторів стільникового зв'язку (англ. MVNO, mobile virtual network operator);
- принцип технологічної нейтральності у використанні РЧР;
- режим колективного та спільного користування спектром;
- використання білих діапазонів White Space РЧР;
- вторинний ринок (Spectrum trading) РЧР.

Розумне місто
- Юридичне визначення терміну «розумне місто».
- Прискорення прийняття рішень місцевими органами щодо інфраструктурних проектів.
- Правовий режим сумісного використання інфраструктурних об'єктів – електроенергетики, водопостачання, газопостачання, опалення, телекомунікацій, освітлення, відеоспостереження тощо.
- Юридичні вимоги щодо застосування сучасних технологій при новому будівництві або капітальному ремонті житлових та інфраструктурних об'єктів.
- Адаптація муніципального законодавства щодо сприяння впровадження технологій IoT.
- Законодавчі зміни щодо регулювання містобудівної діяльності, землекористування тощо.

Окремі технології:

1. 3D принтери:
- продукція, комплектуючі
- правові запобіжники щодо незаконного перехвату.

2. Робомобіль:
- зміни Віденської Конвенції щодо дорожнього руху;
- ліцензування допуску до експлуатації;
- правова регламентація перевірки системи автоматичного керування та програмного забезпечення;
- встановлення юридичної відповідальності за ДТП;
- правовий режим створення та функціонування дорожньої інфраструктури;
- регламентація керування використанням персональними даними.

3. Дрони:
- регулювання безпеки польотів по відношенню до суб'єктів і об'єктів, що знаходяться в повітрі та на землі;
- правовий режим введення оперативних обмежень;
- правовий режим надання дозволів на політ, на збір даних, ліцензій пілотам тощо.

Smart-контракт:

- Інтеграція правового регулювання в традиційну правову систему.
- Визначення юридичного статусу, вимог до його форми і змісту.
- Встановлення юрисдикції (за наявності транскордонних транзакцій).
- Особливості правовідносин, об'єкту та змісту.
- Визначення юридичних ризиків та обмежень використання.
- Правові механізми нагляду, встановлення відповідальності, зокрема при наявності помилок в комп'ютерній програмі.
- Правові вимоги щодо забезпечення достовірності фіксації подій в реальному світі, які є причиною для здійснення певних дій сторін.
- Правові механізми верифікації сторін контракту.
- Протиріччя між захистом персональних даних і відкритістю інформації по всіх транзакціях мережі блокчейнів.
- Пропозицій щодо судового процесу.

Напрями перспективних наукових досліджень

Потребує напрацювання теоретико-методологічних основ та практичних рекомендацій щодо:

1. Засад правового регулювання суспільних відносин в умовах «взаємодії»:

- людина – робот, робот – робот – за ініціативою людини;
- робот – людина, робот – робот – за ініціативою роботу.

2. Вдосконалення всієї системи правового регулювання в умовах прийняття рішень (проявів волевиявлення») роботами з штучним інтелектом.

3. Проведення теоретико-методологічних досліджень щодо вдосконалення (модернізації) правових моделей у:

- цивільному
- інформаційному (комп'ютерні технології, телекомунікації, використання радіочастотного ресурсу тощо)
- морському
- авіаційному
- медичному
- кримінальному
- адміністративному
- сімейному праві тощо.

4. Проведення правових досліджень, пов'язаних із використанням технологій IoT у:

- промисловості
- сільському господарстві
- банківський сфері
- енергетиці
- медицині
- освіті
- державному управлінні
- рітейлі
- збройних силах тощо.

5. Проведення правових досліджень, пов'язаних із забезпеченням:

- лібералізації та конкуренції на багатьох ринках
- захисту прав споживачів
- визначення відповідальності
- безпеки, зокрема кібербезпеки
- приватності (захисту персональних даних)
- захисту інтелектуальної власності та авторського права
- наданням телекомунікаційних послуг.

Перелік контрольних питань:

- Які фактори спричинили потребу у появі технологій Інтернету речей?
- Які перспективи для сфери охорони здоров'я у зв'язку із появою технологій Інтернету речей?
- З яких технічних елементів складаються технології IoT?
- Що таке соціальна трансформація і які фактори є її рушійною силою?
- Дайте характеристику поняттям «інформаційне» та «технологічне» суспільство.

Тест https://forms.gle/xVg7bNSDsC4yq2USA

2. Соціальне підприємництво та Інтернет речей

1. Місія, мета та завдання соціального підприємництва
2. Інтернет речей та охорона здоров'я
3. Інтернет речей та сільське господарство
4. Інтернет речей та зелена енергія
5. Інтернет речей та розумні міста
6. Інтернет речей та транспорт
7. Інтернет речей та роздрібна торгівля

1. Місія, мета та завдання соціального підприємництва.

Соціальне підприємництво – це підприємницька діяльність спрямована на інноваційну, суттєву та позитивну зміну у суспільстві. В той час коли бізнесмени концентровані на створенні фінансового прибутку, соціальні підприємці займаються збільшенням соціального капіталу. Вони задіяні у таких галузях, як освіта, охорона довкілля, боротьба з бідністю та права людини.

НЕ є соціальним підприємництвом:

- Корпоративна соціальна відповідальність бізнесу.
- Бізнес у соціальній сфері.
- Виробництво платних соціальних послуг організаціями різних форм власності.
- Організацією економічного співробітництва і розвитку було прийнято визначення поняття «соціальний капітал».

Соціальний капітал – це мережі з усталеними в них спільними нормами, цінностями та домовленостями, які сприяють співробітництву в цих мережах або серед груп таких мереж.

Залучення соціального капіталу сприяє економічному розвитку. Це є основою соціального підприємництва.

Економічний розвиток – це структурна та інституційна перебудова економіки у відповідності до викликів перед суспільством, які в сьогоднішніх умовах спрямовані на підвищення виробництва промислової продукції, покращення надання послуг населенню та підвищення їхнього рівня добробуту шляхом широкого використання сучасних технологій та інновацій.

Соціальне підприємництво – це діяльність, яка має три орієнтири: соціальний, ринковий та інноваційний.

Таким чином, запровадження сучасних технологій та інновацій, в тому числі, у вигляді IoT безпосередньо реалізує мету створення соціального підприємства, а саме – формування соціального капіталу та створення передумови для економічного розвитку.

Європейський Союз у жовтні 2011 року започаткував ініціативу щодо соціального бізнесу (Social Business Initiative – SBI), спрямовану на створення систем підтримки соціальних підприємств, що впроваджують економічні та соціальні інновації.

В рамках SBI Європейська Комісія розробила визначення соціального підприємництва на основі трьох ключових критеріїв:

- соціальна мета,
- обмежений розподіл прибутку,
- партисипативне управління (participatory governance).

Соціальне підприємство – це суб'єкт соціальної економіки, основною метою якого є соціальний вплив, а не отримання прибутку для своїх власників або акціонерів. Він працює, надаючи товари та послуги для ринку підприємницьким та інноваційним способом, і використовує свій прибуток, головним чином, для досягнення соціальних цілей. Управління ним здійснюється відкрито і відповідально, в тому числі, із залученням працівників, споживачів та зацікавлених сторін, на яких впливає комерційна діяльність такого підприємництва.

Таким чином,

Місія соціального підприємництва полягає у досягненні соціального результату з можливістю одержання прибутку.

Мета соціального підприємництва – це формування соціального капіталу та створення передумов для економічного розвитку.

Завдання соціального підприємництва – вирішення певної соціальної проблеми.

Можна з впевненістю стверджувати, що соціальне підприємництво, так само як і право, є інструментом вирішення певної проблеми, однак за рахунок економічного, а не юридичного механізму врегулювання.

Серед причини, які ускладнюють вчасне реагування законодавця на динамічну зміну суспільних відносин є:

- Перенасичення інформацією;
- «Білий шум»;
- Ускладнення перевірки достовірності інформації.

Рішення

Соціальне підприємництво, яке в змозі локалізувати певну соціальну проблему і вирішити її за допомогою економічних інструментів.

Застосування IoT є яскравим прикладом реалізації обов'язкової ознаки соціального підприємства, а саме використання інновацій.

Проблема дезінформації в багатьох сферах життєдіяльності людини є досить широкою з огляду на можливість поширення інформації через Всесвітню мережу Інтернет.

Позитивний досвід

Так, в 2016 році в Лондоні було зареєстровано соціальне підприємство, яке створило платформу репутації в Інтернеті Right of Reply. Вона дозволяє відновити контроль над своєю репутацією в Інтернеті та «говорити правду», спираючись на запатентований пошук та технологію блокчейну.

Дана платформа спрямована на забезпечення швидких, недорогих та юридично обґрунтованих рішень як для споживачів, так і для компаній задля своєчасного реагування на негативний або помилковий вміст щодо себе чи своєї організації.

Реалізація даного стартапу стала можливою завдяки:

- чіткому формуванню соціальної мети
- передачі частини доходу на благодійність
- використанню інноваційних технологій

Таким чином, причини застосування Інтернету речей:

- Обмеженість когнітивних можливостей людства.

- Протиріччя між вимогою щодо швидкості прийняття рішень та великими обсягами інформації, які необхідно враховувати та опрацьовувати при цьому.

Основна місія застосування Інтернету речей:

Спроможність забезпечити прийняття рішень, максимально адекватних поточній ситуації, в суспільних процесах завдяки можливості в режимі реального часу збирати та обробляти великі обсяги інформації (даних), зокрема інформацію про значну кількість об'єктів та суб'єктів задіяних в цих процесах, та приймати рішення або пропонувати рішення, які виробляються на основі спеціальних математичних алгоритмів, зокрема алгоритмів штучного інтелекту.

Успішність реалізації місії IoT полягає у наявності максимального сприятливого правового забезпечення.

Базові соціальні переваги застосування технологій Інтернету речей: застосування технологій Інтернету речей передбачає ефективне подолання соціальних проблем, тобто формування певної соціальної цінності – задоволення нагальних потреб суспільства в ситуаціях, де більш звичні механізми взаємодії не працюють або працюють з мінімальною користю.

Перші успішні практики використання IoT – сфера надання послуг.

2. Інтернет речай та охорона здоров'я

Перехід від парадигми організації лікування хвороби у пацієнтів ДО парадигми організації всеохоплюючої регулярної профілактики, попередження та ранньої діагностики захворювань

Мета – економічне зростання (людина як ресурс)

Проблема сфери охорони здоров'я – дискретність, тобто інтервал часу, спостереження за станом здоров'я – один раз на рік (при наявності профілактичних оглядів) або від декількох місяців до декількох років.

Рішення

- Обробка даних за допомогою штучного інтелекту (далі – ШІ);

- Збір даних за допомогою технологій IoT.

Американський вчений Д. Хантер зазначає: «потенціал ШІ дозволяє аналізувати величезну кількість даних при створенні ліків, для аналізу сканування очей, схильність до діабету тощо».

Європейська Комісія оприлюднила результати Індексу цифрової економіки та суспільства (DESI) за 2020 рік:

- Держави-члени вжили заходів з мінімізації поширення інфекції та підтримки систем охорони здоров'я, наприклад, шляхом впровадження програм і платформ для полегшення телемедицини та координації ресурсів охорони здоров'я.
- Криза COVID-19 показує, наскільки важливо забезпечити продовження урядової діяльності, коли існують заходи соціального дистанціювання. Успішна стратегія виходу з поточної пандемії потребує надійних цифрових державних послуг у всіх сферах, включаючи електронну охорону здоров'я – e-health (такі як телемедицина, електронні рецепти та обмін медичними даними) та використання передових технологій для вдосконалення державних послуг, в тому числі, Bid Data або AI.

Існуючий досвід України

2018 рік – представники КПІ ім. Ігоря Сікорського взяли участь у проекті програми «EUREKA».

«Future eHealth powered by 5G» – «Майбутня електронна сфера охорони здоров'я на основі технології 5G».
Мета – створити нові сервіси для моніторингу стану здоров'я пацієнтів, надати лікарям оперативний доступ до медичних баз даних тощо.

Вирішення проблеми зменшення дискретності спостереження за станом здоров'я кожної людини стає можливим тільки в умовах використання технологій IP.
Наприклад, в Швейцарії доставка крові буде здійснюватися за допомогою медичних дронів.

Консалтингова компанія Gartner прогнозує, що до 2020 року у 10% населення розвинених країн буде який-небудь орган або переносний пристрій, створений за допомогою 3D-друку, наприклад, буде створено протези і імплантати, причому хірурги будуть використовувати 3D-друк в кожній третій операції.

Економічний стимул – використання технологій IP у сфері охорони здоров'я задля скорочення витрат на лікування хронічних захворювань.

Алгоритм дій при впровадженні E-healthcare:

1. Організація системи збору фізіологічних даних людини спільно з даними його фізичної активності та їх передачі для використання лікарським персоналом клінік.

2. Обов'язкове використання накопиченої в індивідуальній медичній базі даних людини інформації, зібраної від різних датчиків, в різних діагностичних комп'ютерних комплексах.

3. Всі ці маніпуляції з даними про людину, включаючи їх інтеграцію, повинні бути явним чином їм схвалені і це схвалення повинно бути зафіксовано.

4. Проведення дослідження для встановлення кореляційної зв'язку між видами і змістом фізичної активності і вибором методики лікування захворювань для певних параметрів фізичного стану людини.

5. Встановлення методики визначення індивідуальних ризикових зон показників параметрів фізичного стану людини для різних видів захворювань і організація систем оповіщення як людини, так і медичного персоналу, який спостерігає за ним, про входження в ці ризикові зони.

7. Розробити оновлену модель страхової медицини з урахуванням впровадження технологій IP.

3. Інтернет речей та сільське господарство

Ініціатива Європейської Комісії «Європейський зелений курс» (від англ. - The European Green Deal) в плані реалізації даного курсу від 11 грудня 2019 року передбачила:

- Цифрові технології є найважливішим фактором, що сприяє досягненню цілей екологічної природоохоронної діяльності у багатьох галузях.

- Комісія вивчить заходи для забезпечення того, щоб цифрові технології, такі як штучний інтелект, 5G, хмарні та крайові обчислення та Інтернет речей, могли пришвидшити та максимізувати вплив політики щодо боротьби зі зміною клімату та захисту навколишнього середовища.

- Цифровізація також представляє нові можливості для дистанційного моніторингу забруднення повітря та води або для моніторингу та оптимізації використання енергії та природних ресурсів.

Єврокомісія визначила, що для досягнення Європейського Зеленого курсу необхідно переглянути політику щодо чистого енергопостачання в економіці, промисловості, виробництві та споживанні, масштабній інфраструктурі, транспорті, продовольстві та сільському господарстві, будівництві, оподаткуванні та соціальних виплатах.

Український досвід

Постанова КМУ від 24 січня 2020 р. № 33 «Про утворення міжвідомчої робочої групи з питань координації подолання наслідків зміни клімату в рамках ініціативи Європейської Комісії «Європейський зелений курс».

Серед основних завдань міжвідомчої робочої групи було визначено:

«застосування цифрових технологій, зокрема використання штучного інтелекту, хмарних технологій, Інтернету речей, стандартів зв'язку, мобільних мереж, та визначення їх впливу на довкілля з метою сприяння переходу до низьковуглецевого розвитку держави та зменшення ресурсоємності»

Проблеми, що стоять перед сільським господарством:

- формування і функціонування аграрного ринку та його інфраструктури;
- організація найвигіднішого по кількості задіяних ресурсів виробництва сільгосппродукції;
- створення ефективної маркетингової мережі просування сільськогосподарської продукції від виробника до споживача.

У дослідженні Європейського дослідницького кластера IP відзначається, що велику роль у вирішенні проблем сільського господарства, переробки його продукції і доставки її результатів до споживача можуть зіграти технології IP.

У доповіді про розумне сільське господарство вказується на кілька основних напрямків застосування технологій IP:

- Управління автопарком – відстеження сільськогосподарських машин.
- Землеробство, великі й малі поля сільського господарства.
- Моніторинг тваринництва.
- Інфраструктурні об'єкти сільського господарства – теплиці і стайні.
- Рибництво.
- Лісове господарство.

Моніторинг зберігання – ємності для води, паливні баки. Обробка полів, їх полив, моніторинг за кількістю опадів і поживних речовин в ґрунті, станом врожаю, прийняття рішення про необхідність використання гербіцидів і добрив, часу початку збирання врожаю, планування використання сільгосптехніки з метою мінімізації її простою і багато іншого може здійснюватися за допомогою використання технологій IP за мінімальною участю людини.

Інтернет речей дозволяє займатися «точним землеробством» за допомогою:

- геолокаційних сервісів
- спеціальних програм на базі геоінформаційних систем
- Використовуються
- дані GPS, ГЛОНАСС або Galileo
- також датчики
- супутникові світлини і аеросвітлини
- спеціальні програми для агроменеджмента на базі геоінформаційних систем (ГІС).

Фахівці університету штату Пенсильванія розробили сенсори, які дозволяють більш точно визначати момент, коли слід провести полив, і це дає можливість збільшити ефективність використання води.

Автоматизація процесу випасу тварин, контроль за їх переміщенням на ділянки з найбільш поживними рослинами.

4. Інтернет речей та зелена енергетика

Промисловий Інтернет речей (The Industrial Internet of Things, IoT). Індустрія 4.0. (Industrie 4.0)

Промисловий Інтернет речей складається з датчиків, комп'ютерів та мереж, які взаємодіють зі своїм середовищем для генерації даних для поліпшення процесів, формуючи цілі екосистеми, що з'єднують машини з іншими машинами та з людьми, які керують складними процесами, налаштованими на найдрібніші деталі складальних ліній, підвищують ефективність великомасштабної логістики ланцюгів поставок, розподілу і ринкового попиту.

Промисловий IoT напряму пов'язаний із питанням зеленої енергетики, адже дозволяє оптимізувати виробництво на конкретні потреби, а не на велику кількість виробленого товару.

Світовий економічний форум в Давосі 2015:

«промисловий Інтернет принесе безпрецедентні можливості, оскільки він буде поєднувати в собі глобальне охоплення Інтернету з новою можливістю контролю навколишнього фізичного світу, в тому числі машин, заводів та інфраструктури, які визначають сучасний ландшафт.
... При цьому дуже актуальними є нові важливі питання, такі як ланцюги створення вартості продукту, бізнес-моделі і робоча сила, вплив розвитку промислового Інтернету речей на існуючі галузі, визначення пріоритетності бізнес-процесів і урядових заходів, які повинні бути негайно прийняті, щоб забезпечити довгостроковий успіх».

Індустрія 4.0. на прикладі Німеччини:

- Задоволення індивідуальних вимог замовника.
- Підвищення гнучкості виробничих процесів.
- Оптимізація прийняття рішень.
- Підвищення продуктивності та ефективності використання ресурсів.
- Створення додаткових можливостей для створення нових послуг.
- Відповідь на демографічні зміни.
- Робота – життя – баланс.
- Конкурентоспроможна економіка з високими зарплатами.

Три останні складові є суто соціальними та становлять можливість реалізації соціальних потреб за рахунок впровадження технологій IoT.

5. Інтернет речей та розумні міста

Збільшення чисельності міського населення призводить до перевантаженості міст, що викликає нові загрози для суспільства. Наприклад, транспортний колапс, який можна спостерігати у великих містах з роками буду тільки збільшуватись. Підхід «старт міст» покликаний подолати ці проблеми за рахунок новітніх технологій.

Розумне місто можна розглядати як «місто, яке контролює та інтегрує умови функціонування для всіх його найважливіших інфраструктур, в тому числі доріг, мостів, тунелів, наземних і підземних залізничних шляхів, аеропортів, морські портів, комунікацій, водопроводів, електричних мереж, а також великих будівель, що допомагає краще оптимізувати свої ресурси, планувати профілактичні роботи з технічного обслуговування, а також контролювати питання безпеки при максимізації кількості послуг для своїх громадян». Наявність датчиків передачі інформації спеціалізованому суб'єкту цілеспрямовано дозволяє оптимізувати діяльність різних організацій та установ, які забезпечують умови життєдіяльності в містах. Зібрання даних рахунок таких датчиків дає можливість вчасно і повно здійснювати оцінку даних в режимі реального часу.

Це означає вчасне зібрання сміття після наповнення баку, максимальне розвантаження доріг від заторів, синхронізована робота світлофорів,

точкове використання сольових розчинів для боротьби з обмерзанням дорожнього покриття тощо.

Приклад розумних парковок вказує на раціональну можливість подолання проблеми з пошуком місця для автомобіля. Відповідна інформація буде вчасно надаватись власникам авто на їхні смартфони.

На завершення пропонуємо ще один приклад роботи старт міст – розумне освітлення, яке адаптується під рівень світла та, виходячи з цього запрограмоване його включити чи відключити, здійснюючи економію ресурсів. Все у старт містах організовується таким чином, щоб взаємодія в них була максимально оптимізованою, комфортною і безпечною для їх жителів, економною для місцевих служб життєзабезпечення таких міст.

6. Інтернет речей та транспорт

Існує цілком реалістичний прогноз, що найближчим часом робота транспорту за рахунок розвитку технологій Інтернету речей буде здійснюватись автономними автомобілями. Є декілька варіантів таких автомобілів: безпілотні автомобілі (AV), електричні автомобілі (EV) і повністю безпілотний автомобіль п'ятого покоління (A-EV). Окрім цього, автомобілі можуть бути оснащені операційною системою на основі штучного інтелекту (VOS).

Реалізація цієї ідеї дозволить суттєво скоротити час очікування таксі, а також зменшити кількість транспорту на дорозі, що одразу позитивно відобразиться й на екології через зменшення викиді в атмосферу. Це ще один чудовий приклад економії ресурсів за допомогою IoT.

Окрім цього, переваги на дорозі, згадані в темі розумних міст можуть бути синхронізованими з такими авто, що теж стане невимовною перевагою щодо комфортності життя в таких містах. Отже оптимізація ресурсу, в тому числі, часового є безумовною перевагою роботи технологій IoT в транспортній галузі.

7. Інтернет речей та роздрібна торгівля

Ідея технологій Інтернету речей в рітейлі теж не нова, адже вже реалізовується найбільш прогресивними гравцями на ринку. Так, Amazon практикує роботу магазинів без черг та продавців, а також запроваджує технологію автоматизованої доставки товарів дронами. Зменшення людського фактору є ідеєю, яка закладена технологіями Інтернету речей в рітейлі. Наприклад, мережа магазинів Novus визначає потребу і замовляє необхідний товар за рахунок роботи автоматизованої системи, яка на основі даних щодо динаміки продажів, наявності залишків товару самостійно робить аналіз та здійснює замовлення тоді, коли це необхідно й того, що потребує споживач в конкретний відрізок часу. Технологія розумного холодильника теж здобуває деталі більшого поширення в більш економічно розвинених країнах світу. Так, сенсори, які наявні в холодильнику інформують про нестачу чи необхідність закупки певних продуктів, які закінчуються в ньому, а також може самостійно замовляти через відповідні дрони по тій же технології як це робить Amazon.

Перелік контрольних питань:

- Які основні відмінності соціального підприємництва від традиційного бізнесу?

- На які три орієнтири орієнтується соціальне підприємництво? Якщо підприємницька діяльність спрямована на інноваційну, суттєву та позитивну зміну у суспільстві задля збільшення соціального капіталу, це новий вид підприємництва чи соціальна відповідальність бізнесу?

Тест у форматі https://forms.gle/inwj4Kb9UuH8Hz8x7

РОЗДІЛ II.

ЗАГАЛЬНОСИСТЕМНІ ПРАВОВІ ПРОБЛЕМИ ВПРОВАДЖЕННЯ ІНТЕРНЕТУ РЕЧЕЙ

3. Загальні проблеми безпеки впровадження та застосування Інтернету речей

1. Загальні проблеми безпеки, її види
2. Техніко-технологічні джерела загроз безпеки Інтернету речей
3. Особливості архітектурної та мережевої безпеки Інтернету речей
4. Функціональна безпека Інтернету речей
5. Хмарні сервіси, дата-центри та хмарні технології
6. Великі дані, інтелектуальний аналіз та дії

1. Загальні проблеми безпеки, її види

Проблеми національної, інформаційної, державної, економічної, зовнішньополітичної, особистої безпеки бажано розглядати в контексті розуміння категорії вищого порядку абстракції. Такою категорією є категорія «безпека».

Характерні властивості безпеки

Безпека будь-якої системи:
- це бажаний стан
- має системний характер
- має бути формально оцінена
- оцінка – величина кінцева
- стан безперервний в часі
- поняття конкретне
- поняття інтегральне.

Система – сукупність кінцевої множини взаємопов'язаних функціональних елементів, яка реалізує певну кількість інтегративних функцій, які є необхідними для забезпечення досягнення мети її існування (функціонування).

Динамічна система (далі - ДС) це система (біологічна, технічна чи соціальна), яка функціонує в умовах постійних внутрішніх та зовнішніх впливів різної природи та форм.

Впливи можуть мати як позитивний, так і негативний характер.

Позитивні впливи – впливи, які сприяють досягненню мети функціонування ДС і, як мінімум, не погіршують якісні характеристики цього функціонування.

Негативні впливи – впливи, які призводять до істотного погіршення якісних показників функціонування ДС і, навіть, можуть призвести до її руйнування (загибелі).

Пропонуємо розглянути деякі аспекти динамічої системи.

Самозбереження – це прагнення ДС забезпечити досягнення мети свого функціонування за наявності будь-яких негативних впливів.
Основним результатом самозбереження э максимальна нейтралізація дії негативних впливів, які заважають досягненню мети функціонування ДС.
Властивість самозбереження є підґрунтям процесів еволюції.
Самозбереження – атрибутивна властивість.
Самозбереження – це убезпечення від результатів дії негативних впливів або забезпечення стану безпеки ДС в умовах наявності будь-яких негативних впливів.
Самозбереження та безпека – атрибутивні властивості ДС. Безпека – бажаний стан для будь-якої системи
Безпека – це такий стан системи, при якому мінімізується шкода, яка може бути нанесена в результаті реалізації негативних впливів (загроз).

Визначення має високий ступінь універсальності та абстрагування за рахунок того, що прямо або побічно указуються, але не описуються (не конкретизується):
- система (об'єкт), відносно якої можуть бути реалізовані негативні впливи;
- стан системи, для якої визначається безпека;
- види і типи загроз, в результаті реалізації яких може бути нанесена шкода;
- види і розміри можливої шкоди.

Чому інформаційна безпека займає особливе місце? Тому, що:

- інформаційні відносини і процеси пронизують всі суспільні відносин, тому інформаційна безпека як складовий елемент повинна входити у все інші складові національної безпеки – зовнішньополітичну, військову економічну, екологічну та інші;
- в сучасних умовах, коли інформаційні комп'ютерні технології в масовому порядку впроваджуються в багато сфер людської
- діяльності, питання інформаційної безпеки набуває самостійного суспільного значення;
- зовнішні та внутрішні загрози інформаційної безпеки мають комплексний всеосяжний характер для всіх сфер діяльності людини, суспільства і держави.

Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» (2007)

Інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому здійснюється запобігання нанесенню 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.

2. Техніко-технологічні джерела загроз безпеки Інтернету речей

Основний принцип розвитку: всі технології, які дозволяють надати послугу і провести роботи комфортніше, дешевше, швидше, якісніше, безпечніше будуть імплементовані в IP.

Фактори:

1. Архітектура IB: багатозв'язна, багатовимірна, складна, адаптивна, багатофункціональна, ієрархічна або горизонтальна.
2. Ідентифікація всіх елементів IP і інших об'єктів.
3. Безшовна робота технологій передачі даних.
4. Ефективність користування радіочастотним ресурсом.
5. Зниження енергоспоживання і збільшення часу автономності.
6. Транскордонність взаємодії.
7. Підвищення надійності і стійкості.

Проблеми безпеки

Основний принцип: безпека технологій IP – забезпечення надійності, стійкості та ефективності будь-якої людської діяльності.

1. Інфраструктурна безпека (надійність, стійкість, резервування).
2. Технологічна безпека.
3. Кібернетична безпека – центральна проблема.
4. Багаторівнева безпека.
5. Безперервна безпеки.

6. Інтеграція і взаємодія систем безпеки різних систем і комплексів IP.
7. Спеціальний комплексній менеджмент безпеки.

Кібербезпека – інформаційна безпека в умовах використання комп'ютерних систем та/або телекомунікаційних мереж.

Проблеми правового регулювання

Основний принцип: правове регулювання має сприяти використанню технологій IP в інтересах суб'єктів.

Фактори:

1. Необхідність нових правових моделей для регулювання цивільних відносин, реформування телекомунікацій, ефективного використання спектра, забезпечення конкуренції, захисту інтелектуальної власності, забезпечення безпеки і конфіденційності;

2. Технології IP припускають здійснення взаємозв'язку типу машина-машина (M2M), але в інтересах людини;

3. Наявність комплексів IP з штучним інтелектом, які самостійно приймають рішення.

4. Транскордонність суспільних відносин, пов'язаних з IP.

Глобальні тренди

Технологічне прискорення. Поглиблення прірви

Технології прискорюють прогрес – збільшення розриву між переможцями і відстаючими;

Прискорений розвиток роботизації і штучного інтелекту – занадто швидкі зміни в економіці – неможливість розвитку бідних країн по шляху індустріалізації;

Прорив в біотехнологіях – революція в медицині – проблеми морального характеру.

Зміна природи конфлікту. Війна нового покоління

Імовірність виникнення конфліктів збільшується – терористичні загрози і нові технології;

Нові стратегії, технології змінюють характер конфлікту і види озброєнь;

Майбутні конфлікти націлені на руйнування об'єктів інфраструктури, системи соціальних зав'язків, а також державних функцій, особливо в умовах гібридних загроз.

3. Особливості архітектурної та мережевої безпеки Інтернету речей

Особливості архітектурної та мережевої безпеки Інтернету речей:

1) Мережі IoT можуть включати велику кількість пристроїв, тому архітектура безпеки повинна передбачати можливість роботи зі зростаючою кількістю пристроїв та їхніх даних.

2) Пристрої IoT повинні мати лише автентифікований та авторизований доступ до мережі. Цього можна досягти за допомогою різних засобів, зокрема, паролі та сертифікати. Пристрої IoT повинні бути авторизовані для доступу лише до певних ресурсів у мережі на основі їхньої ідентифікації та встановлених для них дозволів.

3) Дані, які передаються між пристроями IoT і мережею, повинні бути зашифровані, щоб запобігти прослуховуванню або перехопленню неавторизованими сторонами.

4) Створення безпечного бар'єру між пристроями IoT та Інтернетом задля блокування спроб несанкціонованого доступу.

5) Системи безпеки IoT повинні бути здатні виявляти та запобігати спробам вторгнення.

6) Конфіденційність даних: пристрої IoT можуть збирати і передавати конфіденційні дані. Архітектура безпеки повинна гарантувати, що ці дані захищені та безпечно зберігаються.

7) Система оновлення пристроїв IoT має передбачати та виявляти вразливі сторони системи безпеки задля запобігання використання їх зловмисниками.

8) Пристрої IoT можуть бути фізично вразливими, наприклад, навмисно пошкодженими чи викраденими. Відповідні заходи фізичної безпеки теж є важливим фактором, який потрібно враховувати.

9) Мережі та технології IoT мають відповідати різним нормам і стандартам, зокрема, GDPR. Архітектура безпеки повинна забезпечувати дотримання цих вимог, щоб уникнути юридичних і фінансових наслідків.

4. Функціональна безпека Інтернету речей

Комплексі та системи IP будуть безперервно забезпечувати людську діяльність у будь-який сфері.

Технології IP базуються на використанні комп'ютерних систем та мереж телекомунікацій (Інтернет).

Об'єкти з технологіями IP – об'єкти критичної інфраструктури.

Основні зони ризиків та бар'єрів:
- техніко-технологічні
- безпеки
- конфіденційності
- сумісності
- стандартизації
- правового регулювання.

Розвиток інформаційної інфраструктури:

- формування правових умов для забезпечення плюралізму і прозорості, засобів масової інформації;
- удосконалення правового регулювання обігу інформації в електронній формі (електронних документів, книг, журналів і т.п.);
- врахування правових особливостей використання інтернет-технологій для поширення масової інформації;
- удосконалення захисту інтелектуальної власності в умовах використання інтернет-технологій.
- подальша лібералізація регулювання ринку телекомунікацій з урахуванням процесів конвергенції;
- стимулювання побудови широкосмугових мереж доступу до Інтернету, в тому числі з використанням радіотехнологій;
- удосконалення інфраструктури телебачення і радіомовлення з урахуванням переходу на цифрові технології;
- створення стимулюючих умов для розвитку сфери програмування і виробництва комп'ютерної техніки і т.п.

Законодавчі обмеження щодо розповсюдження протизаконної інформації

- Дифамація
- Дезінформація та фейки
- Інформаційна війна
- Інформаційна агресія

Законодавча регламентація для мінімізації ризиків застосування ІКТ

Порядок проектування, розбудови, випробувань, передачі в експлуатацію та експлуатації складних ІКТ систем

Правові механізми забезпечення гарантованого супроводження ІКТ їх розробниками

Законодавче визначення об'єктів критичної інфраструктури, як об'єктів протиправних посягань

Несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації

Правові режими обмеження доступу до інформації

Закони про конфіденційну таємницю, лікарську таємницю, персональні дані, профілювання даних тощо

Технічний захист інформації

Закони про технічний, криптографічний захист інформації Захист інтелектуальної власності

Закони про захист інтелектуальної власності, авторського права за умови використання Інтернету.

Висновки

1) розвивати положення теорії інформаційного права,
2) створювати нове інформаційне законодавство,
3) вдосконалювати загальне та спеціальне інформаційне законодавство – необхідно з врахуванням положень інформаційної безпеки.

5. Хмарні сервіси, дата-центри та хмарні технології

Безпека є однією з найважливіших аспектів щодо хмарних сервісів, дата-центрів та хмарних технологій. Оскільки багато організацій зберігають та обробляють важливі дані у хмарних сервісах або дата-центрах, забезпечення безпеки має вирішальне значення. Зазначимо деякі аспекти безпеки щодо хмарних сервісів, дата-центрів та хмарних технологій:

1) Важливо забезпечити конфіденційність, цілісність та доступність даних у хмарних сервісах та дата-центрах. Це може включати шифрування даних, резервне копіювання та моніторинг даних для виявлення несанкціонованого доступу або зміни.

2) Захищені механізми аутентифікації та авторизації важливі для обмеження доступу до систем та даних.

3) Важливо виявляти та реагувати на можливі загрози в реальному часі.

4) Внутрішні загрози, такі як несанкціонований доступ співробітників або інсайдерські загрози, можуть бути також небезпечними. Тому важливо розробляти політики доступу, моніторинг дій користувачів і здійснювати систематичний аудит.

Загальна безпека хмарних сервісів, дата-центрів та хмарних технологій вимагає комплексного підходу та постійного моніторингу та оновлення заходів безпеки.

6. Великі дані, інтелектуальний аналіз та дії

Великі дані, інтелектуальний аналіз та дії передбачають обробку та аналіз великих обсягів даних для виявлення шаблонів, трендів та інсайтів. З точки зору права, ці області мають свої власні правові аспекти, які включають в себе вимоги щодо захисту особистих даних, авторського права та прав інтелектуальної власності, регуляторні вимоги, вимоги щодо зберігання даних, правила щодо кібербезпеки та вимоги до звітності та аудиту. Дотримання цих правових норм є важливим для забезпечення законності та безпеки у використанні великих даних та інтелектуального аналізу. В деяких сферах, таких як охорона здоров'я та фармацевтика, існують обов'язки щодо звітності та аудиту. Організації повинні представляти звіти про те, як вони зберігають, обробляють та забезпечують безпеку даних. У фінансовому секторі існують суворі правила щодо збереження даних. Банки та інші фінансові установи повинні дотримуватися діючих регуляторних вимог щодо збереження фінансових даних на певний строк. Це може включати вимоги до зберігання транзакцій та інших фінансових записів. У рамках Загального регламенту про захист даних (GDPR) в Європейському Союзі, компанії, які обробляють особисті дані європейців, повинні дотримуватися специфічних правил щодо збереження, обробки та передачі таких даних. Наприклад, організація, що збирає особисті дані клієнтів, повинна отримати їхню згоду на обробку та надавати їм право видалення своїх даних.

Перелік контрольних питань:

1. Надайте характеристику інформаційній безпеці в умовах використання комп'ютерних систем та/або телекомунікаційних мереж.

2. Що є основою національної безпеки в сучасному світі?

3. На яких правових засадах ґрунтується розвиток інформаційної інфраструктури?

4. Яким є стан системи, при якому мінімізується шкода, яка може бути нанесена в результаті реалізації загроз?

5. Які ризики від «недостатньої» інформації?

Тест https://forms.gle/FriEHyeJG46DYfTW7

4. Правове забезпечення кібербезпеки критичної інфраструктури Інтернету речей

1. Зміст та сутність правового забезпечення кібербезпеки
2. Основні міжнародні нормативно-правові акти формування глобальної культури кібербезпеки
3. Основні положення Європейської програми забезпечення безпеки критичної інфраструктури.
4. Принципи регулювання для створення європейського промислового, технологічного та дослідницького простору кібербезпеки.
5. Правові механізми забезпечення високого рівня мережевої безпеки та інформаційних систем в ЄС
6. Способи кримінального реагування на кібератаки інформаційних систем ЄС

1. Зміст та сутність правового забезпечення кібербезпеки

Закон України «Про основні засади забезпечення кібербезпеки України» містить наступні поняття з питань кібербезпеки:

кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі;

кіберпростір – середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних;

кіберзлочин – суспільно небезпечне винне діяння у кіберпросторі та/ або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України;

кіберзлочин – суспільно небезпечне винне діяння (у кіберпросторі) у середовищі, середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних та/ або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України;

Однак, в національних стратегіях різних держав немає ні загальноприйнятого, ні однозначного визначення кібербезпеки.

Зазначимо, що кібербезпека має важливе значення для функціонування і розвитку суспільства.

Безперешкодний доступ до послуг Інтернет, забезпечення цілісності та конфіденційності даних – це ті питання, які є основою кібербезпеки.

Термін «кібербезпека»

Дане поняття є суперечливим, але все ж набуло широкого поширення серед фахівців, а також в нормативно-правових документах як на національних рівнях, так і на міжнародному рівні.

Загальна ситуація, яка пов'язана з кібербезпекою

Кібербезпека – інформаційна безпека в умовах використання комп'ютерних систем та телекомунікаційних мереж.

Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» (2007) передбачає, що:

Інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому здійснюється запобігання нанесенню шкоди через:

1. неповноту, невчасність та невірогідність інформації, що використовується;
2. негативний інформаційний вплив;
3. негативні наслідки застосування інформаційних технологій;
4. несанкціоноване поширення, використання та порушення цілісності, конфіденційності та доступності інформації.

З урахуванням вищенаведеного аналізу, сформулюємо таке визначення кібербезпеки:

Кібербезпека це такий стан захищеності життєво важливих інтересів особистості, суспільства і держави, при якому мінімізується нанесення шкоди в умовах використання комп'ютерних систем та/або телекомунікаційних мереж через:

- неповноту, невчасність та невірогідність інформації, що використовується;
- негативний інформаційний вплив;
- негативні наслідки функціонування інформаційних технологій;
- несанкціоноване поширення, використання та порушення цілісності, конфіденційності та доступності інформації.

Отже, дане визначення кібербезпеки засноване на діалектичному зв'язку категорій загального і одиничного в сфері інформаційної безпеки.

Запропонований підхід дозволяє розглядати проблеми кібербезпеки з позицій напрацьованої теоретичної і практичної бази інформаційної безпеки і створювати несуперечливі моделі правового регулювання в цих сферах.

2. Основні міжнародні нормативно-правові акти формування глобальної культури кібербезпеки

Серед нормативних актів, які формували глобальну культуру кібербезпеки необхідно відзначити наступні:

1. Директива Європейського парламенту та Ради 2002/58/ЄС від 12 липня 2002 року, що стосується обробки персональних даних і захисту конфіденційності в секторі електронних комунікацій

2. Регламент ЄС 526/2013 про адміністративні та фінансові положення щодо ENISA: Цей регламент встановлює адміністративні та фінансові положення, що стосуються ENISA, зокрема стосовно його бюджету, управління персоналом та інших аспектів функціонування Агентства.

3. Директива ЄС 2016/1148 про забезпечення високого рівня загальної безпеки мереж і інформаційних систем в ЄС: Ця директива встановлює загальний підхід до кібербезпеки в ЄС та вимагає від держав-членів вжити заходів для покращення безпеки мереж та інформаційних систем.

4. Регламент ENISA (EU) 2019/881: Цей регламент прийнятий з метою зміцнення ролі та повноважень ENISA. Він встановлює правову основу для роботи Агентства та надає йому завдання в галузі кібербезпеки.

5. Інші нормативно-правові акти.

Наприклад, Директива Європейського парламенту та Ради 2002/58/ЄС від 12 липня 2002 року формує основні вимоги до:

- конфіденційності комунікацій, безпеки мереж та послуг,
- збереження даних про трафік абонента,
- комерційних повідомлень («спам»),
- довідників телефонних номерів абонентів,
- вимоги про нерозголошення телефонного номеру під час здійснення дзвінка.

1. Відповідно до Регламенту ЄС № 460/2004 від 10 березня 2004 року про створення Європейського агентства мережевої та інформаційної безпеки у Євросоюзі (далі – Агенство, ENISA European Network and Information Security Agency) було створено відповідне агентство.

2. Регламентом ЄС № 526/2013 від 21 травня 2013 р. про Агентство Європейського Союзу мережевої та інформаційної безпеки (ENISA) та скасування Регламенту (ЄС) № 460/2004 було оновлено ENISA із розширеним набором обов'язків та семирічним мандатом.

3. Регламентом ЄС 2019/881 Європейського Парламенту та Ради від 17 квітня 2019 року про ENISA та про сертифікацію кібербезпеки інформаційних та комунікаційних технологій та скасування Регламенту (ЄС) № 526/2013 (Закон про кібербезпеку) було передбачено постійний мандат даного Агентства.

Лише в одній еволюції нормативно-правових документів щодо даного Агентства очевидним стає те, що ЄС визначив питання кібербезпеки одним з пріоритетних та виявив недоцільним припинення діяльності Агентства.

Наразі воно є центром експертизи з питань кібербезпеки, яке здійснює допомогу у розробці та реалізації політики Союзу, пов'язаної з кібербезпекою та сприяє підвищенню рівня захисту мережевих та інформаційних систем ЄС.

3. Основні положення Європейської програми забезпечення безпеки критичної інфраструктури

1. Директива про конфіденційність та електронні комунікації, відома як Директива ePrivacy, визначає правила для постачальників послуг електронних комунікацій (оператори, провайдери), щодо використання даних своїх абонентів та гарантії забезпечення прав абонентів.

В Директиві викладено основні вимоги до:

- конфіденційності комунікацій;
- безпеки мереж та послуг;
- повідомлення про порушення безпеки даних;
- збереження даних про трафік абонента;
- комерційних повідомлень («спам»);
- довідників телефонних номерів абонентів;
- не розголошення телефонного номеру під час здійснення дзвінка.

4. Принципи регулювання для створення європейського промислового, технологічного та дослідницького простору кібербезпеки.

У 2004 році у Євросоюзі було створено Європейське агентство з питань мережевої та інформаційної безпеки, поточний мандат якого мав би закінчитися в березні 2012 року.

1. Регламент (ЄС) № 460/2004 Європейського Парламенту та Ради від 10 березня 2004 про створення Європейського агентства мережевої та інформаційної безпеки.

Місія Європейського агентства з питань мережевої та інформаційної безпеки (Агентство, ENISA) це допомога ЄС та державам-членам у:

- забезпеченні високого та ефективного рівня мережевої та інформаційної безпеки;
- розвитку культури мережевої та інформаційної безпеки на благо громадян, споживачів, підприємств та організацій державного сектору Європейського Союзу;
- сприянні безперебійному функціонуванню внутрішнього ринку.

Агентство Європейського Союзу з питань кібербезпеки (ENISA)

Регламент (ЄС) 2019/881 Європейського Парламенту та Ради від 17 квітня 2019 року про ENISA (Агентство Європейського Союзу з питань кібербезпеки) та про сертифікацію кібербезпеки інформаційних та комунікаційних технологій та скасування Регламенту (ЄС) № 526/2013 (Закон про кібербезпеку) набув чинності 27.06.2019 р. ENISA має постійний мандат(було Агентство Європейського Союзу мережевої та інформаційної безпеки (ENISA).

Новели:

1. ENISA – Агентство Європейського Союзу з питань кібербезпеки

2. – постійний мандат.

3. Сертифікація кібербезпеки – полегшить бізнес через кордон, а покупці краще зрозуміють особливості безпеки товару чи послуги.

4. Кіберстійкість – покращить реакцію Союзу на кібератаки, підвищить кіберстійкість та підвищить довіру до Єдиного цифрового ринку ЄС.

5. Політика – підтримка Єврокомісії та держав-членів у впровадженні європейської політики у сфері кібербезпеки.

6. Розкриття вразливості – допомога у встановленні та впровадженні на добровільній основі політики розкриття вразливих місць.

7. Нові статутні органи – Правління, Національна група офіцерів зв'язку та Консультативна група.

Місія Європейського агентства з питань з питань кібербезпеки (Агентство, ENISA) полягає у:

1. досягненні високого загального рівня кібербезпеки в усьому Союзі, в тому числі шляхом активної підтримки держав-членів, установ, органів, офісів та агентств Союзу у покращенні кібербезпеки;

2. наданні консультацій та досвіду з питань кібербезпеки для установ, органів, офісів та агентств Союзу, а також для інших зацікавлених сторін Союзу;

3. сприянні зменшенню фрагментації внутрішнього ринку, виконуючи завдання, покладені на нього згідно з цим Регламентом.

Цілі Агентства:

1. бути центром експертизи з питань кібербезпеки завдяки її незалежності, науково-технічної якості наданих консультацій, допомоги та інформації, яку вона надає, прозорості її операційних процедур, методів роботи та ретельності. у виконанні своїх завдань;
2. надавати допомогу установам, органам, установам та агенціям Союзу, а також державам-членам у розробці та реалізації політики Союзу, пов'язаної з кібербезпекою, включаючи галузеву політику щодо кібербезпеки.
3. підтримувати розбудову потенціалу та готовність у всьому Союзі для підвищення захисту їх мережевих та інформаційних систем, розвитку та вдосконалення здатності до кіберстійкості та реагування, а також розвивати навички та компетенції у сфері кібербезпеки;
4. сприяє співпраці, включаючи обмін інформацією та координацію на рівні Союзу, між зацікавленими сторонами з питань кібербезпеки;
5. сприяє збільшенню можливостей кібербезпеки на рівні Союзу щодо запобігання та реагування на кіберзагрози, зокрема у разі транскордонних інцидентів;
6. сприятиме створенню системи и використанню європейської сертифікації з кібербезпеки з метою уникнення фрагментації внутрішнього ринку;
7. сприятиме підвищенню рівня обізнаності у сфері кібербезпеки, включаючи кібергігієну та кіберграмотність серед громадян, організацій та підприємств.

ENISA сприяє розробці та впровадженню політики та права ЄС шляхом:

надання допомоги:

1) шляхом надання її незалежної думки та аналізу, а також проведення підготовчих робота;
2) з таких питань, як управління ризиками, звітування про випадки, обмін інформацією;
3) в розробці та просуванні політики кібербезпеки, пов'язаної із підтримкою загальної доступності та цілісності публічного ядра відкритого Інтернету.

підтримання:

4) розробка та реалізація політики Союзу у сфері електронної ідентичності та довірчих служб;
5) підвищення рівня безпеки електронних комунікацій;
6) захисту даних та конфіденційності;
7) регулярного перегляду діяльності політики Союзу шляхом підготовки щорічного звіту про стан виконання відповідної законодавчої бази з кібербезпеки.

нарощування потенціалу

ENISA надає допомогу з метою:

8) покращення запобігання, виявлення та аналізу та можливості реагувати на кіберзагрози та інциденти, надаючи їм знання та досвід;
9) створення та впровадження політики розкриття вразливих місць на громадських засадах;
10) відповідної підтримки комп'ютерної групи реагування на надзвичайні ситуації для установ, органів та агентств Союзу (CERTEU);

ENISA підтримує обмін інформацією в секторах та між ними, зокрема у галузях, перелічених у Додатку II до Директиви (ЄС) 2016/1148, шляхом надання кращих практик та вказівок щодо наявних інструментів, процедур, а також щодо вирішення регуляторних проблем, пов'язаних з обміном інформацією.

Операційне співробітництво на рівні Європейського Союзу

ENISA оперативно співпрацює з державами-членами, установами, органами, офісами та агенціями Союзу, а також між зацікавленими сторонами.

ENISA співпрацює та взаємодіє з установами, органами, офісами та агенціями Союзу, включаючи CERT-EU, зі службами, що займаються кіберзлочинністю, та з наглядовими органами, що займаються захистом конфіденційності та особистих даних, з метою вирішення спільних проблем, у тому числі шляхом:

1. обмін ноу-хау та найкращими практиками;
2. надання консультацій та видача вказівок з відповідних питань, пов'язаних з кібербезпекою;
3. встановлення практичних заходів для виконання конкретних завдань після консультації з Комісією.

ENISA надає підтримку шляхом:

1. консультування щодо вдосконалення запобігання, виявлення та реагування на інциденти та щодо конкретної кіберзагрози;
2. надання допомоги в оцінці інцидентів, що мають значний або істотний вплив шляхом надання експертизи та сприяння технічному вирішенню таких інцидентів;
3. навчання з питань кібербезпеки та надає підтримку в організації навчань з питань кібербезпеки за їх запитами;
4. масштабну комплексну діяльність на дворічній основі;
5. галузеві навчання з питань кібербезпеки на рівні Союзу.
6. підготовку регулярного поглибленого звіту про технічну ситуацію в кібербезпеці ЄС щодо інцидентів та кіберзагроз.

ENISA сприяє розвитку спільної реакції на масштабні транскордонні інциденти або кризи, пов'язані з кібербезпекою, головним чином шляхом:

a. узагальнення та аналіз звітів з національних джерел;
b. забезпечення ефективного обміну інформацій;
c. сприяння технічному вирішенню таких інцидентів чи криз;
d. перевірки планів співпраці щодо реагування на інциденти чи кризи на рівні Союзу та тестування таких планів на національному рівні.

Сертифікаційна рамка кібербезпеки Європейського Союзу (EU Cybersecurity Certification Framework) – це ініціатива ЄС, спрямована на створення єдиної системи сертифікації та маркування продуктів, послуг та процесів у галузі кібербезпеки. Ця рамка спроектована для забезпечення високого рівня кібербезпеки в ЄС та забезпечення довіри споживачів до цифрових продуктів та послуг.

Агентство Європейського Союзу з питань кібербезпеки (ENISA) (European Union Agency for Cybersecurity) грає ключову роль у впровадженні цієї рамки. ENISA є незалежним органом ЄС, створеним для підтримки та координації дій у галузі кібербезпеки в ЄС. Однією з його головних функцій є надання технічної та експертної підтримки при розробці та впровадженні стандартів безпеки, які стосуються продуктів та послуг у сфері кібербезпеки.

Робоча програма європейської сертифікації кібербезпеки:

- визначає ***стратегічні пріоритети*** майбутніх європейських схем сертифікації кібербезпеки;
- ***включає перелік продуктів ІКТ, ІКТ-послуг та ІКТ-процесів*** або їх категорій, які ***рекомендовані*** до включення до сфери європейської схеми сертифікації кібербезпеки, на основі наступного:
  - наявність та розробка **національних схем сертифікації кібербезпеки**;
  - наявність **відповідного законодавства** чи політики Союзу чи держав-членів;
  - наявність **ринкового попиту**;
  - розвиток ландшафту кіберзагроз;
  - **запит на підготовку конкретної схеми-кандидата** Європейській групі з сертифікації кібербезпеки (ECCG).

У контексті Сертифікаційної рамки кібербезпеки ЄС ENISA відіграє важливу роль у сприянні створенню та підтримці єдиної системи сертифікації, яка б забезпечувала високий рівень кібербезпеки продуктів та послуг на ринку ЄС. ENISA також сприяє обміну інформацією та координації між державами-членами ЄС у сфері кібербезпеки та допомагає визначити та вирішити проблеми, пов'язані з кібербезпекою.

Забезпечення кібербезпеки в IoT є складною і тривалою задачею, і вимагає спільних зусиль виробників пристроїв, розробників програмного забезпечення, операторів мереж і організацій, які використовують IoT.

З огляду на європейський досвід, варто розглянути відзначити схеми сертифікації кібербезпеки в ЄС. Цілями безпеки європейських схем сертифікації кібербезпеки є:

- ***захищати*** збережені, передані або іншим чином оброблювані дані від:
  - випадкового або несанкціонованого зберігання, обробки, доступу чи розкриття,
  - випадкового або несанкціонованого знищення, втрати чи зміни або відсутності доступності,

  протягом усього життєвого циклу продукту ІКТ, ІКТ-послуги чи ІКТ;
- ***мандатний принцип доступу*** – уповноважені особи, програми чи машини можуть ***мати доступ лише*** до даних, послуг або функцій, на доступ до яких вони мають право; виявляти та документувати відомі залежності та вразливості;
- ***документування дій*** – фіксувати, які дані, послуги чи функції були доступні, використані чи оброблені іншим способом, у який час та ким;
- ***контроль дій*** – можливість перевірки, до яких даних, служб чи функцій зверталися, використовувались чи іншим чином оброблялися, у який час та ким;
- перевірити, чи продукти ІКТ, ІКТ-послуги та ІКТ-процеси ***не містять відомих вразливих місць***;
- ***відновлення функціонування*** – своєчасно відновити наявність та доступ до даних, послуг та функцій у разі фізичного чи технічного інциденту;
- ***гарантування***, що ІКТ-продукти, ІКТ-послуги та ІКТ-процеси:
  - захищені за замовчуванням та дизайном;
  - забезпечені сучасними програмними та апаратними засобами, які не містять загальновідомих вразливих місць, та забезпечені механізмами безпечного оновлення.

5. Правові механізми забезпечення високого рівня мережевої безпеки та інформаційних систем в ЄС

Адміністративна та управлінська структура ENISA

1) Правління;

2) Виконавча рада;

3) Виконавчий директор;

4) Консультативна група ENISA;

5) національна мережа офіцерів зв'язку.

Склад Правління

Правління складається з одного члена, призначеного кожною державою-членом, та двох членів, призначених Комісією.

Усі члени мають право голосу.

Кожен член Правління має заступника. Цей заступник представляє члена у відсутності члена.

Члени Правління та їх заступники призначаються на основі їхніх знань у галузі кібербезпеки з урахуванням їх відповідних управлінських, адміністративних та бюджетних навичок.

Комісія та держави-члени докладуть зусиль для обмеження обігу своїх представників у Правлінні, щоб забезпечити безперервність роботи Правління. Комісія та держави-члени прагнуть досягти гендерного балансу.

Голова Правління

Правління обирає голову та заступника голови з числа своїх членів більшістю у дві третини членів.

Їх термін повноважень складає чотири роки, який може бути поновлений один раз.

Якщо, однак, їхнє членство в Правлінні закінчується в будь-який час протягом терміну їх повноважень, термін їх повноважень автоматично закінчується на цю дату.

Заступник голови замінює Голову за посадою, якщо Голова не може виконувати його обов'язки.

Інші розділи Директиви.

Виконавча рада як допоміжний орган Правління:
a. готує рішення, які приймаються Правлінням;
b. забезпечує спостереження за висновками та рекомендаціями, що випливають з розслідувань Європейського бюро протидії шахрайству (фр. Office européen de lutte anti-fraude – OLAF) та різних внутрішніх або зовнішніх аудиторських звітів та оцінок;

c. допомагає та консультує Виконавчого директора у виконанні рішень Правління з адміністративних та бюджетних питань;
d. складається з п'яти членів, які призначаються з числа членів Правління;
e. одним із членів є Голова Правління, який може також очолювати Виконком, а інший – один із представників Комісії.
f. строк повноважень членів Виконавчої ради складає чотири роки. Цей строк може бути поновлюваний.

Правління встановлює правила процедури Виконавчої ради.

У разі необхідності через невідкладність, Виконавчий комітет може приймати певні тимчасові рішення від імені Правління, зокрема з питань адміністративного управління, включаючи припинення делегування повноважень органу, що призначає, та бюджетних питань.

Про будь-які подібні тимчасові рішення повідомляється Правлінню без зайвих затримок.

Потім Правління приймає рішення про затвердження чи відхилення тимчасового рішення не пізніше трьох місяців після прийняття рішення.

Виконавча рада не приймає рішень від імені Правління, які потребують схвалення більшості в дві третини членів Правління.

Обов'язки виконавчого директора
1) незалежно керує ENISA;
2) підзвітний Правлінню;
3) звітує перед Європейським Парламентом та Європейською Радою про виконання своїх обов'язків, коли його запросять.

Несе відповідальність за:
a. щоденне управління ENISA;
b. виконання рішень, прийнятих Правлінням;
c. підготовка проекту єдиного програмного документа та подання його на розгляд Правління перед його поданням до Комісії;
d. виконання єдиного програмного документа та звітування перед Правлінню;

e. підготовка зведеного річного звіту про діяльність ENISA, включаючи виконання річної робочої програми ENISA, та представлення його Правлінню для оцінки та прийняття;
f. виконання інших завдань, покладених на цього Виконавчого директора.

Виконавчий директор може:
g. створити спеціальні робочі групи, що складаються з експертів, включаючи експертів компетентних органів держав-членів. Порядок призначення виконавчих директорів експертів робочих груп та функціонування робочих груп визначаються у внутрішніх правилах роботи ENISA.
h. створити місцеві представництва в державах-членах.

Загальні положення щодо ENISA

ENISA є органом Союзу та має Союзну правосуб'єктність.

У кожній державі-члені ENISA має найбільш широку правоздатність, надану юридичним особам відповідно до національного законодавства.

Зокрема, він може придбати або розпоряджатися рухомим та нерухомим майном та бути учасником судочинства.

ENISA представляє виконавчий директор.

Інші розділи:
1) Відповідальність ENISA;
2) Мовні домовленості;
3) Захист персональних даних;
4) Співпраця з третіми країнами та міжнародними організаціями;
5) Правила безпеки щодо захисту конфіденційної не засекреченої інформації та секретної інформації;
6) Договір про штаб-квартиру та умови експлуатації;
7) Адміністративний контроль.

Європейська система сертифікації кібербезпеки

Мета:
1) поліпшення умов для функціонування внутрішнього ринку;
2) шляхом підвищення рівня кібербезпеки;
3) узгоджений підхід до європейських схем сертифікації кібербезпеки;
4) єдиний цифровий ринок для ІКТ-продуктів, ІКТ-послуг та ІКТ-процесів;
5) впровадження механізму встановлення європейських схем сертифікації кібербезпеки;
6) Засвідчення того, що продукти ІКТ, ІКТ-послуги та ІКТ-процеси відповідають визначеним вимогам безпеки.

Мета забезпечення кібербезпеки – забезпечити:
доступність, достовірність, цілісність або конфіденційність даних, які зберігаються, передаються або оброблюються, або функцій або послуг, пропонованих або є доступними через продукти, послуги та процеси протягом їх життєвого циклу.

Робоча програма європейської сертифікації кібербезпеки
a. визначає стратегічні пріоритети майбутніх європейських схем сертифікації кібербезпеки
b. включає перелік продуктів ІКТ, ІКТ-послуг та ІКТ-процесів або їх категорій, які рекомендовані до включення до сфери європейської схеми сертифікації кібербезпеки, на основі наступного:
c. наявність та розробка національних схем сертифікації кібербезпеки,
d. наявність відповідного законодавства чи політики Союзу чи держав-членів;
e. наявність ринкового попиту;
f. розвиток ландшафту кіберзагроз;
g. запит на підготовку конкретної схеми-кандидата Європейській групі з сертифікації кібербезпеки (ECCG).
h. Перша робоча програма Союзу публікується до 28 червня 2020 р.
i. Оновлення не рідше одного разу на три роки та, якщо це необхідно, частіше.

Цілі безпеки європейських схем сертифікації кібербезпеки

1) захищати збережені, передані або іншим чином оброблювані дані від:
   - випадкового або несанкціонованого зберігання, обробки, доступу чи розкриття;
   - випадкового або несанкціонованого знищення, втрати чи зміни або відсутності доступності;
   - протягом усього життєвого циклу продукту ІКТ, ІКТ-послуги чи ІКТ;

2) мандатний принцип доступу – уповноважені особи, програми чи машини можуть мати доступ лише до даних, послуг або функцій, на доступ до яких вони мають право;

3) виявляти та документувати відомі залежності та вразливості;

4) документування дій – фіксувати, які дані, послуги чи функції були доступні, використані чи оброблені іншим способом, у який час та ким;

5) контроль дій – можливість перевірки, до яких даних, служб чи функцій зверталися, використовувались чи іншим чином оброблялися, у який час та ким;

6) перевірити, чи продукти ІКТ, ІКТ-послуги та ІКТ-процеси не містять відомих вразливих місць;

7) відновлення функціонування – своєчасно відновити наявність та доступ до даних, послуг та функцій у разі фізичного чи технічного інциденту;

8) гарантування, що ІКТ-продукти, ІКТ-послуги та ІКТ-процеси:

9) захищені за замовчуванням та дизайном;

10) забезпечені сучасними програмними та апаратними засобами, які не містять загальновідомих вразливих місць, та забезпечені механізмами безпечного оновлення.

Інші положення щодо сертифікації

b. Запит на європейську схему сертифікації кібербезпеки
c. Підготовка, прийняття та перегляд європейської схеми сертифікації кібербезпеки
d. Рівні надійності європейських схем сертифікації кібербезпеки
e. Самооцінка відповідності
f. Складові європейських схем сертифікації кібербезпеки
g. Додаткова інформація про кібербезпеку для сертифікованих ІКТ-продуктів, ІКТ-послуг та ІКТ-процесів
h. Сертифікація кібербезпеки
i. Національні схеми та сертифікати щодо кібербезпеки
j. Національні органи з сертифікації кібербезпеки
k. Експертна оцінка
l. Органи з оцінки відповідності
m. Повідомлення
n. Європейська група з сертифікації кібербезпеки
o. Право подати скаргу
p. Право на ефективний судовий засіб захисту
q. Штрафні санкції.

6. Способи кримінального реагування на кібератаки інформаційних систем ЄС

Під віданням Агентства ENISA є питання протидії кібератакам.

Як зазначено в Регламенті ЄС 2019/881 від 17 квітня 2019 року, «кібератаки як явище стаються дедалі частіше, і зв'язана економіка й суспільство як найбільш вразливі до кіберзагроз та кібератак вимагають надійнішого захисту.

Кібератаки часто носять транскордонний характер.

Компетенції відповідних органів у сфері кібербезпеки та правозастосування та вживані ними заходи з реагування в рамках їхніх політик переважно обмежені національними рамками».

Для вирішення цієї проблеми необхідно:

1) скоординоване реагування в межах ЄС на основі спеціальних політик та взаємної допомоги між державами-учасницями.
2) необхідність регулярних оцінювань стану кібербезпеки та стійкості.
3) систематичні прогнози проблем та загроз, які можуть постати.

ENISA повинна регулярно готувати детальний технічний звіт ЄС про стан кібербезпеки стосовно інцидентів та кібератак на основі:

a. доступної для громадськості інформації,
b. власного аналізу та звітів,
c. наданої інформації від команди CSIRT держав-членів
d. наданої інформації від єдиних контактних пунктів з безпеки мережевих та інформаційних систем («єдині контактні пункти»), створеними відповідно до Директиви (ЄС) 2016/1148, Європейським центром кіберзлочинності у Європолі, Розвідувально-ситуаційним центром Європейського Союзу (EU INTCEN) при Європейській службі зовнішніх справ.

Передбачається заохочення суб'єктів, що здійснюють розробку ІКТ до підвищення рівня забезпечення безпеки задля того, щоб імовірність виникнення кібератак та потенційного впливу від них була мінімальною.

Концепція вбудованої безпеки забезпечення безпеки:

e. продукту ІКТ,
f. послуги ІКТ
g. процесу ІКТ.

Серед термінологічної складової варто виділити, зокрема, «незаконний доступ», який вважається таким у випадку, якщо його вчинено шляхом порушення заходів безпеки; «незаконне перехоплення», що полягає у здійсненні навмисного перехоплення за допомогою технічних засобів не публічної передачі комп'ютерних даних інформації з системи.

Великий акцент робиться на міжнародному співробітництві з партнерами за межами ЄС.

Кібербезпека є невід'ємною частиною безпеки європейців.

Поліпшення кібербезпеки є надзвичайно важливим для:

1) щоб люди могли довіряти інноваціям, підключенню та автоматизації та отримувати вигоди від них;
2) захисту основних прав і свобод, включаючи права на приватність та захист персональних даних;
3) свободи вираження поглядів та інформації.

Нова Стратегія кібербезпеки ЄС для цифрового десятиріччя утворює ключовий компонент політики «2030 Цифровий компас: європейський шлях протягом цифрового десятиліття».

СТІЙКІСТЬ, ТЕХНОЛОГІЧНИЙ СУВЕРЕНІТЕТ І ЛІДЕРСТВО

Критична інфраструктура та основні послуги ЄС дедалі більше взаємозалежні та оцифровані.

Все, що підключено до Інтернету речі в ЄС:

- автоматизовані автомобілі;
- системи промислового управління;
- побутова техніка;
- ланцюжки поставок тощо,

повинно бути:

- захищеним, спроектованим із врахуванням кіберінцидентів;
- швидко виправлено після виявлення вразливостей.

Це є фундаментальним для надання приватному та державному сектору ЄС можливості вибору з найбільш безпечної інфраструктури та послуг.

Стратегічні ініціативи

В майбутньому ЄС повинен забезпечити заходи регулювання Інтернету безпечних речей;

Інтернет безпечних речей

Правила внутрішнього ринку ЄС включають захист від небезпечних товарів та послуг.

Комісія:

1) опрацьовує прозорі рішення щодо безпеки та сертифікації згідно із Законом про кібербезпеку;
2) затверджує робочу програму Союзу (1 квартал 2021 р.) щодо прийняття європейських схем сертифікації кібербезпеки із стимулюванням безпечних продуктів та послуг без шкоди для ефективності;
3) по мірі поширення Інтернету речей буде вимагати посилення дій як для забезпечення загальної стійкості, так і для підвищення кібербезпеки;
4) розгляне комплексний підхід, включаючи можливі нові горизонтальні правила для посилення кібербезпеки всіх підключених продуктів та супутніх послуг, розміщених на внутрішньому ринку.

Перелік контрольних питань:

1. В чому полягає зміст Директиви про конфіденційність та електронні комунікації?

2. В чому суть місії Агентства Європейського Союзу з питань кібербезпеки?

3. Які цілі Агентства Європейського Союзу з питань кібербезпеки?

4. Який суб'єкт є центром експертизи з питань кібербезпеки в ЄС?

5. Які органи включає адміністративна та управлінська структура ENISA?

6. Сформулюйте та порівняйте поняття інформаційної безпеки та кібербезпеки.

7. Дайте характеристику принципам європейських схем сертифікації кібербезпеки.

Тест https://forms.gle/YtSBXNYezVZgmKu6

5. Правові особливості захисту персональних даних

Загальний регламент захисту персональних даних GDPR

1. Основні положення Європейського регламенту
2. Законодавче регулювання обробки персональних даних компетентними органами у кримінальній сфері

1. Основні положення Європейського регламенту щодо захисту особистих даних осіб та їх вільного переміщення

Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС.

Регламент має 11 глав (99 статей), включаючи наступне:

1. Загальні положення;
2. Принципи;
3. Права суб'єкта даних;
4. Контролер та процесор;
5. Передача персональних даних третім країнам або міжнародним організаціям;
6. Незалежні органи нагляду;
7. Співпраця та послідовність;
8. Засоби захисту, відповідальність та штрафні санкції;
9. Положення, що стосуються конкретних ситуацій обробки;
10. Делеговані акти та акти виконання;
11. Заключні положення.

Регламент (ЄС) 2018/1725 Європейського парламенту і Ради від 23 жовтня 2018 року про захист фізичних осіб стосовно обробки персональних даних установами, органами, установами та агентствами Союзу і про вільне переміщення таких осіб дані і скасовує Регламент (ЄС) № 45/2001 і Рішення № 1247/2002 / ЄС набрав чинності з 12.12.2019 р.

Предмет і цілі

Регламент:

1) установлює норми щодо захисту фізичних осіб у зв'язку з опрацюванням персональних даних і норми про вільний рух персональних даних.
2) захищає фундаментальні права і свободи фізичних осіб, зокрема їхнє право на захист персональних даних.

Вільний рух персональних даних у всьому Союзі не повинно бути обмежено чи заборонено із причин, пов'язаних із захистом фізичних осіб у зв'язку з опрацюванням персональних даних.

Сфера дії

Регламент:

поширюється на опрацювання персональних даних повністю чи частково:

- із застосуванням автоматизованих засобів;
- із застосуванням неавтоматизованих засобів, які формують частину картотеки або призначені для внесення до картотеки.

не застосовують до опрацювання персональних даних:

- в ході діяльності, що виходить за межі дії права Союзу;
- державами-членами під час реалізації діяльності, що виходить за межі глави 2 розділу V Договору про ЄС;
- фізичною особою під час задоволення особистих або побутових потреб;
- компетентними органами для цілей запобігання, розслідування, виявлення або переслідування за вчинення кримінальних злочинів або для виконання кримінальних покарань, у тому числі, для захисту від загроз громадській безпеці або запобігання таким загрозам.

Територіальна сфера дії

Регламент застосовується до обробки персональних даних: в контексті діяльності установи контролера або оператора в Союзі, незалежно від того, чи відбувається обробка в Союзі чи ні.

a. суб'єктів даних, що знаходяться в Союзі, контролером або оператором, що не є заснованим в Союзі, коли дії по обробці пов'язані з:
b. постачанням товарів чи наданням послуг таким суб'єктам даних у Союзі, незалежно від того, чи вимагають оплату від таких суб'єктів даних; або
c. контроль за їх поведінкою в тій мірі, в якій це відбувається в Союзі.
d. контролером, що не є заснованим в Союзі, але знаходиться в місці, де законодавство держав-членів застосовується на підставі публічного міжнародного права.

Критерії визначення територіальної сфери дії GDPR

1. Критерій місцезнаходження.

2. Критерій цільового спрямування діяльності.

Керівництво 3/2018 щодо територіального обсягу GDPR.

Критерій місцезнаходження

Установа контролера або оператора не знаходиться на території ЄС, а обробка персональних даних пов'язана з:

- постачанням товарів чи наданням послуг суб'єктам персональних даних у Європейському Союзі, незалежно від того, чи вимагається оплата від таких суб'єктів персональних даних; або
- моніторингом поведінки суб'єктів персональних даних, якщо така поведінка має місце у межах

Критерій цільового спрямування діяльності

- Чи персональні дані, які обробляються, дійсно належать суб'єктам персональних даних, що знаходяться на території ЄС?

- Чи оброблення персональних даних безпосередньо пов'язано з постачанням товарів та послуг або з моніторингом поведінки суб'єктів персональних даних на території ЄС?

Види діяльності, які можуть містити в собі моніторинг поведінки суб'єкта

1) Здійснення рекламної діяльності;

2) Діяльність, пов'язана з визначенням геолокації;

3) Діяльність пов'язану з онлайн відстежуванням через використання cookies;

4) Послуги з аналітики стану здоров'я або послуги щодо надаються онлайн;
   a. Діяльність, пов'язану зі здійсненням відеоспостереження;
   b. Діяльність, пов'язану з маркетинговими опитуваннями та інше.

Основні поняття та принципи GDPR

персональні дані це будь-яка інформація, що стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати («суб'єкт даних»);

фізична особа, яку можна ідентифікувати, є такою особою, яку можна ідентифікувати, прямо чи опосередковано, зокрема, за такими ідентифікаторами як:
1. ім'я
2. ідентифікаційний номер
3. дані про місцеперебування
4. онлайн-ідентифікатор або
5. за одним чи декількома факторами, що є визначальними для:
   - фізичної,
   - фізіологічної,
   - генетичної,
   - розумової,
   - економічної,
   - культурної чи
   - соціальної

   сутності такої фізичної особи.

До персональних даних належать:
- ПІБ;
- номер телефону;
- адреса електронної пошти та проживання;
- номер банківського рахунку, банківської картки і строк її дії;
- відомості про національність;
- політичні або релігійні погляди;
- дані про групу крові;
- фото;
- біометричні та паспортні дані;
- ідентифікаційний код;
- підпис;
- інформація про рівень особистих доходів;
- поточне місце перебування;
- IP-адреса та ін.

«Обробка (опрацювання)» означає будь-яку дію або низку дій з персональними даними або наборами персональних даних з використанням автоматизованих засобів або без них, таких як:
- збирання, реєстрація,
- організація, структурування,
- зберігання, адаптація чи зміна,
- пошук, ознайомлення,
- використання, розкриття через передавання,
- розповсюдження чи надання іншим чином,
- упорядкування чи комбінування,
- обмеження, стирання чи знищення.

«Згода» суб'єкта даних означає будь-яке:
- вільно надане,
- конкретне,
- поінформоване та
- однозначно зазначене

бажання суб'єкта даних, яким він або вона, шляхом оформлення заяви чи проявом чітких ствердних дій підтверджує згоду на опрацювання своїх персональних даних.

«Профайлінг» означає будь-яку форму автоматизованої обробки персональних даних, що складається із використання персональних даних для оцінювання окремих персональних аспектів, що стосуються фізичної особи, зокрема, для аналізу або прогнозування аспектів, що мають відношення до:
- продуктивності суб'єкта даних на роботі,
- економічної ситуації,
- здоров'я,
- особистих переваг,
- інтересів,
- надійності,
- поведінки,
- місцезнаходження або пересування;

«Контролер» означає фізичну чи юридичну особу, орган публічної влади, агентство чи інший орган, який самостійно чи спільно з іншими визначає цілі та засоби обробки персональних даних;

якщо цілі та засоби такої обробки визначаються законодавством Союзу чи держави-члена, контролер або спеціальні критерії його призначення може бути передбачено законодавством Союзу чи держави-члена;

«Оператор» (процесор) означає фізичну чи юридичну особу, орган публічної влади, агентство чи інший орган, який обробляє персональні дані від імені контролера;

«Третя сторона» означає фізичну чи юридичну особу, орган публічної влади, агентство чи орган, який не є суб'єктом даних, контролером, оператором та особами, які під безпосереднім керівництвом контролера або оператора, уповноважені обробляти персональні дані;

«Одержувач» означає фізичну чи юридичну особу, орган публічної влади, агентство чи інший орган, якому розкривають персональні дані, незалежно від того, чи є вони третьою стороною.

Проте органи публічної влади, що можуть отримувати персональні дані в рамках конкретного запиту згідно з законодавством Союзу чи держави-члена, не вважаються одержувачами.

Обробка даних такими органами публічної влади має відповідати нормам про захист даних відповідно до цілей обробки;

«Порушення персональних даних» – означає порушення безпеки, що призводить до випадкового або незаконного знищення, втрати, зміни, несанкціонованого розголошення або доступу до персональних даних, що передаються, зберігаються або обробляються іншим чином;

Приклади перекладу

«Головна установа» для контролера, який має установи в декількох державах-членах, означає – його центральну адміністрацію в Союзі, якщо рішення про цілі та засоби обробки персональних даних не приймаються в іншій установі контролера в Союзі та яка має повноваження виконувати такі рішення, і в цьому випадку організація, яка приймала такі рішення, повинна вважатися головною установою;

«Головний осідок» означає:
щодо контролера, що має осідки в декількох державах-членах, – осідок його центральної адміністрації в Союзі, за винятком випадків, коли рішення про цілі та засоби опрацювання персональних даних ухвалено в іншому осідку контролера в Союзі, і якщо такий інший осідок має повноваження забезпечувати виконання таких рішень; у такому разі, осідок, де було ухвалено такі рішення, необхідно вважати головним;

«Головна установа» для оператора, що має установи в декількох державах-членах, означає його центральну адміністрацію в Союзі або, якщо оператор не має центральної адміністрації в Союзі, це установа оператора в Союзі, де відбувається основна діяльність з обробки в тій мірі, в якій на оператора покладаються особливі зобов'язання відповідно до цього Регламенту;

«Наглядовий орган» це один або декілька незалежних публічних органів на які держава-член покладає відповідальність за моніторинг застосування Регламенту, для того, щоб захистити фундаментальні права та свободи фізичних осіб у сфері опрацювання та сприяти вільному руху персональних даних у межах Союзу;

«Відповідний наглядовий орган» означає наглядовий орган, якого стосується опрацювання персональних даних, оскільки:

a. контролер або оператор має установу на території держави-члена такого наглядового органу;
b. суб'єкти даних, що перебувають на території держави-члена такого наглядового органу, зазнають істотного впливу чи ймовірно будуть зазнавати істотного впливу в результаті опрацювання;
c. до такого наглядового органу було подано скаргу.

«Транскордонне опрацювання» означає опрацювання персональних даних:

- що відбувається у контексті діяльності установ контролера чи оператора в Союзі у більше ніж одній державі-члені, якщо контролер або оператор мають установи в більше ніж одній державі-члені; або
- що відбувається контексті діяльності однієї установи контролера або оператора в Союзі, але яке істотно впливає чи ймовірно істотно впливатиме на суб'єктів даних у декількох державах-членах.

Принципи опрацювання персональних даних

Персональні дані необхідно:

1) опрацьовувати у законний, правомірний і прозорий спосіб щодо суб'єкта даних («законність, правомірність і прозорість»);

2) збирати для визначених, чітких і законних цілей і в подальшому не опрацьовувати у спосіб, що є несумісним з такими цілями; подальше опрацювання для цілей архівації в інтересах суспільства, наукових чи історичних цілей дослідження або статистичних цілей, відповідно до статті 89 (1), не вважатиметься несумісним з початковими цілями («обмеження цілей»);

3) вважати достатніми і відповідними та обмежити їх мірою необхідності в них з огляду на цілі опрацювання («мінімізація даних»);

4) вважати точними і, за необхідності, оновлювати; необхідно вживати усіх відповідних заходів для того, щоб забезпечити, що неточні персональні дані, зважаючи на цілі їхнього опрацювання, було стерто чи виправлено без затримки («точність»);

5) зберігати в формі, що дозволяє ідентифікацію суб'єктів даних не довше, ніж це є необхідним для цілей їхнього опрацювання;

6) персональні дані можна зберігати протягом більш тривалих періодів, доки їх опрацьовують винятково для досягнення цілей суспільних інтересів, цілей наукового чи історичного дослідження або статистичних цілей відповідно до статті 89(1) за умов вжиття відповідних технічних і організаційних заходів, передбачених цим Регламентом для гарантування прав і свобод суб'єкта даних («обмеження зберігання»);

7) опрацьовувати в спосіб, що забезпечує належну безпеку персональних даних, у тому числі, захист проти несанкціонованого чи незаконного опрацювання та проти ненавмисної втрати, знищення чи завдання шкоди, із застосуванням відповідних технічних і організаційних інструментів («цілісність і конфіденційність»).

Принцип законного опрацювання даних

Опрацювання є законним, лише якщо і в тій мірі, в якій має місце хоча б одне з наступного:

1) суб'єкт даних надав згоду на опрацювання своїх персональних даних для однієї чи декількох спеціальних цілей;

2) опрацювання є необхідним для виконання контракту, стороною якого є суб'єкт даних, або для вжиття дій на запит суб'єкта даних до укладення договору;

3) опрацювання є необхідним для дотримання встановленого законом зобов'язання, яке поширюється на контролера;

4) опрацювання є необхідним для того, щоб захистити життєво важливі інтереси суб'єкта даних або іншої фізичної особи;

5) опрацювання є необхідним для виконання завдання в суспільних інтересах або здійснення офіційних повноважень, покладених на контролера;

6) опрацювання є необхідним для цілей законних інтересів контролера або третьої сторони, окрім випадків, коли над такими інтересами переважають інтереси фундаментальних прав і свобод суб'єкта даних, що вимагають охорони персональних даних, особливо, якщо суб'єктом даних є дитина.

Це пункт не застосовують до опрацювання, яке здійснюють публічні органи у ході виконання своїх завдань.

Держави-члени можуть мати або вводити уточнені положення для застосування норм цього Регламенту, визначивши більш чітко спеціальні вимоги опрацювання та інші засоби для забезпечення законного та правомірного опрацювання, в тому числі, для інших спеціальних ситуацій опрацювання, як це передбачено главою IX.

Законодавчу базу визначає:

1. законодавство Союзу;
   або
2. законодавство держави-члена, яке поширюється на контролера. Мету опрацювання необхідно означити в такій законодавчій базі або, в частині опрацювання, вказаного в пункті (e) параграфа 1, її необхідно обов'язково передбачити для виконання завдання в суспільних інтересах чи здійснення офіційних повноважень, покладених на контролера.

Така законодавча база може містити спеціальні положення для адаптації застосування правил цього Регламенту, між іншим:

- загальні умови, що регулюють питання законності опрацювання контролером;
- типи даних, що підлягають опрацюванню;
- відповідні суб'єкти даних;
- установи, яким можна розкривати персональні дані та цілі такого розкриття;
- цільове обмеження;
- періоди зберігання;
- операції опрацювання і процедури опрацювання, в тому числі, заходи щодо забезпечення законного та справедливого опрацювання як ті, що вживають в інших спеціальних ситуаціях опрацювання, як передбачено в главі IX.

Законодавство Союзу або держави-члена повинно відповідати меті суспільного інтересу та бути пропорційним наявній законній цілі.

Якщо опрацювання для іншої цілі, ніж тієї для якої відбувалося збирання персональних даних, не засновано на згоді суб'єкта даних або на законодавстві Союзу чи держави-члена, що є необхідним і пропорційним заходом у демократичному суспільстві для гарантування цілей, вказаних у статті 23(1), контролер, для того, щоб переконатися, чи є опрацювання для іншої цілі сумісним із ціллю первинного збирання персональних даних, повинен врахувати, між іншим:

- будь-який зв'язок між цілями, для яких збирають персональні дані, і цілями запланованого подальшого опрацювання;
- контекст збирання персональних даних, зокрема, щодо взаємозв'язку між суб'єктами даних і контролера;
- специфіку персональних даних, зокрема, питання опрацювання спеціальних категорій персональних даних, згідно зі статтею 9,

або опрацювання персональних даних про судимості і кримінальні злочини, згідно зі статтею 10;
- можливі наслідки запланованого подальшого опрацювання для суб'єктів даних;
- наявність належних гарантій, що можуть передбачати шифрування чи використання псевдонімів.

Умови для згоди

1. Якщо обробка базується на згоді, контролер повинен бути в змозі продемонструвати, що суб'єкт даних погодився на обробку своїх персональних даних.

2. Якщо згода суб'єкта даних дається в контексті письмової декларації, яка стосується також інших питань, запит про згоду подається у спосіб, який чітко відрізняється від інших питань, у зрозумілій та легкодоступній формі, використовуючи чітка і проста мова. Будь-яка частина такої заяви, яка є порушенням цього Положення, не є обов'язковою.

4. Суб'єкт даних має право відкликати свою згоду в будь-який час. Відкликання згоди не впливає на законність обробки на основі згоди до її відкликання. Перш ніж дати згоду, про це повідомляється суб'єкт даних. Вийти з нього так само просто, як і дати згоду.

6. Здійснюючи оцінку того, чи є згода вільно наданою, необхідно максимально враховувати те, чи залежить, між іншим, виконання договору, в тому числі надання послуги, від згоди на опрацювання персональних даних, що не є необхідною для виконання такого договору. (cookies файли)

Окреме правове регулювання:

Умови, що застосовуються до згоди дитини в сфері послуг інформаційного суспільства
- Опрацювання спеціальних категорій персональних даних
- Опрацювання персональних даних про судимості і кримінальні злочини
- Опрацювання, що не вимагає ідентифікації

Контролер:
- вживає відповідних заходів для надання будь-якої інформації та будь-якого повідомлення, що стосується обробки суб'єкта даних у стислій, прозорій, зрозумілій та легкодоступній формі, використовуючи чітку інформацію простою мовою, зокрема для будь-якої інформації, адресованої спеціально дитині;
- сприяє здійсненню прав суб'єктів даних;
- надає інформацію про дії, вжиті за запитом суб'єкту даних без надмірної затримки та в будь-якому випадку протягом місяця з моменту отримання запиту.

Інформація надається у письмовій формі або іншими способами, включаючи, де це доцільно, електронними засобами.

На запит суб'єкта даних інформація може бути надана усно за умови, що особа суб'єкта даних доведена іншими способами.

Інформація, яка надається, коли особисті дані збираються від суб'єкта даних

Контролер на момент отримання персональних даних надає суб'єкту даних всю наступну інформацію:

ідентифікатор та контактні дані контролера та, де це можливо, представника контролера;

контактні дані посадової особи із захисту даних, де це можливо;

цілі обробки, для яких призначені персональні дані, а також правова основа для обробки;

законні інтереси, які переслідує контролер або третя сторона; одержувачі або категорії одержувачів персональних даних, якщо такі є;

той факт, що контролер має намір передавати персональні дані третій країні чи міжнародній організації.

Інформація, яка надається, якщо особисті дані не були отримані від суб'єкта даних

Контролер надає суб'єкту даних таку інформацію:

- ідентифікатор та контактні дані контролера та, де це можливо, представника контролера;
- контактні дані посадової особи із захисту даних, де це можливо;
- цілі обробки, для яких призначені персональні дані, а також правова основа для обробки;
- категорії відповідних персональних даних;
- одержувачі або категорії одержувачів персональних даних, якщо такі є;
- той факт, що контролер має намір передавати персональні дані третій країні чи міжнародній організації.
- період, протягом якого особисті дані будуть зберігатися, або критерії, які використовуються для визначення цього періоду;
- законні інтереси, які переслідує контролер або третя сторона;
- наявність права вимагати від контролера доступу до та виправлення або видалення персональних даних або обмеження на обробку щодо суб'єкта даних та заперечення проти обробки, а також права на переносимість даних;
- з якого джерела беруться персональні дані та, якщо вони застосовуються, чи надходили вони з загальнодоступних джерел;
- наявність автоматизованого прийняття рішень, включаючи профілювання.

Права суб'єкта персональних даних

1. Право доступу
2. Виправлення та видалення (знищення) (стирання)
3. Право на видалення («право бути забутим»)
4. Право на обмеження обробки
5. Право на заперечення та автоматизоване індивідуальне прийняття рішень

Право доступу суб'єкта даних

Суб'єкт даних має право отримати доступ до персональних даних та наступної інформації:

1) цілі обробки та категорії відповідних персональних даних;
2) одержувачі або категорії одержувачів, зокрема одержувачі в третіх країнах або міжнародних організаціях;
3) де це можливо, передбачений період, протягом якого будуть зберігатися особисті дані;
4) наявність права вимагати від контролера виправлення чи стирання персональних даних або обмеження обробки персональних даних, що стосуються суб'єкта даних, або заперечення проти такої обробки;
5) право подати скаргу до контролюючого органу;
6) будь-яка наявна інформація щодо джерел персональних даних;
7) наявність автоматизованого прийняття рішень, включаючи профілювання і змістовну інформацію про логіку, що застосовується, а також про значення та передбачені наслідки такої обробки для суб'єкта даних.

Виправлення та видалення (знищення) (стирання)

Суб'єкт даних має право без зайвих затримок отримати виправлення контролером недостовірних персональних даних, що стосуються його або її.

Враховуючи цілі обробки, суб'єкт даних має право заповнити неповні персональні дані, в тому числі шляхом надання додаткової заяви.

Право на видалення («право бути забутим»)

Суб'єкт даних має право на видалення особистих даних, що стосуються його, а контролер зобов'язаний видаляти без зайвих затримок за однією з наступних підстав:

- персональні дані більше не потрібні стосовно цілей, для яких вони були зібрані чи іншим чином оброблені;
- суб'єкт даних відкликає згоду, на якій базується обробка і якщо немає іншої правової підстави для обробки;
- суб'єкт даних заперечує проти обробки відповідно до норм Регламенту;
- персональні дані були незаконно оброблені;

- особисті дані повинні бути видалені для відповідності юридичним зобов'язанням законодавства Союзу чи держав-членів, яким підпорядковується контролер;
- персональні дані були зібрані стосовно дитини с порушенням вимог Регламенту.

Контролер, який оприлюднив і зобов'язаний видалити персональні дані, вживає розумних заходів, включаючи технічні, для інформування контролерів, які обробляють персональні дані, про те, що суб'єкт даних вимагає видалення такими контролерами будь-яких посилань на такі персональні дані, їхні копії чи реплікації.

Видалення персональних даних не застосовуються в тій мірі, в якій необхідна обробка:
- для реалізації права на свободу вираження поглядів та інформації;
- для дотримання юридичного зобов'язання, яке вимагає обробки відповідно до законодавства Союзу чи держав-членів, якому підпорядковується контролер,
- для виконання завдання, що виконується в інтересах суспільства, або у здійсненні службових повноважень, наданих контролеру;
- з міркувань суспільного інтересів у сфері охорони здоров'я;
- з метою архівації в суспільних інтересах, в цілях статистичних, наукових чи історичних досліджень;
- для подання, здійснення чи захисту судових позовів.

Право на обмеження обробки

Суб'єкт даних має право отримати від контролера обмеження обробки з наступних причин:
- точність персональних даних може оспорюватись суб'єктом даних, протягом періоду, що дозволяє контролеру перевірити точність персональних даних;
- обробка є незаконною, і суб'єкт даних виступає проти видалення персональних даних та вимагає замість них обмеження їх використання;
- контролер більше не потребує персональних даних для цілей обробки, але вони вимагаються суб'єктом даних для встановлення, здійснення чи захисту юридичних вимог;
- суб'єкт даних заперечує проти обробки в очікуванні перевірки щодо того чи переважають законні підстави контролера законні підстави суб'єкта даних.

Якщо обробка обмежена відповідно до вимог Регламенту, такі персональні дані, за винятком зберігання, обробляються лише:
- за згодою суб'єкта даних або
- для подання, здійснення чи захисту судового позову або
- для захисту прав іншої фізичної чи юридичної особи або з важливих суспільних інтересів Союзу чи держави-члена.

Суб'єкт даних, який отримав обмеження на обробку, має бути повідомлений контролером до зняття обмеження на обробку.

Право на заперечення та автоматизоване індивідуальне прийняття рішень

Суб'єкт даних має право, в будь-який час заперечувати на підставах, що стосуються його конкретної ситуації обробку персональних даних, які стосуються його чи її, включаючи профілювання.

Контролер може продовжувати обробляти персональні дані лише за наявності вагомих законних підстав, які перекривають інтереси, права та свободи суб'єкта даних або для встановлення, здійснення чи захисту судових позовів.

У випадку опрацювання персональних даних для цілей прямого маркетингу, суб'єкт даних повинен мати право заборонити таке опрацювання персональних даних, у тому числі, профайлінгу, тією мірою, якою це стосуються такого прямого маркетингу.

Якщо суб'єкт даних заперечує проти обробки для цілей прямого маркетингу, особисті дані більше не обробляються для таких цілей.

Автоматизоване індивідуальне прийняття рішень, включаючи профілювання.
Суб'єкт даних має право не підлягати прийняттю рішення, яке ґрунтується виключно на автоматизованій обробці, включаючи профілювання, якщо воно спричиняє юридичні наслідки щодо нього чи її аналогічного впливу чи настільки ж істотно впливає на нього.

Виключення, якщо рішення:
b. необхідно для укладення або виконання договору між суб'єктом даних та контролером даних;
c. уповноважений законодавством Союзу чи держав-членів, яким підпорядковується контролер встановлює відповідні заходи щодо захисту прав та свобод суб'єкта даних та законних інтересів; або
d. ґрунтується на явній згоді суб'єкта даних.

Для пунктів (a) та (c) пункту 2, контролер даних вживає відповідних заходів для захисту прав і свобод суб'єкта даних та законних інтересів, забезпечує право на отримання людського втручання з боку контролера, висловити свою точку зору та оскаржити рішення.

Законом може бути обмежено обсяг зобов'язань та прав коли воно є необхідним в інтересах:
1) національної безпеки; оборони; громадської безпеки;
2) запобігання, розслідування, виявлення або переслідування за скоєння кримінальних злочинів або для виконання кримінальних покарань, у тому числі, захисту від або запобіганню загрозам громадській безпеці;
3) інших важливих цілей загального суспільного інтересу, зокрема економічного чи фінансового, в тому числі, питань валютної, бюджетної і податкової політики, охорони суспільного здоров'я та соціального забезпечення;
4) незалежності судових органів і судових процесів;
5) запобігання, розслідування, виявлення або переслідування за порушення етичних норм для регульованих професій;
6) моніторингу, перевірки чи регуляторної функції, пов'язаної, навіть періодично, з реалізацією офіційних повноважень у випадках, вказаних у пунктах;
   - захисту суб'єкта даних або прав і свобод інших осіб;
   - виконання цивільно-правових позовів.

При цьому будь-який законодавчий механізм повинен містити спеціальні положення, за необхідності, принаймні щодо:
a. цілей опрацювання чи категорій опрацювання;
b. категорій персональних даних;
c. обсяг введених обмежень;
d. гарантій запобігання зловживанню чи незаконному доступу або передаванню;
e. детальної інформації щодо контролера або категорій контролерів;
f. періодів зберігання та застосовних гарантій, з огляду на специфіку, обсяг та цілі
g. опрацювання чи категорій опрацювання;
h. ризиків для прав і свобод суб'єктів даних; або
i. право суб'єктів даних бути повідомленими про обмеження, якщо це не може завдати шкоди цілі обмеження.

Повноваження контролера та оператора.

Відповідальність контролера

1. Зважаючи на специфіку, обсяг, контекст і цілі опрацювання, а також ризики різної ймовірності та труднощі для прав і свобод фізичних осіб, контролер повинен вжити необхідних технічних і організаційних заходів для того, щоб гарантувати та бути здатним довести, що опрацювання здійснюють згідно з цим Регламентом. За необхідності, такі заходи необхідно переглядати та оновлювати.

2. У разі їхньої пропорційності щодо опрацювання даних заходи повинні передбачати реалізацію відповідних політик щодо захисту даних контролером.

3. Дотримання затверджених кодексів поведінки чи затверджених механізмів сертифікації можна використовувати як елемент підтвердження відповідності обов'язкам контролера.

Захист даних за проектом (планом) та за замовчуванням

Контролер повинен, звертаючи увагу на сучасний стан можливостей та обмежень як під час визначення засобів для обробки, так і під час самої обробки, застосовувати відповідні технічні та організаційні заходи, такі як:
- псевдонімізація,
- мінімізація даних,
- застосування всіх необхідних заходів та засобів при обробці з метою задоволення вимог цього Регламенту та захисту прав суб'єктів даних.

За замовчуванням обробляються лише ті особисті дані, їх кількість, ступінь обробки, період зберігання та їх доступність, що необхідні для кожної конкретної мети обробки, а також що за замовчуванням особисті дані не будуть доступні без втручання особи невизначеному числу фізичних осіб.

Затверджений механізм сертифікації може використовуватися як елемент доказування відповідності вимогам.

Спільні контролери

Якщо два чи декілька контролерів спільно визначають цілі та засоби опрацювання, вони є спільними контролерами, які на умовах прозорості домовляються встановити свої відповідні обов'язки, що відображають зміст зобов'язань за цим Регламентом.

За домовленістю можна призначити координаційний центр для суб'єктів даних.

Домовленість повинна належним чином відображати відповідні ролі та відносини спільних контролерів щодо суб'єктів даних. Сутність домовленості необхідно повідомити суб'єкту даних.

Незалежно від умов домовленості суб'єкт даних може скористатися своїми правами за цим Регламентом щодо та проти кожного з контролерів.

Представники контролерів або операторів, які не створені в Союзі

У разі наявності екстериторіальності контролер або оператор повинен призначити в письмовій формі представника в Союзі.

Представник в ЄС

Цей обов'язок не застосовують до:

1) опрацювання, яке призначено для окремого випадку, воно не передбачає, у великих обсягах, опрацювання спеціальних категорій даних, або

2) опрацювання даних про судимості і кримінальні злочини, та ймовірно не призведе до виникнення ризику для прав і свобод фізичних осіб, з огляду на специфіку, контекст, масштаб і цілі опрацювання; або

3) органу чи установи публічної влади.

Представник має бути визначений в одній з держав-членів, де перебувають суб'єкти даних, чиї персональні дані опрацьовують:
1) у зв'язку з пропонуванням їм товарів чи послуг, або
2) чию поведінку відстежують.

Представник отримує мандат від контролера або оператора, за яким до нього можуть звертатися окрім або замість контролера або оператора, зокрема, наглядові органи і суб'єкти даних, з усіх питань, пов'язаних з опрацюванням, з метою забезпечення відповідності цьому Регламенту.

Призначення представника контролером чи оператором не зачіпає юридичних дій, які можуть бути порушені проти контролера чи самого оператора.

Якщо обробка повинна здійснюватися від імені контролера, контролер повинен використовувати лише операторів, що надають достатні гарантії для здійснення відповідних технічних та організаційних заходів таким чином, щоб обробка відповідала вимогам цього Регламенту та забезпечувала захист права суб'єкта даних.

Оператор не повинен залучати іншого оператора без попереднього конкретного або загального письмового дозволу контролера.

У разі загального письмового дозволу оператор повідомляє контролера про будь-які намічені зміни, що стосуються додавання або заміни інших операторів, тим самим надаючи можливість контролеру заперечувати проти таких змін.

Обробка оператором регулюється договором або іншим правовим актом відповідно до законодавства Союзу чи держави-члена, який є обов'язковим стосовно контролера та визначає:
a. предмет та тривалість обробки,
b. характер та мета обробки,
c. тип персональних даних та

d. категорії суб'єктів даних та
e. зобов'язання та права контролера.

Цей договір чи інший правовий акт, зокрема, передбачає, що оператор:
1) обробляє персональні дані лише за документально підтвердженими інструкціями контролера;
2) забезпечує, щоб особи, уповноважені обробляти персональні дані, взяли на себе зобов'язання щодо;
3) вживає всіх заходів, необхідних відповідно до законодавства;
4) беручи до уваги характер обробки, допомагає контролеру відповідними технічними та організаційними заходами, наскільки це можливо, для виконання зобов'язання контролера відповідати на запити щодо здійснення прав суб'єкта даних;
5) допомагає контролеру у забезпеченні дотримання зобов'язань з урахуванням характеру обробки та інформації, доступної процесору;
6) за вибором контролера видаляє або повертає всі персональні дані контролеру після закінчення надання послуг, пов'язаних з обробкою, та видаляє наявні копії, якщо законодавство Союзу чи держав-членів не вимагає зберігання персональних даних;
7) надає контролеру всю інформацію, необхідну для доказування виконання зобов'язань та допускає та сприяє проведенню аудитів, включаючи перевірки, що проводяться контролером або іншим аудитором, дорученим контролером.
8) Оператор негайно інформує контролера, якщо, на його думку, його вказівка порушує цей Регламент або інші положення законодавства Союзу або держави-члена щодо захисту даних.

Data Processing Agreement

Українська компанія співпрацює з європейською компанією, яка є контролером. Співпраця, зокрема, стосується і обробки персональних даних.

Контролер (європейська компанія), має обов'язок укласти письмову угоду з українським контрагентом щодо обробки ПД.

Письмова угода може бути як:
a. додаткові умови про особливості обробки ПД (невід'ємний додаток до основної угоди);
b. окрема Угода щодо обробки ПД (Data Processing Agreement).

Data Processing Agreement **має включати такі зобов'язання:**
- обробка персональних даних повинна здійснюватися виключно на підставі письмових вказівок контролера;
- гарантії приватності;
- гарантії вжиття належних заходів безпеки;
- право залучати субпідрядників (субператорів) тільки на підставі попередньої письмової згоди контролера;
- обов'язок видалити або повернути персональні дані після закінчення терміну надання послуг;
- обов'язок надання контролеру допомоги та інформації для забезпечення відповідності вимогам GDPR.

Безпека персональних даних

Контролер та оператор повинні впроваджувати відповідні технічні та організаційні заходи для забезпечення рівня безпеки, відповідного ризику, включаючи, зокрема, у відповідних випадках:
- псевдонімізація та шифрування персональних даних;
- можливість забезпечити постійну конфіденційність, цілісність, доступність та стійкість процесорних систем та послуг;
- можливість своєчасно відновити доступність та доступ до персональних даних у разі фізичного чи технічного інциденту;
- процес регулярного тестування, оцінки та оцінки ефективності технічних та організаційних заходів щодо забезпечення безпеки обробки.

Офіцер із захисту даних

Контролер та оператор призначають службовця із захисту даних, коли:
1) опрацювання здійснюється органом державної влади або установою, за винятком судів, що діють як судові інстанції;
2) основна діяльність контролера або оператора складається з операцій з обробки, які в силу своєї природи, обсягу та / або їх цілей потребують регулярного та систематичного моніторингу суб'єктів даних у великих масштабах; або
3) основна діяльність контролера чи оператора полягає у обробці у великому масштабі спеціальних категорій даних або стосуються кримінальних судимостей та правопорушень.

Група підприємств може призначити одного службовця із захисту даних, за умови, його легкої доступності для кожного закладу.

Якщо контролер або оператор є публічним органом чи установою, може бути призначений єдиний службовець захисту даних для декількох таких органів, враховуючи їх організаційну структуру та розмір.

Посадова особа із захисту даних призначається на основі професійних якостей та, зокрема, експертних знань закону та практики захисту даних та здатності виконувати завдання.

Службовець захисту даних може бути співробітником контролера чи оператора або виконувати завдання на підставі договору на надання послуг.

Контролер або оператор оприлюднює контактні дані посадової особи із захисту даних та повідомляє їх наглядовому органу.

Сертифікація

Заохочується запровадження механізмів сертифікації захисту даних та штампів і знаків захисту даних з метою підтвердження відповідності цьому законодавству операцій обробки, які здійснюють контролери і оператори.

Необхідно брати до уваги особливі потреби мікропідприємств, малих і середніх підприємств.

Механізми сертифікації можна запровадити з метою підтвердження наявності належних гарантій, які надають контролери або оператори, на яких не поширюється дія цього Регламенту в межах передавання персональних даних до третіх країн чи міжнародних організацій.

Такі контролери або оператори повинні взяти на себе зобов'язання, які є обов'язковими і можливими для виконання, за допомогою договірних або інших юридично зобов'язальних інструментів, для того, щоб застосувати зазначені належні гарантії, у тому числі, гарантії щодо прав суб'єктів даних.

1. Сертифікація є добровільною і доступною шляхом реалізації прозорого процесу.

2. Сертифікація відповідно до цієї статті не знижує ступінь відповідальності контролера або оператора щодо відповідності цьому Регламенту та не обмежує завдання і повноваження наглядових органів.

3. Контролер або оператор, який подає своє опрацювання до механізму сертифікації, надає органу сертифікації або, у разі необхідності, компетентному наглядовому органу, всю інформацію та доступ до опрацювання даних, що є необхідним для проведення процедури сертифікації.

4. Сертифікацію видають контролеру або оператору на строк до трьох років, її може бути поновлено на тих самих умовах, якщо і надалі буде виконано відповідні вимоги.

Передача персональних даних третім країнам або міжнародним організаціям

Загальний принцип передачі даних

Будь-яка передача персональних даних, які піддаються обробці або призначені для обробки після передачі до третьої країни або до міжнародної організації, має відбуватися лише в тому випадку, якщо контролер і оператор дотримуються умов Регламенту, в тому числі, для наступних актів передавання персональних даних з третьої країни чи міжнародної організації до іншої третьої країни чи міжнародної організації.

Передача на підставі рішення про відповідність

Передача персональних даних до третьої країни або міжнародної організації може відбуватися, коли Комісія вирішила, що третя країна, територія або один або декілька визначених секторів у цій третій країні або відповідної міжнародної організації забезпечує відповідний (адекватний) рівень захисту.

Така передача не потребує конкретного дозволу.

Оцінюючи відповідність рівня захисту **враховуються такі елементи:**
1) верховенство закону,
2) повага до прав людини та основних свобод,
3) відповідне законодавство (щодо громадської безпеки, оборони, національної безпеки та кримінального права та доступу державних органів до персональних даних, правила захисту даних, професійні правила та заходи безпеки)
4) правила щодо подальшої передачі персональних даних до іншої третьої країни чи міжнародної організації, які виконуються у цій країні чи міжнародній організації,
5) судова практика,
6) ефективні та правозастосовні дані права суб'єкта
7) ефективні адміністративні та судові компенсації для суб'єктів даних, особисті дані яких передаються;
8) існування та ефективне функціонування одного або декількох незалежних органів нагляду в третій країні або якій підпорядковується міжнародна організація, відповідальна за забезпечення та забезпечення дотримання правил захисту даних, включаючи належні правозастосовчі повноваження, для надання допомоги та консультування суб'єктів даних у здійсненні своїх прав та співпраці з наглядовими органами держав-членів; і
9) міжнародні зобов'язання, які третя країна чи міжнародна організація взяла на себе, або інші зобов'язання, що випливають із юридично обов'язкових конвенцій чи інструментів, а також від її участі у багатосторонніх або регіональних системах, зокрема стосовно захисту персональних даних.

Комісія, після проведення оцінювання відповідності рівня захисту, може вирішити, у формі впроваджувального акту, що третя країна, територія чи один або декілька визначених секторів у межах третьої країни, або міжнародна організація забезпечує належний рівень захисту даних у значенні параграфа 2 цієї статті.

Імплементаційний акт:
a. передбачає механізм періодичного перегляду, щонайменше кожні чотири роки;
b. уточнює територіальне та секторальне застосування та, за необхідності, визначає наглядовий орган або органи;
c. ухвалюють відповідно до експертної процедури, вказаної в Регламенті.

Передавання з урахуванням належних гарантій

За відсутності рішення Комісії про відповідність контролер або оператор можуть передавати персональні дані до третьої країни чи міжнародної організації за умови надання належних гарантій та наявності дієвих засобів правового захисту для суб'єктів даних.

Належні гарантії можна надавати без запиту на отримання від наглядового органу будь-якого спеціального дозволу:
d. юридично зобов'язальним інструментом, що підлягає застосуванню, між публічними органами чи організаціями;
e. зобов'язальними корпоративними правилами;
f. стандартними положеннями щодо захисту даних, ухваленими Комісією відповідно до експертної процедури;
g. затвердженим кодексом поведінки в поєднанні із зобов'язаннями контролера або оператора в третій країні, що підлягають обов'язковому виконанню, щодо вжиття належних гарантій, у тому числі, в частині прав суб'єктів даних; або
h. затвердженим механізмом сертифікації в поєднанні із зобов'язаннями контролера або оператора в третій країні, що підлягають обов'язковому виконанню,

Зобов'язальні корпоративні правила

Компетентний наглядовий орган затверджує зобов'язальні корпоративні правила відповідно до механізму послідовності за умови, що вони:
1. a) мають обов'язкову юридичну силу, застосовує і забезпечує їх виконання кожний зацікавлений член групи підприємств або групи підприємств, що здійснюють спільну господарську діяльність, в тому числі, їхні працівники;
1. b) прямо надають суб'єктам даних права, як можна реалізувати, у зв'язку з опрацюванням їхніх персональних даних; і
1. c) відповідають вимогам, встановленим у параграфі 2.

2. Зобов'язальні корпоративні правила, вказані в параграфі 1, повинні чітко визначати принаймні:
   a) структуру та контактні дані групи підприємств або групи підприємств, що здійснюють спільну господарську діяльність, та кожного з їхніх членів;

b) передавання даних чи низку актів передавання, у тому числі категорії персональних даних, тип опрацювання і його цілі, тип суб'єктів даних, що зазнали впливу, та визначення відповідної третьої країни чи країн;
c) механізми для звітування до компетентного наглядового органу про будь-які законні вимоги, які поширюються на члена групи підприємств або групи підприємств, що здійснюють спільну господарську діяльність в третій країні, що ймовірно матимуть суттєві негативні наслідки для гарантій, передбачених зобов'язальними корпоративними правилами; та
d) відповідне навчання з питань захисту даних для персоналу, що має постійний або регулярний доступ до персональних даних.

3. Комісія має право визначити формат і процедури для обміну інформацією між контролерами, операторами і наглядовими органами для виконання зобов'язальних корпоративних правил у значенні цієї статті.

Такі імплементаційні акти ухвалюють відповідно до експертної процедури встановленої у Регламенті.

Передача або розкриття, які прямо не дозволені законодавством Союзу

Будь-яке рішення суду або трибуналу та будь-яке рішення адміністративного органу в третій країні, що вимагає від контролера або оператора передати чи розкрити персональні дані, може бути визнане чи виконане у будь-який спосіб, якщо воно базується на міжнародній угоді, такій як договір про взаємну правову допомогу, яка є чинною для третьої країни, що подає запит, і Союзом або державою-членом, без обмеження інших підстав для передавання відповідно до цієї глави.

Відступи від конкретних ситуацій.

У разі відсутності рішення про відповідність або відповідних гарантій, включаючи обов'язкові корпоративні правила, передачу або набір передачі персональних даних третій країні або міжнародній організації мають місце лише за однієї з таких умов:

1) суб'єкт даних явно погодився на запропоновану передачу, після того як був поінформований про можливі ризики таких передач для суб'єкта даних через відсутність рішення про адекватність та відповідних гарантій;

2) передача необхідна для виконання договору між суб'єктом даних та контролером або здійснення переддоговірних заходів, вжитих на вимогу суб'єкта даних;

3) передача необхідна для укладення або виконання договору, укладеного в інтересах суб'єкта даних між контролером та іншою фізичною або юридичною особою;

4) передача необхідна з важливих причин, що становлять суспільний інтерес;

5) передача необхідна для формування, здійснення або захисту судових позовів;

6) передача необхідна для захисту життєвих інтересів суб'єкта даних або інших осіб, якщо суб'єкт даних фізично чи юридично не може дати згоду;

7) передача проводиться з реєстру, який відповідно до законодавства Союзу чи держав-членів призначений для надання інформації для громадськості та який відкритий для консультацій ні громадськістю, ні будь-якою особою, яка може виявити законний інтерес, але лише для в тій мірі, коли умови, визначені законодавством Союзу чи країн-членів для консультацій, виконані в конкретному випадку.

Положення, що стосуються конкретних ситуацій обробки

- Обробка та свобода вираження поглядів та інформації
- Опрацювання та публічний доступ до офіційних документів
- Обробка національного ідентифікаційного номера
- Обробка в контексті зайнятості

Обробка та свобода вираження поглядів та інформації

За законом узгоджується право на захист персональних даних з правом на свободу вираження поглядів та інформації, включаючи обробку для журналістських цілей та цілей академічної, художньої чи літературної виразності.

Для журналістських цілей або з метою академічного художнього чи літературного вираження передбачаються винятки або відхилення від вимог Регламентам, якщо вони необхідні для узгодження права на захист персональних даних зі свободою вираження поглядів та інформації.

Кожна держава-член повідомляє Комісію про положення свого закону і негайно про будь-які наступні закони про внесення змін або поправки, що стосуються їх.

Опрацювання та публічний доступ до офіційних документів

Особисті дані в офіційних документах, що зберігаються державним органом чи державною або приватною установою для виконання завдання в інтересах суспільства, можуть бути розкриті органом чи установою відповідно до законодавства Союзу чи держав-членів, щодо якого орган підпорядковується для того, щоб узгодити доступ громадськості до офіційних документів з правом захисту персональних даних відповідно до цього Регламенту.

Обробка національного ідентифікаційного номера

Держави-члени можуть додатково визначити конкретні умови для обробки національного ідентифікаційного номера або будь-якого іншого ідентифікатора загального застосування.

У такому випадку національний ідентифікаційний номер або будь-який інший ідентифікатор загального застосування застосовується лише під відповідними гарантіями прав та свобод суб'єкта даних відповідно до цього Регламенту.

Обробка в контексті зайнятості

Держави-члени можуть законодавством або колективними договорами передбачити більш конкретні правила для забезпечення захисту прав і свобод щодо обробки персональних даних працівників у контексті зайнятості.

Ці правила включають відповідні та конкретні заходи щодо захисту людської гідності суб'єкта даних, законних інтересів та основних прав.

Кожна держава-член повідомляє Комісію про ті положення свого закону, які вона приймає відповідно та негайно про будь-які наступні поправки, що стосуються їх.

Гарантії та відхилення, пов'язані з обробкою для архівації в інтересах суспільства, наукових чи історичних цілях дослідження або статистичних цілей

Обробка для архіваційних, наукових, історичних або статистичних цілей в інтересах суспільства підлягає захисту відповідно до Регламенту, прав та свобод суб'єкта даних.

Ці гарантії повинні забезпечувати проведення технічних та організаційних заходів, зокрема для забезпечення дотримання принципу мінімізації даних.

Ці заходи можуть включати псевдонімізацію за умови, що ці цілі можуть бути виконані таким чином.

Якщо ці цілі можуть бути виконані шляхом подальшої обробки, яка не дозволяє або більше не дозволяє ідентифікувати суб'єктів даних, ці цілі повинні бути виконані таким чином.

Якщо персональні дані обробляються для наукових або історичних цілей дослідження або статистичних цілей, законодавство Союзу чи держав-членів може передбачати відхилення від прав за умови дотримання умов та гарантій, зазначених вище у пункті 1, оскільки такі права, ймовірно, можуть зробити неможливими або серйозно зашкодити досягненню конкретних цілей, і такі відступи необхідні для виконання цих цілей.

Якщо особисті дані обробляються з метою архівації в інтересах суспільства, законодавство може передбачати відхилення від прав за умови дотримання умов та гарантій в пункті 1, оскільки такі права, ймовірно, можуть зробити неможливими або серйозно зашкодити досягненню конкретних цілей, і такі відступи необхідні для виконання цих цілей.

Обов'язки секретності

Держави-члени можуть прийняти конкретні правила для встановлення повноважень наглядових органів, контролерів чи процесорів, які підпадають під дію законодавства Союзу чи держав-членів. або правила, які встановлені національними компетентними органами, зобов'язання щодо професійної таємниці або інших рівнозначних зобов'язань щодо збереження таємниці, якщо це необхідно і пропорційно для узгодження права захисту персональних даних із обов'язком секретності.

Ці правила застосовуються лише стосовно персональних даних, які контролер або обробник отримав в результаті або отримав у ході діяльності, на яку поширюється цей обов'язок секретності.

Існуючі правила захисту церков та релігійних об'єднань

Якщо в державі-члені церкви та релігійні об'єднання чи громади застосовують, на момент набрання чинності цим Регламентом, комплексні правила, що стосуються захисту фізичних осіб щодо обробки, такі правила можуть продовжувати застосовуватися за умови, що вони приведені у відповідність до цього Регламенту.

Церкви та релігійні об'єднання, які застосовують комплексні правила відповідно до пункту 1 цієї статті, підлягають нагляду незалежного контролюючого органу, який може бути конкретним, за умови, що він відповідає умовам, встановленим Регламентом.

Незалежні органи нагляду

«наглядовий орган» це один або декілька незалежних публічних органів на які держава-член покладає відповідальність за моніторинг застосування Регламенту, для того, щоб захистити фундаментальні права та свободи фізичних осіб у сфері опрацювання та сприяти вільному руху персональних даних у межах Союзу;

«відповідний наглядовий орган» означає наглядовий орган, якого стосується опрацювання персональних даних, оскільки:

a. контролер або оператор має установу на території держави-члена такого наглядового органу;
b. суб'єкти даних, що перебувають на території держави-члена такого наглядового органу, зазнають істотного впливу чи ймовірно будуть зазнавати істотного впливу в результаті опрацювання;
c. до такого наглядового органу було подано скаргу;

Наглядовий орган

Кожна держава-член створює один чи більше незалежних публічних органів відповідальних за моніторинг застосування Регламенту (наглядовий орган).

Наглядові органи співпрацюють між собою та Комісією відповідно до Регламенту.

За наявності більше одного наглядового органу держава-член призначає наглядовий орган, який повинен представляти ці органи в Раді, та встановлює механізм забезпечення дотримання іншими органами правил, що стосуються механізм узгодженості.

Кожна держава-член приймає закон, відповідного до якого утворюються та функціонують наглядові органи.

Незалежність

Наглядовий орган діє абсолютно незалежністю відповідно до цього Регламенту.

Наглядовий орган:

1) має бути забезпечено людськими, технічними та фінансовими ресурсами, приміщеннями та інфраструктурою, необхідними для ефективного виконання своїх завдань та здійснення своїх повноважень;

2) обирає та має власний персонал, який підпорядковується виключному керівництву члена або членів відповідного наглядового органу;

3) має окремий публічний річний бюджет, який може бути частиною загального державного або національного бюджету;

4) підлягає фінансовому контролю, який не впливає на його незалежність.

Члени наглядового органу

1) мають бути позбавлені зовнішнього впливу, прямого чи опосередкованого, і не мають шукати чи приймати сторонніх інструкції;

2) мають утримуватися від будь-яких дій, несумісних із їхніми обов'язками, і не можуть займатися будь-якою несумісною роботою.

3) призначаються відповідно до прозорої процедури: парламентом, або урядом, або главою держави, або спеціальним незалежним органом;

4) повинні мати кваліфікацію, досвід та навички, зокрема в галузі захисту персональних даних, необхідних для виконання своїх обов'язків та здійснення своїх повноважень;

5) обов'язки закінчуються у разі закінчення строку повноважень, відставки або примусового звільнення відповідно до законодавства;

6) може бути звільнений лише у випадках серйозних проступків або якщо член більше не відповідає умовам, необхідним для виконання обов'язків.

Правила про створення контролюючого органу

Держава-член передбачає законодавчі вимоги для:

a. створення наглядового органу (НО);
b. правила та порядок, кваліфікаційні та інші умови призначення членів НО;
c. тривалість першого терміну дії членів НО, не менше чотирьох років, а також визначення кількості повторних термінів;
d. визначення обов'язків членів та співробітників НО, заборони на дії, професії та вигоди, несумісні з ними під час і після закінчення терміну повноважень, та правила припинення працевлаштування.

Члени та персонал НО відповідно до законодавства мають обов'язок дотримання професійної таємниці під час та після їх повноважень стосовно будь-якої конфіденційної інформації, яка стала їм відома у процесі виконання своїх завдань або здійснення своїх повноважень.

Під час їх повноважень цей обов'язок професійної таємниці, зокрема, поширюється на повідомлення фізичних осіб про порушення цього Регламенту.

Компетентність

Наглядовий орган має компетенцію щодо виконання завдань та здійснення повноважень, покладених на нього відповідно до цього Регламенту, на території своєї власної держави-члена.

Якщо обробку здійснюють органи публічної влади або приватні органи, наглядовий орган відповідної держави-члена є компетентним.

Наглядові органи не є компетентними здійснювати контроль за обробкою персональних даних судами, що діють у їх судовому порядку.

Компетенція керівного наглядового органу

Наглядовий орган за місцезнаходженням контролера або оператора має компетенцію діяти як керівний наглядовий орган для будь-якої обробки, зокрема, для транскордонної, що здійснює контролер або оператор відповідно до процедури,

Завдання

Наглядовий орган на своїй території виконує всі завдання встановлені Регламентом.

Повноваження

Наглядовий орган має всі дослідні, виправні повноваження та повноваження щодо надання дозволів та дорадчих питань, що дозволяє йому виконувати всі завдання відповідно до компетенції встановленої Регламентом.

Засоби захисту, відповідальність та штрафи.

Суб'єкт даних має право:
1. подати скаргу до контролюючого органу;
2. на ефективний судовий захист проти наглядового органу;
3. на ефективний судовий захист проти контролера чи оператора.

Представництво суб'єктів даних

Суб'єкт даних має право доручити:

- неприбутковому органу, організації чи об'єднанню, який був належним чином створений відповідно до законодавства держави-члена, має встановлені законом цілі, що є в інтересах суспільства, і є активним у сфері захисту прав і свобод суб'єктів даних щодо захисту їх персональних даних,

- подати скаргу від свого імені, користуватися правами зазначеними у статтях 77, 78 та 79, від свого імені та здійснювати право на отримання компенсації, зазначене у статті 82, від свого імені, якщо це передбачено законодавством держав-членів.

Право на компенсацію та відповідальність

Будь-яка особа, яка зазнала матеріальних чи нематеріальних збитків внаслідок порушення цього Регламенту, має право отримати від контролера чи оператора компенсацію за зазнану шкоду.

Будь-який контролер, який бере участь у обробці, несе відповідальність за шкоду, заподіяну обробкою, яка порушує цей Регламент.

Оператор несе відповідальність за шкоду, заподіяну обробкою лише тоді, коли він не дотримувався зобов'язань цього Регламенту, спеціально спрямованих на операторів, або якщо він діяв поза або суперечить законним вказівкам контролера.

Контролер або оператор звільняється від відповідальності, якщо доведе, що він жодним чином не несе відповідальності за подію, що спричинила шкоду.

Загальні умови накладення адміністративних штрафів

Кожен наглядовий орган забезпечує, щоб накладення адміністративних штрафів відповідно до цієї статті стосовно порушень цього Регламенту у кожному окремому випадку було ефективним, пропорційним та запобіжним.

Оперативні штрафи, залежно від обставин кожного окремого випадку, накладаються на додаток заходів або замість них. При вирішенні питання про накладення адміністративного штрафу та вирішенні розміру адміністративного штрафу в кожному окремому випадку належно враховується наступне:
a. характеру, тяжкості та тривалості порушення з урахуванням характеру сфери чи мети відповідної обробки, а також кількості постраждалих суб'єктів даних та рівня завданої ними шкоди;
b. навмисний чи недбалий характер порушення;
c. будь-які дії, вжиті контролером або процесором для зменшення шкоди, завданої суб'єктам даних;
d. ступінь відповідальності контролера чи обробника за врахування технічних та організаційних заходів, що здійснюються ними відповідно до статей 25 та 32;
e. будь-які попередні порушення контролером чи оператором;

f. ступінь співпраці з наглядовим органом з метою усунення порушення та пом'якшення можливих несприятливих наслідків порушення;
g. категорії персональних даних, постраждалих від порушення;
h. спосіб, яким про порушення стало відомо наглядовому органу, зокрема, чи, і якщо так, то в якій мірі, контролер чи оператор повідомили про порушення;
i. будь-який інший обтяжуючий чи пом'якшуючий фактор, застосовний до обставин справи, наприклад, отримані фінансові вигоди або збитки, уникнути, прямо чи опосередковано, від порушення.

Якщо контролер або оператор навмисно чи з необережності за ті ж або пов'язані з ними операції з обробки порушує кілька положень цього Положення, загальний розмір адміністративного штрафу не повинен перевищувати розмір, визначений за найважчі порушення.

За порушення наступних положень:
- зобов'язання контролера та обробника відповідно до статей 8, 11, 25 до 39 та 42 та 43;
- зобов'язання органу з сертифікації відповідно до статей 42 та 43;
- зобов'язання органу моніторингу відповідно до статті 41 (4).

відповідно до пункту 2 застосовуються адміністративні штрафи до 10000 000 євро, або у випадку зобов'язання – до 2% від загального світового річного обороту попереднього фінансового року залежно від того, яка сума є вищою.

За порушення наступних положень:
- основні принципи обробки, включаючи умови згоди відповідно до статей 5, 6, 7 та 9;
- права суб'єктів даних відповідно до статей 12–22;
- передача персональних даних одержувачу в третій країні або міжнародній організації відповідно до статей 44–49;
- будь-які зобов'язання відповідно до законодавства держав-членів, прийнятих відповідно до глави IX;
- невиконання наказу або тимчасове або остаточне обмеження на обробку або зупинення потоків даних контролюючим органом відповідно до статті 58 (2) або ненадання доступу з порушенням статті 58 (1).

відповідно до пункту 2 застосовуються адміністративні штрафи до 20000 000 євро, або у випадку зобов'язання – до 4% від загального світового річного обороту попереднього фінансового року залежно від того, яка сума є вищою:

За невиконання наказу контролюючого органу, зазначеного у статті 58 (2), відповідно до пункту 2 цієї статті, накладаються адміністративні штрафи до 20000 000 EUR, або у випадку підприємства, що становить до 4% загального світового річного обороту попереднього фінансового року, залежно від того, яка сума є вищою.

Без шкоди для коригуючих повноважень наглядових органів відповідно до статті 58 (2) кожна держава-член може встановити правила щодо того, чи можуть і в якій мірі накладатися адміністративні штрафи на органи державної влади та органи, створені в цій державі-члені.

Здійснення наглядовим органом своїх повноважень відповідно до цієї статті підлягає відповідним процедурним гарантіям відповідно до законодавства Союзу та держав-членів, включаючи ефективний судовий засіб захисту та належний процес.

Якщо правова система держави-члена не передбачає адміністративних штрафів, ця стаття може застосовуватися таким чином, що штраф ініціюється компетентним наглядовим органом та накладається компетентними національними судами, забезпечуючи, щоб ці правові засоби захисту були ефективні та мають аналогічний ефект від адміністративних штрафів, накладених наглядовими органами.

У будь-якому випадку, накладені штрафи повинні бути ефективними, пропорційними та стримуючими.

Держави-члени повинні повідомити Комісію про положення своїх законів, які вони приймають відповідно до цього пункту, до 25 травня 2018 року, та невідкладно про будь-які наступні закони про поправки чи поправки, що стосуються їх.

2. Законодавче регулювання обробки персональних даних компетентними органами у кримінальній сфері.

Відповідно до положень GDPR, опрацювання персональних даних про судимості і кримінальні злочини або пов'язані заходи безпеки здійснюють лише під контролем офіційного органу або у разі, якщо опрацювання дозволено законодавством Союзу або держави-члена, що передбачають належні гарантії для прав і свобод суб'єктів даних. Будь-який всеосяжний реєстр судимостей необхідно вести лише під контролем офіційного органу.

Такі дані регулюються особливо Загальним регламентом про захист даних. Вони представляють собою чутливі дані, які повинні оброблятися з відповідною обережністю, аналогічно до особливих категорій персональних даних. Вони підпорядковані особливим правилам, але не включаються безпосередньо до «особливих категорій персональних даних». Вони мають власний юридичний режим.

Офіційні органи, такі як правоохоронні агентства чи судові установи, мають вести обробку таких даних у рамках своєї компетенції та відповідно до законодавства. Законодавство ЄС або держави-члена може передбачати обробку даних про судимості і кримінальні злочини за певних умов та з урахуванням належних гарантій для прав і свобод суб'єктів даних. Будь-який реєстр судимостей повинен вестися лише під контролем офіційного органу. Це означає, що облік і збереження інформації про судимості має бути під суворим наглядом відповідних правоохоронних органів або інших офіційних органів, які мають відповідні повноваження. Ці обмеження та правила спрямовані на забезпечення належного захисту прав і свобод суб'єктів даних, а також на запобігання можливому зловживанню та недопущенню несанкціонованої обробки чутливих даних у контексті кримінальних справ та безпеки.

Приклади накладання штрафів

Хорватія.

Одна з кредитних установ (Хорватія, Загребі) систематично відмовляла громадянам у наданні інформації про свої персональні дані.

Незважаючи на зауваження AZOP (Croatian Personal Data Protection Agency) установа продовжувала відмовляти громадянам у доступі до їх персональних даних.

Після чисельних скарг АЗОП провів розслідування та встановив, що за період з 25 травня 2018 року по 30 квітня 2019 року в установу надійшло близько 2500 запитів від громадян, яким також було відмовлено.

AZOP призначив національній кредитній установі штраф у розмірі EUR20,000,000 за порушення вимог GDPR.

Швеція.

Шведське управління захисту даних (DPA) зробило зауваження Google за те, що вони не видалили два результати пошуку в 2017 році.

Зокрема, Google звинувачували за те, що вони зробили «занадто вузьку» оцінку того, які URL-адреси слід фактично видалити з результатів пошуку, а також за несвоєчасне видалення результатів пошуку.

У 2018 році, з огляду на те, що Google не повністю виконала раніше видане розпорядження, DPA ініціювала подальший аудит.

За результатами аудиту DPA накладає на Google як оператора пошукової системи за невідповідність вимогам GDPR, зокрема, за не виконання своїх зобов'язань щодо реалізації користувачами права на видалення даних штраф у розмірі 75 мільйонів шведських кронів (приблизно 7 мільйонів євро).

Перелік контрольних питань:

1. Що включають в себе персональні дані?
2. Коли набрав чинності Загальний регламент про захист даних (GDPR)?
3. Які критерії визначення сфери дії GDPR Вам відомі
4. Вкажіть основні поняття та принципи GDPR.
5. Наведіть характеристику суб'єкта даних, контролера оператора, процесора.
6. Які права є у суб'єкта даних згідно з GDPR.
7. Дайте характеристику повноваженням контролера та оператора.
8. Зазначте умови передачі персональних даних третім країнам.

Тест https://forms.gle/anRBz1NGQMrP8MvQ9

6. Електронна ідентифікація та довірчі послуги на внутрішньому ринку ЄС

1. Концептуальні підходи до формування системи правового регулювання електронної ідентифікації та надання довірчих послуг
2. Правові механізми впровадження електронної ідентифікації
3. Правові механізми надання електронних довірчих послуг

1. Концептуальні підходи до формування системи правового регулювання електронної ідентифікації та надання довірчих послуг

Ключовий фактор економічного та соціального розвитку ЄС: формування довіри до Інтернет-середовища.

Відсутність довіри, зокрема через відчутну відсутність правової визначеності, змушує споживачів, бізнес та органи державної влади вагатися здійснювати операції в електронному форматі та застосовувати нові послуги.

Для створення єдиного цифрового ринку необхідно:
- домогтися швидкого прогресу у ключових областях цифрової економіки;
- сприяти запровадженню єдиного інтегрованого цифрового ринку шляхом полегшення транскордонного використання он-лайн послуг;
- забезпечити:
  - використання безпечної електронної ідентифікації та автентифікації,
  - створення належних умов для взаємного транскордонного визнання ключових компонентів,
  - електронну ідентифікацію,
  - використання електронних документів та електронних підписів,
  - електронні послуги доставки.

Головні проблеми на шляху розвитку ефективної цифрової економіки, загрози при користуванні переваг єдиного цифрового ринку і транскордонних цифрових послуг є:
- фрагментація цифрового ринку,
- відсутність сумісності,
- зростання кіберзлочинності,
- національні схеми електронної ідентифікації не визнаються на території інших держав-членів.

Шляхи вирішення проблеми:

- Забезпечити безпеку електронних послуг та електронних підписів.
- Створити інфраструктури відкритого ключа на загальноєвропейському рівні.
- Створити портал для забезпечення транскордонної сумісності електронних підписів та підвищення рівня безпеки транзакцій, що здійснюється з використанням Інтернету.
- Забезпечити взаємне визнання засобів електронної ідентифікації та полегшити транскордонне надання численних он-лайн послуг на внутрішньому ринку ЄС.

Регламент ЄС № 910/2014 «Про електронну ідентифікацію та довірчі послуги для електронних транзакцій в межах внутрішнього ринку 23 липня 2014 р.

Мета Регламенту – забезпечення:
- належного функціонування внутрішнього ринку,
- належний рівень безпеки засобів електронної ідентифікації та довірчих послуг.

Регламент встановлює:
- умови взаємного визнання засобів електронної ідентифікації фізичних та юридичних осіб, які підпадають під нотифіковану схему електронної ідентифікації іншої держави-члена;
- правила щодо довірчих послуг, зокрема щодо електронних транзакцій; і
- правову базу для:
- електронних підписів,
- електронних печаток,
- електронних штампів часу,
- електронних документів,
- електронних служб зареєстрованої доставки та
- служб сертифікації для автентифікації веб-сайтів.

Сфера дії Регламенту

1) застосовується до схем електронної ідентифікації, про які було повідомлено державою-членом, а також до постачальників довірчих послуг, які створені в Союзі;

2) не застосовується до надання трастових послуг, які використовуються виключно в закритих системах, що є результатом національного законодавства або угод між визначеним набором учасників;

3) не зачіпає національного законодавства чи законодавства Союзу, пов'язаного з укладанням та дійсністю контрактів чи інших юридичних чи процесуальних зобов'язань, що стосуються юридичної форми.

Основні поняття

електронна ідентифікація – процес використання даних ідентифікації особи в електронній формі, що однозначно представляє або фізичну, або юридичну особу, або фізичну особу, яка представляє юридичну особу;

засоби електронної ідентифікації – матеріальна та / або нематеріальну одиницю, що містить ідентифікаційні дані особи, і яка використовується для автентифікації онлайн-послуги;

ідентифікаційні дані особи – набір даних, що дозволяє встановити особу фізичної або юридичної особи або фізичної особи, яка представляє юридичну особу;

схема електронної ідентифікації – система електронної ідентифікації, за якою засоби електронної ідентифікації видаються фізичним або юридичним особам або фізичним особам, що представляють юридичні особи;

автентифікація – електронний процес, який дозволяє підтвердити електронну ідентифікацію фізичної або юридичної особи або підтвердження походження та цілісності даних в електронній формі;

довіряюча сторона – фізичну або юридичну особу, яка покладається на електронну ідентифікацію або послугу довіри;

електронний підпис – означає дані в електронній формі, які додаються або логічно асоціюються з іншими даними в електронній формі і які використовуються підписантом для підписання;

вдосконалений електронний підпис – електронний підпис, який відповідає встановленим вимогам;

кваліфікований електронний підпис – вдосконалений електронний підпис, який створюється кваліфікованим пристроєм для створення електронного підпису і який базується на кваліфікованому сертифікаті електронних підписів;

дані створення електронного підпису – унікальні дані, які використовуються підписантом для створення електронного підпису;

сертифікат на електронний підпис – електронна атестація, яка пов'язує дані про підтвердження електронного підпису з фізичною особою та підтверджує принаймні ім'я або псевдонім цієї особи;

довірча послуга – електронна послуга, яка зазвичай надається за винагороду, яка складається з:

a. створення, перевірка та підтвердження електронних підписів, електронних печаток або електронних штампів часу, електронних зареєстрованих служб доставки та сертифікатів, пов'язаних із цими послугами, або
b. створення, перевірка та перевірка сертифікатів для автентифікації веб-сайтів; або
c. збереження електронних підписів, печаток або сертифікатів, пов'язаних із цими послугами;

кваліфікована довірча служба – довірча служба, яка відповідає застосовним вимогам, встановленим у цьому Регламенті

орган з оцінки відповідності – орган, який акредитований відповідно до цього Регламенту як компетентний для проведення оцінки відповідності кваліфікованого постачальника послуг довіри та кваліфікованого тресту послуги, які вона надає

постачальник довірчих послуг – фізична або юридична особа, яка надає одну або кілька довірчих трастових послуг як кваліфікований, так і некваліфікований постачальник трастових послуг;

сертифікат для автентифікації веб-сайту – атестація, яка дає змогу автентифікувати веб-сайт і комунікує веб-сайт на фізичну або юридичну особу, якій видано сертифікат;

кваліфікований сертифікат для автентифікації веб-сайту – сертифікат для аутентифікації веб-сайту, який видається кваліфікованим постачальником послуг довіри та відповідає вимогам, встановленим у Додатку IV;

2. Правові механізми впровадження електронної ідентифікації

Взаємне визнання

Електронна ідентифікація, яка є обов'язковою для доступу до послуги, що надається органом державного сектору за допомогою інтернет-технологій, може бути здійснення в будь який держави–члені із застосуванням засобів електронної ідентифікації та автентифікації, що видані органом державного сектору в будь-який держави-члені та які мають бути визнані у будь-який інший держави-члені для цілей транскордонної автентифікації за умови дотримання таких умов:

- засоби електронної ідентифікації видаються за схемою електронної ідентифікації, яка включена до переліку, опублікованого Комісією відповідно до статті 9 Регламенту;

- рівень впевненості засобів електронної ідентифікації відповідає рівню впевненості, рівному або вищому за рівень впевненості (суттєвого або високого), який вимагається відповідним органом державного сектору для доступу до цієї послуги в Інтернеті в держави-члені, в який необхідна обов'язкова ідентифікація відповідний орган державного сектору використовує рівень впевненості суттєвий або високий щодо доступу до цієї послуги в Інтернеті.

Засоби електронної ідентифікації, що видаються за схемою електронної ідентифікації, включеною до переліку, опублікованого Комісією відповідно до статті 9, і який відповідає низькому рівню впевненості, можуть бути визнані органами державного сектору для цілей транскордонної автентифікації для послуга, що надається в Інтернеті цими органами.

Вимоги до схеми електронної ідентифікації

1. засоби електронної ідентифікації (ЗЕІ) за схемою електронної ідентифікації видаються:

2. державою-членом, яка повідомляє;

3. за мандатом держави-члена, що повідомляє; або

4. незалежно від держави-члена, яка повідомляє, та визнані цією державою-членом;

5. ЗЕІ за схемою електронної ідентифікації можуть бути використані для доступу щонайменше до однієї послуги, яка надається

6. органом державного сектору і яка вимагає електронної ідентифікації у держави-члені, що повідомляє;

7. схема електронної ідентифікації та ЗЕІ, що видаються відповідно до неї, відповідають вимогам принаймні одного рівня впевненості, встановленого в імплементаційному акті, зазначеному у статті 8 (3);

8. держава-член, що повідомляє, гарантує, що ідентифікаційні дані особи, що однозначно представляють відповідну особу, присвоюються

9. відповідно до технічних специфікацій, стандартів та процедур для відповідного рівня впевненості, встановленого в імплементаційному акті,

10. сторона, яка видає ЗЕІ за цією схемою, гарантує, що засоби електронної ідентифікації приписуються особі, зазначеній у пункті (d) цієї статті, відповідно до технічних специфікацій, стандартів та процедур для відповідного рівня впевненості, встановлених у імплементаційний акт, зазначений у статті 8 (3);

11. держава-член, що повідомляє, забезпечує доступність автентифікації в Інтернеті, так що будь-яка довіряюча сторона, створена на території іншої держави-члена, зможе підтвердити дані ідентифікації особи, отримані в електронній формі.

Рівні впевненості в схемах електронної ідентифікації

Схема електронної ідентифікації повинна визначати низький, суттєвий та / або високий рівень надійності ЗЕІ, виданих відповідно до цієї схеми.

Рівні впевненості низький, суттєвий та високий повинні відповідати, відповідно, наступним критеріям:

- низький рівень впевненості стосується ЗЕІ, який забезпечує обмежений ступінь довіри до заявленої індивідуальності особи та характеризується посиланням на технічні специфікації, стандарти та процедури, пов'язані з цим, включаючи технічний контроль, метою якого є зменшення ризику зловживання або зміни ідентичності;
- суттєвий рівень впевненості відноситься до ЗЕІ, який забезпечує значну ступінь довіри до заявленої індивідуальності особи, і характеризується посиланням на технічні специфікації, стандарти та процедури, пов'язані з цим, включаючи технічний контроль, метою якого є істотне зменшення ризику неправильного використання або зміни ідентичності;
- високий рівень впевненості стосується ЗЕІ, який забезпечує вищий ступінь довіри до заявленої індивідуальності особи, ніж засоби електронної ідентифікації із значним рівнем впевненості, і характеризується посиланням до пов'язаних з ними технічних специфікацій, стандартів та процедур, включаючи технічний контроль, метою якого є запобігання неправильного використання або зміни ідентичності.

Мінімальні технічні характеристики, стандарти та процедури повинні бути встановлені з посиланням на надійність та якість наступних елементів:

a. процедура підтвердження та перевірки особи фізичних або юридичних осіб, які подають заявку на видачу засобів електронної ідентифікації;
b. порядок видачі запитуваних засобів електронної ідентифікації;
c. механізм автентифікації, за допомогою якого фізична або юридична особа використовує засоби електронної ідентифікації, щоб підтвердити свою особу надійній стороні;
d. суб'єкт, що видає засоби електронної ідентифікації;
e. будь-який інший орган, який бере участь у заявці на видачу засобів електронної ідентифікації; і
f. технічні характеристики та специфікації безпеки виданих засобів електронної ідентифікації.

Порушення безпеки

- Якщо або схема електронної ідентифікації, або автентифікація порушена або частково порушена таким чином, що впливає на надійність транскордонної автентифікації цієї схеми, держава-член, що повідомляє, невідкладно призупиняє або анулює цю транскордонну автентифікацію або відповідні компрометовані частини та інформує інші держави-члени та Комісію.

- Коли порушення або компрометація усуваються, держава-член відновлює транскордонну автентифікацію та інформує інші держави-члени та Комісію без зайвої затримки.

- Якщо порушення або компрометація не будуть усунені протягом трьох місяців після зупинення чи відкликання, держава-член, що повідомляє, повідомляє інші держави-члени та Комісію про скасування схеми електронної ідентифікації.

Відповідальність

1. Держава-член, що повідомляє, несе відповідальність за шкоду, заподіяну навмисно або з необережності будь-якій фізичній або юридичній особі внаслідок невиконання своїх зобов'язань.

2. Сторона, яка видає ЗЕІ, несе відповідальність за шкоду, заподіяну навмисно або з необережності будь-якій фізичній або юридичній особі внаслідок невиконання зобов'язання.

3. Сторона, яка здійснює процедуру автентифікації, несе відповідальність за шкоду, заподіяну навмисно або з необережності будь-якій фізичній або юридичній особі через неможливість забезпечення правильної роботи автентифікації.

Параграфи 1, 2 та 3 застосовуються відповідно до національних норм про відповідальність.

Співпраця та взаємодія

1. Національні схеми електронної ідентифікації повинні бути сумісними.

2. Для цих цілей встановлюється система взаємодії.

3. Структура взаємодії повинна відповідати наступним критеріям:
   1) вона прагне бути технологічно нейтральною і не проводить дискримінації між якимись національними технічними рішеннями щодо електронної ідентифікації в межах держави-члена;
   2) вона дотримується європейських та міжнародних стандартів, де це можливо;
   3) це полегшує реалізацію принципу конфіденційності за задумом;
   4) він забезпечує обробку персональних даних відповідно до Директиви 95/46 / ЄС.

Структура взаємодії складається з:
- посилання на мінімальні технічні вимоги, що стосуються рівнів впевненості;
- відображення національних рівнів достовірності повідомлених схем електронної ідентифікації до рівнів впевненості;
- посилання на мінімальні технічні вимоги щодо сумісності;
- посилання на мінімальний набір ідентифікаційних даних особи, що однозначно представляє фізичну або юридичну особу, який доступний в електронних схемах ідентифікації;
- правила процедури;
- порядок вирішення спорів;
- загальні стандарти оперативної безпеки.

Співпраця між державами-членами включає:

- обмін інформацією, досвідом та передовою практикою щодо схем електронної ідентифікації та, зокрема, технічних вимог, що стосуються рівня сумісності та рівня забезпечення;
- обмін інформацією, досвідом та передовою практикою щодо роботи з рівнями надійності схем електронної ідентифікації відповідно до статті 8;
- експертна перевірка схем електронної ідентифікації, що підпадають під дію цього Регламенту; і
- вивчення відповідних подій у секторі електронної ідентифікації.

3. Правові механізми надання електронних довірчих послуг

Відповідальність та тягар доказування

Постачальники довірчих послуг несуть відповідальність за шкоду, заподіяну навмисно або з необережності будь-якій фізичній або юридичній особі внаслідок невиконання зобов'язань, передбачених цим Регламентом.

Тягар доведення намірів або недбалості некваліфікованого постачальника довірчих послуг покладається на фізичну або юридичну особу, яка вимагає відшкодування шкоди, зазначеної у першому підпункті.

Намір або недбалість кваліфікованого постачальника послуг довірчого обслуговування вважається передбаченим, якщо тільки цей постачальник послуг кваліфікованого довірчого обслуговування не доведе, що збиток, зазначений у першому підпункті, стався без наміру або недбалості цього постачальника послуг кваліфікованого довірчого обслуговування.

Якщо постачальники довірчих послуг належним чином інформують своїх клієнтів про обмеження у використанні послуг, які вони надають, і коли ці обмеження впізнаються третіми сторонами, постачальники довірчих послуг не несуть відповідальності за збитки, спричинені використанням послуг, що перевищує вказані обмеження.

Міжнародні аспекти

Довірчі послуги, що надаються постачальниками довірчих послуг, заснованих у третій країні, визнаються юридично еквівалентними кваліфікованим довірчим послугам, що надаються кваліфікованими провайдерами довірчих послуг, заснованими в Союзі, де довірчі послуги, що походять з третьої країни, визнаються відповідно до угоди, укладеної між відповідний Союз та третя країна або міжнародна організація відповідно до статті 218 ДФЕС.

Наглядовий орган

Держави-члени призначають наглядовий орган, створений на їх території, або, за взаємною згодою з іншою державою-членом, наглядовий орган, створений у цій іншій державі-члені. Цей орган відповідає за наглядові завдання у відповідній державі-члені.

Наглядовим органам надаються необхідні повноваження та достатні ресурси для виконання покладених на них завдань.

Держави-члени повідомляють Комісії імена та адреси відповідних призначених їм наглядових органів.

Роль контролюючого органу повинна бути наступною:

1. здійснювати нагляд за кваліфікованими постачальниками трастових послуг, створеними на території призначеної держави-члена, щоб шляхом попередньої та пост наглядової діяльності забезпечити відповідність цих постачальників кваліфікованих довірчих послуг та кваліфікованих довірчих послуг вимогам, встановленим у цьому Регламенті;

2. вжити заходів, якщо це необхідно, стосовно некваліфікованих постачальників довірчих послуг, створених на території призначеної держави-члена, шляхом здійснення постнаглядової діяльності, коли їм повідомляють, що ці некваліфіковані постачальники довірчих послуг або довірчі послуги, які вони надають, нібито відповідають вимогам, встановленим цим Регламентом.

Завдання контролюючого органу включають, зокрема:

- співпрацювати з іншими наглядовими органами та надавати їм допомогу;

- аналізувати звіти про оцінку відповідності;

- інформувати інші наглядові органи та громадськість про порушення безпеки або втрату цілісності;

- звітувати перед Комісією про свою основну діяльність відповідно до пункту 6 цієї статті;

- проводити аудит або вимагати від органу з оцінки відповідності проведення оцінки відповідності кваліфікованих постачальників довірчих послуг;

- співпрацювати з органами захисту даних, зокрема, повідомляючи їх без зайвої затримки, про результати перевірок кваліфікованих постачальників довірчих послуг, де правила захисту персональних даних виявляються порушеними;

- надати кваліфікований статус довірчим постачальникам послуг та послугам, які вони надають, та анулювати цей статус.

Вимоги безпеки до довірчих постачальників послуг

Кваліфіковані та некваліфіковані постачальники довірчих послуг вживають відповідних технічних та організаційних заходів для управління ризиками, що становлять безпеку трастових послуг, які вони надають.

Кваліфіковані та некваліфіковані постачальники довірчих послуг повинні без зайвої затримки, але в будь-якому випадку протягом 24 годин після того, як про це дізналися, повідомити наглядовий орган та, де це можливо, інші відповідні органи, такі як компетентний національний орган, про інформацію безпеки або уповноваженого органу з захисту даних, будь-якого порушення безпеки або втрати цілісності, що суттєво впливає на надану послугу довіри або на персональні дані, що в ній зберігаються.

Якщо порушення безпеки або втрата цілісності може негативно вплинути на фізичну або юридичну особу, якій надано довірену послугу, постачальник довірчих послуг також повинен повідомити фізичну або юридичну особу про порушення безпеки або втрату цілісності без надмірна затримка.

За необхідності, зокрема, якщо порушення безпеки або втрата цілісності стосується двох або більше держав-членів, нотифікований наглядовий орган інформує наглядові органи інших зацікавлених держав-членів та ENISA.

Кваліфіковані довірчі послуги

Вимоги до кваліфікованих постачальників послуг довіри

1. Видаючи кваліфікований сертифікат на довірчу послугу, постачальник кваліфікованих довірчих послуг перевіряє, відповідними засобами та відповідно до національного законодавства, особу та, якщо це допустимо, будь-які конкретні атрибути фізичної або юридичної особи, якій кваліфікований видається сертифікат.
   Інформація, зазначена в першому підпункті, перевіряється відповідно до національного законодавства:
   a. фізичною присутністю фізичної особи або уповноваженого представника юридичної особи; або
   b. віддалено, з використанням засобів електронної ідентифікації, для яких до видачі кваліфікованого сертифіката була забезпечена фізична присутність фізичної особи або уповноваженого представника юридичної особи і яка відповідає вимогам, викладеним у статті 8 щодо рівні впевненості «значний» або «високий»; або
   c. за допомогою сертифіката кваліфікованого електронного підпису або кваліфікованої електронної печатки, виданого відповідно до пунктів (a) або (b);

2. Постачальник кваліфікованих довірчих послуг зобов'язаний:
   1) інформувати наглядовий орган про будь-які зміни у наданні його кваліфікованих довірчих послуг та про намір припинити цю діяльність;
   2) найняти персонал та, якщо це можливо, субпідрядників, які мають необхідний досвід, надійність, досвід та кваліфікацію

та які пройшли відповідну підготовку щодо правил безпеки та захисту персональних даних, і застосовуватимуть адміністративні та управлінські процедури, що відповідають європейським або міжнародним стандартам;
   3) підтримувати достатні фінансові ресурси та / або отримувати відповідне страхування відповідальності відповідно до національного законодавства;
   4) чітко та всебічно повідомляти будь-яку особу, яка бажає скористатися кваліфікованою послугою довіри, про точні умови використання цієї послуги, включаючи будь-які обмеження щодо її використання;
   5) використовувати надійні системи та продукти, які захищені від модифікацій та забезпечують технічну безпеку та надійність підтримуваних ними процесів;
   6) використовувати надійні системи для зберігання наданих йому даних у перевіряній формі

3. Постачальник кваліфікованих довірчих послуг зобов'язаний:
   a. вжити відповідних заходів проти підробки та крадіжки даних;
   b. реєструвати та зберігати доступними протягом відповідного періоду часу, включаючи після припинення діяльності постачальника послуг кваліфікованого довірчого обслуговування, всю відповідну інформацію стосовно даних, виданих та отриманих постачальником послуг кваліфікованих довірчих послуг, зокрема, з метою надання юридичних доказів з метою забезпечення безперервності служби. Такий запис може здійснюватися в електронному вигляді;
   c. мати сучасний план припинення для забезпечення безперервності служби відповідно до положень, перевірених наглядовим органом відповідно до пункту (i) статті 17 (4);
   d. забезпечити законну обробку персональних даних відповідно до Директиви 95/46 / ЄС;
   e. у випадку, якщо постачальники кваліфікованих довірчих послуг видають кваліфіковані сертифікати, встановити та постійно оновлювати базу даних сертифікатів.

Довірені списки

Кожна держава-член створює, підтримує та публікує списки довірених осіб, включаючи інформацію, що стосується кваліфікованих постачальників довірчих послуг, за яких вона відповідає, разом з інформацією, що стосується наданих ними кваліфікованих довірчих послуг.

Держави-члени повинні створювати, підтримувати та публікувати захищеним чином електронно підписані або скріплені печаткою довірені списки, у формі, придатній для автоматизованої обробки.

Держави-члени повідомляють Комісії без необґрунтованої затримки інформацію про орган, відповідальний за створення, ведення та публікацію національних довірених списків, та деталі, де такі списки публікуються, сертифікати, що використовуються для підписання або печатки довірених списків, та будь-які інші зміни до них.

Комісія надає громадськості через захищений канал інформацію в електронному підписі або запечатаною формі, придатній для автоматизованої обробки.

Електронні підписи

Правові наслідки електронних підписів

Електронному підпису не може бути відмовлено в юридичній дії та прийнятності як доказі в судовому процесі лише на тій підставі, що він знаходиться в електронній формі або що він не відповідає вимогам щодо кваліфікованих електронних підписів.

1. Кваліфікований електронний підпис має еквівалентну юридичну силу рукописного підпису.

2. Кваліфікований електронний підпис на основі кваліфікованого сертифіката, виданого в одній державі-члені, визнається кваліфікованим електронним підписом у всіх інших державах-членах.

Вимоги до вдосконалених електронних підписів

Удосконалений електронний підпис повинен відповідати таким вимогам:
- він однозначно пов'язаний з підписантом;
- він здатний ідентифікувати підписанта;
- він створюється з використанням даних створення електронного підпису, які підписант може, з високим рівнем довіри, використовувати під своїм єдиним контролем; і
- він пов'язаний з підписаними даними таким чином, що будь-яка подальша зміна даних може бути виявлена.

Електронні підписи в державних службах

Якщо держава-член вимагає вдосконаленого електронного підпису для використання Інтернет-послуг, що пропонуються органом державного сектору або від його імені, ця держава-член визнає вдосконалені електронні підписи на основі кваліфікованого сертифіката на електронні підписи та кваліфіковані електронні підписи принаймні у форматах або з використанням методів.

Якщо держава-член вимагає вдосконаленого електронного підпису на основі кваліфікованого сертифіката для використання Інтернет-послуг, що пропонуються органом державного сектору або від його імені, ця держава-член повинна визнати вдосконалені електронні підписи на основі кваліфікованого сертифіката та кваліфікованого електронного підписи щонайменше у форматах або з використанням методів, визначених у актах імплементації.

Держави-члени не повинні вимагати транскордонного використання в Інтернет-службі, що пропонується органом державного сектору, електронного підпису на вищому рівні безпеки, ніж кваліфікований електронний підпис.

Кваліфіковані сертифікати на електронний підпис

Кваліфіковані сертифікати електронних підписів повинні відповідати вимогам.

На кваліфіковані сертифікати електронних підписів не поширюється жодна обов'язкова вимога, що перевищує вимоги.

Якщо кваліфікований сертифікат для електронних підписів був анульований після первинної активації, він втрачає свою силу з моменту його анулювання, і його статус ні за яких обставин не може бути скасовано.

За умови дотримання таких умов держави-члени можуть встановити національні правила щодо тимчасового призупинення дії кваліфікованого сертифіката для електронного підпису:

a) якщо тимчасово призупинено дію кваліфікованого сертифіката для електронного підпису, цей сертифікат втрачає свою дію на період призупинення;
b) період призупинення повинен бути чітко зазначений у базі даних сертифікатів, а статус призупинення повинен бути видимим протягом періоду призупинення у службі, що надає інформацію про статус сертифіката.

Вимоги до кваліфікованих пристроїв для створення електронного підпису

Кваліфіковані пристрої для створення електронного підпису повинні відповідати вимогам.

Комісія може шляхом імплементаційних актів встановити контрольні номери стандартів для кваліфікованих пристроїв для створення електронного підпису. Відповідність вимогам, передбачається, коли кваліфікований пристрій для створення електронного підпису відповідає цим стандартам. Ці виконавчі акти повинні бути прийняті відповідно до процедури експертизи.

Сертифікація кваліфікованих пристроїв для створення електронного підпису

Відповідність кваліфікованих пристроїв для створення електронного підпису вимогам повинна засвідчуватися відповідними державними або приватними органами, визначеними державами-членами.

Сертифікація базується на одному з наступного:

a) процес оцінки безпеки, проведений відповідно до одного зі стандартів оцінки безпеки продуктів інформаційних технологій, включених до переліку, складеного відповідно до другого підпункту; або
b) процес, відмінний від процесу, зазначеного в пункті (a), за умови, що він використовує порівнянні рівні безпеки та за умови, що державний або приватний орган, зазначений у параграфі 1, повідомляє про цей процес Комісію. Цей процес може бути використаний лише за відсутності стандартів, зазначених у пункті (a), або коли триває процес оцінки безпеки, зазначений у пункті (a).

Аутентифікація веб-сайту

Вимоги до кваліфікованих сертифікатів для автентифікації веб-сайтів

Кваліфіковані сертифікати для автентифікації веб-сайтів повинні відповідати вимогам, встановленим у Додатку IV.

Комісія може шляхом імплементаційних актів встановити контрольні номери стандартів кваліфікованих сертифікатів для автентифікації веб-сайтів. Відповідність вимогам, встановленим у Додатку IV, передбачається, коли кваліфікований сертифікат для автентифікації веб-сайту відповідає цим стандартам. Ці виконавчі акти повинні бути прийняті відповідно до процедури експертизи.

Кваліфіковані сертифікати для автентифікації веб-сайту повинні містити:

- зазначення, принаймні у формі, придатній для автоматизованої обробки, що сертифікат виданий як кваліфікований сертифікат для автентифікації веб-сайту;

- набір даних, що однозначно представляє кваліфікованого постачальника послуг довіри, що видає кваліфіковані сертифікати, включаючи принаймні державу-член, в якій цей постачальник знаходиться, та:

- для юридичної особи: ім'я та, де це можливо, реєстраційний номер, як зазначено в офіційних документах,

- для фізичної особи: ім'я особи;

- для фізичних осіб: принаймні ім'я особи, якій видане посвідчення, або псевдонім. Якщо використовується псевдонім, він повинен бути чітко зазначений;

- для юридичних осіб: принаймні ім'я юридичної особи, якій видано свідоцтво, і, де це можливо, реєстраційний номер, як зазначено в офіційних записах;

- елементи адреси, включаючи принаймні місто та державу, фізичної або юридичної особи, якій видано свідоцтво, і, якщо це допустимо, як зазначено в офіційних записах;

- деталі початку та закінчення строку дії сертифіката;

Кваліфіковані сертифікати для автентифікації веб-сайту повинні містити:

1) доменне ім'я (імена), яким керує фізична або юридична особа, якій видано сертифікат; деталі початку та закінчення строку дії сертифіката;

2) ідентифікаційний код сертифіката, який повинен бути унікальним для кваліфікованого постачальника послуг довіри;

3) вдосконалений електронний підпис або вдосконалена електронна печатка постачальника кваліфікованих послуг довірчого обслуговування;

4) місце, де сертифікат, що підтверджує вдосконалений електронний підпис або вдосконалену електронну печатку, зазначений у пункті (h), надається безкоштовно;

5) місцезнаходження служб статусу дійсності сертифіката, за допомогою яких можна дізнатись про стан дійсності кваліфікованого сертифіката.

Перелік контрольних питань:

1. Який документ ЄС встановив умови взаємного визнання засобів електронної ідентифікації фізичних та юридичних осіб.
2. Поясніть значення кваліфікованого електронного підпису.
3. Яким вимогам повинен відповідати удосконалений електронний підпис.
4. Що таке сертифікат на електронний підпис?
5. Поясніть значення довірчих послуг та кваліфікованих довірчих послуг.
6. Поясніть процес електронної ідентифікації.
7. Кого представляє собою постачальник довірчих послуг?
8. Ким видаються засоби електронної ідентифікації (ЗЕІ) за схемою електронної ідентифікації?

Тест https://forms.gle/Jh6CgWtX9nqFSCNv

РОЗДІЛ III

ПРАВОВІ ПРОБЛЕМИ ЗАСТОСУВАННЯ БАЗОВИХ ТЕХНОЛОГІЙ ІНТЕРНЕТУ РЕЧЕЙ

7. Правові проблеми застосування хмарних технологій та великих даних (big data)

1. Основні положення Європейської ініціативи щодо хмарних технологій
2. Правові проблеми створення системи конкурентоспроможної економіки знань в Європі

1. Основні положення Європейської ініціативи щодо хмарних технологій.

Хмарні обчислення (англ. cloud computing) – це модель забезпечення повсюдного та зручного мережевого доступу до загального пулу конфігуруємих обчислювальних ресурсів:

- серверів,
- пристроїв зберігання даних,
- операційних систем,
- СУБД,
- додатків і
- сервісів

як разом, так і окремо, які можуть бути оперативно надані і звільнені з мінімальними експлуатаційними витратами і / або зверненнями до провайдера.

Основні переваги:

- не потрібні великі обчислювальні потужності ПК (смартфон, планшет тощо);
- відмовостійкість;
- певний рівень безпеки;
- висока швидкість обробки даних;
- економія на вартості софту – всі необхідні програми вже є в сервісі, де будуть працювати додатки;
- економія пристроїв для збереження даних.

Основні недоліки

- залежність у забезпеченні кібербезпеки від сторонньої компанії;
- ризик доступу сторонніх до даних;
- поява хмарних монополістів;
- необхідність мережі передачі даних для роботи;
- небезпека хакерських атак на сервер (при зберіганні даних на комп'ютері ви в будь-який час можете відключитися від мережі і очистити систему за допомогою антивірусу);
- волатильність політики монетизації надання послуг;

Класифікація моделей надання послуг хмарних технологій

- **SaaS:** Software as a Service, «Програмне забезпечення як послуга»;
- **PaaS:** Platform as a Service, «Платформа як послуга»;
- **IaaS:** Infrastructure as a Service, «Інфраструктура як послуга»;
- **DaaS:** Data as a Service, «Дані як послуга»;
- **WaaS:** Workplace as a Service, «Робоче місце як послуга»;
- **AaaS:** All as a Service, «Усе як послуга».

Це означає, що користувачі:

- можуть керувати майже необмеженою обчислювальною потужністю на вимогу,
- їм не потрібно робити великих капітальних вкладень для задоволення своїх потреб і що
- вони можуть дістатися до своїх даних з будь-якого місця через Інтернет,
- можуть потенційно зменшити витрати на IT та
- забезпечити можливість розробки багатьох нових сервісів.

Використовуючи хмару:

- найменші фірми можуть охопити все більші ринки,
- уряди можуть зробити послуги більш привабливими та ефективними навіть при скороченні витрат.

Природа та переваги хмарних обчислень

Хмарні обчислення мають ряд визначальних особливостей:

- обладнання (комп'ютери, пристрої зберігання даних) належить постачальнику хмарних обчислень, а не користувачеві, який взаємодіє з ним через Інтернет;

- використання апаратури динамічно оптимізується через мережу комп'ютерів, так що точне розташування даних або процесів та інформація, яка апаратура фактично обслуговує певного користувача в даний момент, в принципі не повинні турбувати користувача, навіть якщо це може мати важливе значення для відповідного правового середовища;

- хмарні постачальники часто переміщують навантаження своїх користувачів навколо (наприклад, з одного комп'ютера на інший або з одного центру обробки даних в інший) для оптимізації використання наявного обладнання;

- віддалене апаратне забезпечення зберігає та обробляє дані та робить їх доступними, наприклад, через додатки (щоб використовувати хмарні обчислення точно так само, як споживачі вже сьогодні використовують свої облікові записи веб-пошти);

- організації та особи можуть отримувати доступ до їх контенту та користуватися своїм програмним забезпеченням, коли і де вони потребують;

- хмарна настройка складається з шарів: апаратного забезпечення, проміжного програмного забезпечення або платформи та прикладного програмного забезпечення.

- стандартизація важлива, особливо на середньому шарі, оскільки дає можливість розробникам звертатися до широкого кола потенційних клієнтів та надає користувачам вибір;

- користувачі зазвичай платять за користування, уникаючи великих передових та постійних витрат, необхідних для створення та експлуатації складного обчислювального обладнання;

- в той же час, користувачі можуть дуже легко змінювати кількість обладнання, яке вони використовують (наприклад, за кілька секунд принести нову ємність пам'яті в Інтернеті за допомогою декількох клацань миші).

Ключові сфери, які потребують дії:

- фрагментація єдиного цифрового ринку через різні національні законодавчі рамки та невизначеності щодо застосовного законодавства, цифрового контенту та розташування даних;

- занепокоєння щодо доступу та переносу даних, контролю за змінами та правами власності на дані, встановлення відповідальності за збої в сервісі (простої або втрата даних),

права користувача на оновлення системи, що визначаються в односторонньому порядку, постачальником прав власності на дані, створені в хмарних додатках, або як вирішуються суперечки.

- джунглі стандартів створюють плутанину через, з одного боку, поширення стандартів, а з іншого – відсутність визначеності щодо того, які стандарти забезпечують належний рівень сумісності форматів даних, щоб дозволити переносимість; ступінь існування гарантій захисту персональних даних; або проблема порушень даних та захисту від кібератак.

- побудова публічно доступних хмарних пропозиції («публічна хмара» які відповідають європейським стандартам не лише в регуляторному плані, але й в плані конкурентоспроможності, відкритості та безпеки.

- Це не перешкоджає державним органам створювати спеціальні приватні хмари для обробки конфіденційних даних, але в цілому навіть хмарні послуги, що використовуються державним сектором, повинні, наскільки це можливо, бути предметом конкуренції на ринку, щоб забезпечити найкраще співвідношення ціни та якості.

Цифровий порядок денний для Європи

У програмі «Цифровий порядок денний для Європи» Комісія поставила собі за мету «спростити оформлення авторських прав, управління та транскордонне ліцензування».

Ключові дії, визначені в Цифровому порядку денному для досягнення цих цілей, відслідковуються та підвищують потенціал Європи використовувати нові цікаві можливості хмарних обчислень як для виробників, так і для споживачів цифрового контенту.

Має бути зроблена оцінка необхідності уточнення сфери застосування виключення з приватного копіювання та застосувань зборів, зокрема, наскільки послуги хмарних обчислень дозволяють отримати пряму винагороду правоволодільці, що виключені з режиму приватного збору за копіювання.

Дії щодо створення цифрової впевненості

- захист даних – ключове питання, що може перешкодити застосуванню хмарних обчислень;
- 27 варіантів національних законодавчих рамок;
- проблеми міжнародної передачі даних;
- нова законодавча база має забезпечити необхідні умови для прийняття кодексів поведінки та стандартів хмари;
- договірне право також було проблемою для негативного впливу на цифрову довіру споживачів, які не мали впевненості у своїх правах та бракували захисту, а торговцям необхідна база, яка полегшила б їм пропонувати свою продукцію в Інтернеті.

Поняття та характеристика Великих даних (big data)

«Великі дані» (англ. Big data) – величезні об'єми різнорідної інформації, які за умови застосування методів та технологій економічно доцільної обробки є джерелом предметно та локально корисної інформації.

Ознаки Big data

3 головних властивості – «VVV».

1. **Volume** – обсяг інформації. Розмір великих даних обчислюється по фізичному обсягу інформації.

2. **Velocity** – регулярний аналіз даних в зв'язку з їх постійним оновленням. Як і будь-яка інформація, Біг дата постійно змінюється. Тому для актуальних даних потрібно проводити регулярну обробку масивів інформації.

3. **Variety** – різноманітність форматів даних.

Big data в бізнесі може бути структурованою і неструктурованою, приблизне співвідношення 20% – це структуровані дані, а решта 80% – не структуровані дані.

Джерела Big data

Окремих джерел великих даних не існує.

Суть методу полягає в тому, що він включає в себе різні джерела і отримує з них раніше невідому інформацію.

До джерел big data можна віднести наступні:

- Інтернет,
- соціальні мережі,
- засоби масової інформації,
- форуми, сайти.
- Корпоративна інформація,
- архіви,
- сховища даних,
- дані приладів, датчиків, метеорологічні показники тощо.

Переваги Big data в бізнесі

Використання системи аналізу великих даних в бізнесі має такі переваги:

- Легке планування роботи.
- Підвищення швидкості відкриття поліпшених проектів.
- Збільшення шансів нових проектів на отримання прибутковості і затребуваності.
- Можливість аналізу ступеня задоволеності споживачів.
- Полегшення пошуку і залучення потенційних клієнтів.
- Збільшення швидкості інтеграції зі споживачами і контрагентами.
- Раціоналізації інтеграції в системі поставок.
- Поліпшення якості споживчого сервісу і швидкості інтеграції.
- Поліпшення лояльності користувачів.

Вільний обмін неособистими даними в Європейському Союзі

Регламент (ЄС) 2018/1807 Європейського Парламенту та Ради від 14 листопада 2018 р. про рамки для вільного обміну неособистими даними в Європейському Союзі

Мета

забезпечення вільного потоку даних, окрім персональних даних всередині Союзу, шляхом встановлення правил, що стосуються вимог щодо

- локалізації даних,
- доступності даних для компетентних органів та
- перенесення даних для професійних користувачів.

Сфера застосування Регламенту

Регламент застосовується до обробки електронних даних, крім персональних даних у Союзі, а це:

- надається як послуга користувачам, які проживають або мають представництво в Союзі, незалежно від того, постачальник послуг є в Союзі чи ні; або
- здійснюється фізичною або юридичною особою, яка проживає або має представництво в Союзі для власних потреб.

У випадку набору даних, що складається як з не персональних, так і з персональних даних, це Положення застосовується до частини, що не стосується персональних даних, у наборі даних.

Поняття

«дані» означають дані, окрім персональних даних, як визначено у пункті 1 статті 4 Регламенту (ЄС) 2016/679;

«обробка» означає будь-яку операцію або набір операцій, які виконуються над даними або наборами даних в електронному форматі, незалежно від автоматизованих засобів, таких як збір, запис, організація, структурування, зберігання, адаптація чи зміна, пошук, консультація, використання, розкриття інформації шляхом передачі, розповсюдження чи іншим доступом до них, вирівнювання або поєднання, обмеження, стирання чи знищення;

«проект акту» означає текст, розроблений з метою прийняття як закон, підзаконний акт або адміністративне положення загального характеру, текст знаходиться на стадії підготовки, на якій все ще можуть бути внесені суттєві зміни;

«постачальник послуг» означає фізичну чи юридичну особу, яка надає послуги з обробки даних;

«вимога щодо локалізації даних» означає будь-яке

- зобов'язання,
- заборону,
- умову,
- обмеження чи
- іншу вимогу,

передбачену законами, положеннями або адміністративними положеннями держави-члена або що випливає із загальної та послідовної адміністративної практики в державі-члені та в органах, що регулюються публічним законодавством, у тому числі у сфері державних закупівель, яка нав'язує обробку даних на території конкретної держави-члена або перешкоджає обробці даних у будь-якій іншій державі-члені;

«компетентний орган» означає орган держави-члена або будь-який інший орган, уповноважений національним законодавством виконувати державну функцію або здійснювати офіційні повноваження, який має право отримати доступ до даних, оброблених фізичною або юридичною особою для виконання своїх повноважень, передбачені законодавством Союзу чи національним законодавством;

«користувач» означає фізичну чи юридичну особу, включаючи державний орган чи орган, що регулюється публічним законодавством, які використовують або вимагають послуги з обробки даних;

«професійний користувач» означає фізичну чи юридичну особу, включаючи державний орган чи орган, що регулюється публічним законодавством, які використовують або вимагають послуги з обробки даних для цілей, пов'язаних з їх торгівлею, бізнесом, ремеслом, професією чи завданням.

Вільне переміщення даних в межах Союзу

Вимоги до локалізації даних забороняються, якщо вони не обґрунтовані з міркувань громадської безпеки відповідно до принципу пропорційності.

До 30 травня 2021 року держави-члени забезпечують скасування будь-яких існуючих вимог щодо локалізації даних, встановлених законом, підзаконним актом або адміністративним положенням загального.

Держави-члени повинні надавати детальну інформацію про будь-які вимоги щодо локалізації даних, викладених у законі, постанові або адміністративному забезпеченні загального характеру та застосовних на їх території, у відкритому доступі через єдиний національний інформаційний пункт.

Доступність даних для компетентних органів

Цей Регламент не впливає на повноваження компетентних органів вимагати або отримувати доступ до даних для виконання своїх повноважень відповідно до законодавства Союзу чи національного законодавства.

Доступ до даних компетентними органами не може бути відхилений на підставі того, що дані обробляються в іншій державі-члені.

Якщо запит про допомогу передбачає отримання запитуваним органом доступу до будь-якого приміщення фізичної чи юридичної особи, включаючи будь-яке обладнання та засоби обробки даних, такий доступ повинен відповідати законодавству Союзу чи національному процесуальному законодавству.

Держави-члени можуть накладати ефективні, пропорційні та стримувальні санкції за невиконання зобов'язання щодо надання даних відповідно до законодавства Союзу та національного законодавства.

Перенесення даних

Комісія заохочує та сприяє розробці саморегулюючих кодексів поведінки на рівні Союзу («кодексів поведінки»), щоб сприяти конкурентоспроможній економіці даних, що базується на принципах прозорості та сумісності та з урахуванням належного врахування відкритих стандартів, що охоплюють, серед іншого, такі аспекти:

- кращі практики для полегшення підключення постачальників послуг та перенесення даних у структурованому, загальновживаному та машиночитанному форматі, включаючи відкриті стандартні формати, якщо цього вимагає постачальник послуг, що отримує дані;

- мінімальні вимоги до інформації, для забезпечення надання професійним користувачам для укладення договору на обробку даних, достатньо детальною, чіткою та прозорою інформацією щодо процесів, технічних вимог, строків та зборів, що застосовуються у випадку, якщо професійний користувач хоче перейти на іншого постачальник послуг або перенесення даних назад до власних IT-систем;

- підходи до схем сертифікації, які полегшують порівняння продуктів та послуг з обробки даних для професійних користувачів з урахуванням встановлених національних чи міжнародних норм, щоб полегшити порівнянність цих товарів та послуг.

- такі підходи можуть включати, серед іншого, управління якістю, управління інформаційною безпекою, управління безперервністю бізнесу та управління довкіллям;

- дорожні карти комунікацій, що використовують мультидисциплінарний підхід для підвищення обізнаності щодо кодексів поведінки серед відповідних зацікавлених сторін.

Комісія забезпечує, щоб кодекси поведінки розроблялися у тісній співпраці з усіма відповідними зацікавленими сторонами, включаючи асоціації МСП та стартапів, користувачів та постачальників хмарних послуг.

Порядок співпраці між владою

Кожна держава-член призначає єдиний пункт зв'язку щодо застосування цього Регламенту.

Якщо компетентний орган в одній державі-члені прохання про допомогу у іншої держави-члена відповідно до статті 5 (2), щоб отримати доступ до даних, він повинен направити належним чином обґрунтований запит в призначений останнім єдиний пункт зв'язку. Запит повинен

містити письмове пояснення причин і правових підстав для отримання доступу до даних.

Будь-яка інформація, якою обмінюються в контексті запитуваної допомоги і яка надається відповідно до статті 5 (2), використовується тільки щодо питання, по якому вона була запрошена.

Окремі пункти зв'язку надають користувачам загальну інформацію про цих Правилах, в тому числі про кодексах поведінки.

Керівництво щодо Регламенту про рамки вільного обміну неособистими даними в Європейському Союзі

Неперсональні дані

Неособисті дані можуть бути класифіковані за походженням як:

- дані, які не стосувались ідентифікованої або фізичної особи, яку можна ідентифікувати, наприклад, дані про погодні умови, що створюються датчиками, встановленими на вітрових турбінах, або дані про потреби у технічному обслуговуванні промислових машин;

- дані, це анонімізовані персональні дані, тобто дані за допомогою яких неможливо ідентифікувати фізичну особу.

Змішаний набір даних

Змішаний набір даних складається як з особистих, так і з неособистих даних.

Змішані набори даних представляють більшість наборів даних, що використовуються в економіці даних, і є поширеними через технологічні розробки, такі як:
- Інтернет речей (тобто об'єкти, що з'єднують цифровим шляхом),
- штучний інтелект та
- технології, що дозволяють проводити аналітику великих даних.

Перенесення даних та їх перемикання між постачальниками хмарних послуг

Однією з цілей регулювання вільного потоку неособистих даних є уникнення практики блокування постачальників.

Ці практики виникають, коли користувачі не можуть перемикатися між постачальниками послуг, оскільки їх дані «заблоковані» в системі постачальника, наприклад, через специфічний формат даних або договірні домовленості, і не можуть бути передані поза IT-системою постачальника.

Перенос даних без перешкод є важливим, щоб дозволити користувачам вільно вибирати між постачальниками послуг з обробки даних та таким чином забезпечити ефективну конкуренцію на ринку.

Переносимість даних між підприємствами стає все більш важливою для широкого спектру цифрових галузей, включаючи хмарні послуги.

2. Правові проблеми створення системи конкурентоспроможної економіки знань в Європі

ЄС може стати провідною моделлю для суспільства, в якому дані будуть надавати можливості людям приймати кращі рішення як у бізнесі, так і державному секторі.

Для реалізації цієї амбіції ЄС має розбудовувати:
- найміцнішу законодавчу базу – із захисту даних, основних прав, безпеки та кібербезпеки;
- внутрішній ринок з конкурентними компаніями будь-якого розміру та різноманітної промислової бази;
- систему злагодженого вирішення питання, починаючи від підключення до обробки та зберігання даних, обчислювальної потужності та кібербезпеки.
- досконалу структуру управління для обробки даних та збільшити кількість якісних даних, доступних для використання та повторного використання.

Важливість даних для економіки та суспільства

Дані будуть трансформувати спосіб виробництва, споживання та використання. Переваги відчуватимуться в кожному аспекті нашого життя, починаючи від більш свідомого споживання енергії та відстеження продуктів, матеріалів та продуктів харчування, до більш здорового життя та покращення охорони здоров'я.

Персоналізована медицина краще реагуватиме на потреби пацієнтів, дозволяючи лікарям приймати рішення, що підтримуються даними. Це дасть можливість в потрібний час адаптувати правильну терапевтичну стратегію до потреб потрібної людини та / або визначити схильність до захворювання та / або забезпечити своєчасну та цілеспрямовану профілактику.

Бачення

- повага до європейських цінностей та основних прав та переконання, що людина є і повинна залишатися в центрі;
- бізнес та державний сектор в ЄС можуть бути наділені повноваженнями за допомогою використання даних для прийняття кращих рішень;
- необхідним є використання можливостей, що надаються даними для соціального та економічного блага;
- дані на відміну від більшості економічних ресурсів – можуть бути тиражуються при майже нульовій вартості, а використання їх однією людиною чи організацією не перешкоджає одночасному використанню інша людина чи організація;
- необхідно забезпечити кращий доступ до даних та відповідальне їх використання;
- створити привабливе політичне середовище до 2030 р.;
- створити єдиний європейський простір даних – справжній єдиний ринок даних, відкритий для даних з усього світу – де особисті та не персональні дані, включаючи чутливі бізнес-дані, захищені.

Міжгалузева рамка управління для доступу та використання даних

Підтримка: Інвестиції в дані та зміцнення європейських можливостей та інфраструктури для розміщення, обробки та використання даних, сумісність

Компетенції: розширення можливостей для осіб, вкладення коштів у навички та в малі та середні підприємства

Спільні європейські простори даних у стратегічних секторах та сферах, що становлять суспільний інтерес

Єврокомісія підтримає створення дев'яти загальноєвропейських просторів даних:

- Спільний європейський промисловий (виробничий) простір даних для підтримки конкурентоспроможності та ефективності промисловості ЄС.
- Спільний європейський простір даних «Зелена угода» щодо змін клімату.
- Спільний європейський простір даних про мобільність для позиціонування Європи на передньому плані розвитку інтелектуальної транспортної системи, включаючи сполучені автомобілі та інші види транспорту.
- Спільний європейський простір даних про охорону здоров'я.
- Спільний європейський простір фінансових даних.
- Спільний європейський простір даних про енергетику.
- Спільний європейський простір даних про сільське господарство.
- Спільний європейський простір даних для державного управління
- Спільний європейський простір даних про навички, щоб зменшити невідповідність навичок між системою освіти та навчання, з одного боку, та потребами ринку праці, з іншого.

Перелік контрольних питань

1. Охарактеризуйте правову і технічну складову забезпечення доступу до хмарних послуг
2. У чому полягає відмінність моделей надання хмарних послуг (SaaS, PaaS, DaaS, AaaS)
3. Які ознаки Big data?
4. Які ризики для держави бізнесу суспільства несе повсюдне застосування хмарних технологій
5. У чому полягають переваги використання хмарних сервісів
6. Які дані не включає Регламент ЄС про рамки для вільного обміну неособистими даними в ЄС?

Тест https://forms.gle/obvA31eu4TNE6pMu9 7.

8. Правове регулювання використання роботів та штучного інтелекту

1. Базові положення рекомендацій Європейського парламенту щодо визначення цивільно-правового регулювання використання роботів
2. Теоретико-методологічні засади визначення правосуб'єктності роботів з штучним інтелектом
3. Проблеми правового регулювання надання послуг роботами з штучним інтелектом

1. Базові положення рекомендацій Європейського парламенту щодо визначення цивільно-правового регулювання використання роботів

Етичні принципи
для проектувальників, виробників і користувачів роботів.

Роботи – багатоцільові інструменти. Роботи не повинні розроблятися виключно або в першу чергу для знищення або нанесення шкоди людям, за винятком інтересів національної безпеки.

Люди, а не роботи, є суб'єктами, що несуть відповідальність. Роботи повинні бути спроектовані так, щоб, наскільки це практично можливо, забезпечити дотримання існуючих законів і основних прав і свобод людей, включаючи конфіденційність.

Роботи – це продукція (вироби). Вони повинні бути спроектовані і виготовлені таким чином, щоб забезпечити їх безпеку і захист.

Роботи – це предмет матеріального світу. Вони не повинні бути призначені для використання вразливості користувачів, викликати емоційний відгук або залежність, їх технічний характер повинен бути очевидний.

Робота завжди можна співвідносити з особою, яка несе юридичну відповідальність за нього.

Висновок:

Зміст вище наведених принципів свідчить про те, що їх автори не бачать можливості для роботів бути самостійним суб'єктів у відносинах з людьми.

Інтенсивна розробка та використання AI породила безліч складних етичних проблем, які переходять в конкретні юридичні проблеми.

Для юристів є багато роботи щодо вирішення правових проблем, до яких практично не залучали практиків і вчених.

Комітет з правових питань Глобальної ініціативи IEEE з етичних міркувань в області штучного інтелекту.

Юристи повинні бути частиною дискусії щодо регулювання, управління, внутрішнього і міжнародного законодавства в цих областях тому, що отримання величезної вигоди, яку потенційно несе людству і нашій планеті використання AI, має гарантуватися продуманою системою правового регулювання в майбутньому.

Необхідно забезпечити прогрес з одного з найважливіших питань:
- забезпечення високого рівня захисту даних,
- цифрових прав і етичних стандартів,
- використанні переваг і
- запобігання ризиків
- при розвитку AI та робототехніки.

Європейська комісія створили Експертну групи високого рівня з питань штучного інтелекту для збору експертних матеріалів і створення широкого союзу різних зацікавлених сторін.

Завдання – консультування Європейської комісії з вирішення середньострокових і довгострокових завдань і можливостей, пов'язаних з AI, шляхом надання рекомендацій, які будуть використовуватися в процесі розробки
- політики,
- процесу законодавчої оцінки та
- визначення цифрової стратегії наступного покоління.

Штучний інтелект **(AI)** – це технологія загального призначення, яка може поліпшити розвиток і добробут людей, щоб сприяти:
- позитивній стійкої глобальної економічної діяльності,
- збільшити інновації і продуктивність, а також
- допомогти відповісти на ключові глобальні проблеми.

AI також створює проблеми:
- для суспільств і економік,
- в частині економічних зсувів, нерівності та конкуренції,
- у перехідних процесах на ринку праці,
- для демократії і прав людини.

Довідково.

OECD – організація економічного співробітництва та розвитку (Organisation for Economic Co-operation and Development) – міжнародна економічна організація розвинених країн, що визнають принципи представницької демократії та вільної ринкової економіки. 1948 р. Париж.
На 1.05.2018–36 держав, 60% світового ВВП.

Система AI – це машинна (комп'ютерна – авт.) система, яка може, для заданого набору визначених людиною цілей, робити
- прогнози,
- рекомендації або
- рішення,

що впливають на реальні або віртуальні середовища.

Системи штучного інтелекту призначені для роботи з різними рівнями автономії.

Основна характеристика робота – «автономність»:
- здатності «думати» для себе і
- приймати власні рішення

для впливу на навколишнє середовище, без прямого зовнішнього контролю, що властиво роботам з AI (когнітивні роботи), які будуть навчатись з минулого досвіду та самі модифікувати свої алгоритми, тому їх поведінка не буде цілком передбачуваною, що, ймовірно, стане проблемою, яка заслуговує серйозної етичної уваги і роздумів.

Довідково.

Організація Об'єднаних Націй з питань освіти, науки і культури (ЮНЕСКО, United Nations Educational, Scientific and Cultural Organization, UNESCO) – спеціалізована установа в Організації Об'єднаних Націй (ООН), спрямовані на заохочення міжнародного миру і безпеки через міжнародну співпрацю в галузі освіти, наук та культури.

Має 193 держави-члени та 11 асоційованих членів, а також партнерів у неурядовому, міжурядовому та приватному секторах. Штаб-квартира у Парижі, Франція, ЮНЕСКО має 53 регіональні виїзні бюро та 199 національних комісій, що сприяють виконанню її глобального мандату.

ЮНЕСКО була заснована в 1945 році в якості наступника комітету Ліги Націй «Міжнародного комітету з інтелектуальної співпраці».

2. Теоретико-методологічні засади визначення правосуб'єктності роботів з штучним інтелектом

Визначення поняття інтелект» та «штучний інтелект»

До цих пір не сформульовано більш-менш узгодженої думки щодо філософського фундаментального поняття «інтелект».

Експерти і філософи уникають вирішення проблеми визначення загальноприйнятої дефініції терміну AI, незважаючи на те, що це має життєво важливе значення для регулювання та управління, тому що закони і політика просто не будуть працювати без нього.

Існує понад 200 визначень терміну «штучний інтелект»

Штучний інтелект – це наука і техніка створення інтелектуальних машин, особливо інтелектуальних комп'ютерних програм.
[Джон Маккарті (John McCarthy, 1956 р.]

Штучний інтелект оцінюється загальною здатністю агента досягати мети в широкому діапазоні середовищ.
[Ш. Легг і М. Хаттер]

Штучний інтелект – це розробка гнучкого агента, здатного адаптуватися до різних ситуацій, які раніше не були відомі і не вивчалися через досвід, та досягати мети, що недоступно для традиційних комп'ютерних систем.
[João Paulo A. Lenardon. The regulation of artificial intelligence. Tilburg University, 2017]

Перелік когнітивних функцій (далі - КФ) людини:

1. Відносно інформації (**даних**):
   - сприйняття,
   - запам'ятовування,
   - обмін,
   - аналіз,
   - зіставлення,
   - оцінювання,
   - узагальнення
   - використання.

2. Мовлення та розуміння мови.
   Складні:
   - визначення мети, планування, прийняття рішень;
   - вибору стратегії і конкретних дій, експертної оцінки ситуації;
   - перетворення тексту в мову і навпаки;
   - розпізнавання об'єктів і їх класифікації (гносиз);
   - планування та здійснення цілеспрямованої рухової діяльності (праксис);
   - самонавчання, самоорганізації, генерування нових знань;
   - тощо.

   Надто складні:
   - свідомість,
   - суб'єктивні переживання;почуття гідності, поваги, краси тощо;
   - емоції;
   - емпатія тощо.

Тест Тюрінга

Тест Тюрінга – тест, створений у 1950 р. задля визначення здатності ЕОМ проявляти інтелектуально обумовлену поведінку, що тотожна до поведінки людини і яку неможливо відрізнити від поведінки людини.

Ідею запропонував англійський вчений Алан Тюрінг у статті «Обчислювальні машини та розум» (1950 р.)

Зміст тесту

- Суддя взаємодіє з одним комп'ютером і однією людиною.
- Суддя одночасно задає питання комп'ютеру і людині.
- На підставі аналізу відповідей суддя має визначити чия відповідь: людини чи з комп'ютерної програми.
- Якщо суддя не може визначитись хто зі співрозмовників є людиною, то вважається, що комп'ютерна програма пройшла тест.

Умови проведення тесту

- Всі учасники тесту не бачать один одного.
- Бесіда ведеться в режимі «тільки текст», наприклад, за допомогою клавіатури і екрану (комп'ютера-посередника).
- Листування має проводитися через контрольовані проміжки часу, щоб суддя не міг робити висновки, виходячи зі швидкості відповідей.

Проходження тесту Тюрінга означає, що комп'ютерна програма проявляє: інтелектуально обумовлену поведінку, що тотожна до поведінки людини і яку неможливо відрізнити від поведінки людини.

Штучний інтелект – це те, що:

- копіює (моделює) роботу людського мозку (інтелекту, розумової діяльності тощо);
- має когнітивні функції еквівалентні (тотожні) за критеріями, характеристиками і показниками когнітивним функціям людини (фізичної особи).

Алгоритми створення AI нейронні мережі

- генетичні алгоритми,
- теоретичні проксі,
- експертні системи,
- байєсівські мережі,
- нечітка логіка,
- еволюційне програмування тощо.

Штучний інтелект (**ШІ**, **AI** (англ.)) – це певна сукупність комп'ютерних програмних та апаратних методів, способів, технологій і засобів, які реалізують одну, кілька, частину або всі когнітивні функції (КФ) шляхом еквівалентної імітації (моделювання) відповідних когнітивних функцій людини.

Штучний інтелект з повним набором КФ має змогу самостійно **(без участі людини)**

- визначати як стратегічну мету діяльності, так і ціль конкретних дій;
- аналізувати, прогнозувати, планувати, приймати і виконувати рішення;
- адаптувати власну поведінку при зміні зовнішніх та внутрішніх умов;
- навчатись, організовуватись, структурно перебудовуватись, розвиватись тощо;
- функціонувати в складних, багатовимірних процесах;
- добавляти, інтегрувати та вдосконалювати КФ в тій ступені, в якій це необхідно для виконання рішень.

Класифікація штучного інтелекту

- прикладний AI Імітація (моделювання, виконання) однієї або декількох когнітивних функцій людини

- загальний AI. Імітація (моделювання, виконання) безлічі когнітивних функцій людини, відповідних актуальному рівню розвитку науки і техніки

- супер AI Імітація (моделювання, виконання) безлічі когнітивних функцій людини, відповідних актуальному рівню розвитку науки і техніки, додаючи свідомість, суб'єктивні переживання, почуття гідності, поваги, краси тощо

Типи штучного інтелекту

Прикладний AI (**ПШІ**, **Applied Artificial Intelligence**, **AAI**) – це штучний інтелект, який реалізує

- одну або кілька когнітивних функцій людини,
- що використовуються при реалізації
- конкретної діяльності без участі людини
- для досягнення поставлених цілей, зміст яких, їх критерії та параметри
- заздалегідь задані людиною.

Загальний AI (**ЗШІ**, **Artificial General Intelligence**, **AGI**) – це штучний інтелект, який реалізує

- частину або повну сукупність когнітивних функцій людини,
- що використовуються при реалізації
- будь-якої діяльності без участі людини
- для досягнення цілей
- критерії та параметри яких або заздалегідь задаються, або визначаються самостійно.

Супер AI (**СШІ**, **Artificial Superintelligence**, **ASI)** – це штучний інтелект, який реалізує

- повну множину когнітивних функцій людини, додаючи свідомість, суб'єктивні переживання, почуття гідності, поваги, краси тощо, які значно перевищують людські інтелектуальні показники,
- що дозволяє здійснювати
- будь-яку діяльність без участі людини
- для досягнення цілей
- самостійно визначених відповідно до самостійно встановлених критеріїв та параметрів.

Проблема:

AI, як сукупність комп'ютерних програм, не може самостійно імітувати (моделювати) когнітивну функцію людини, яка полягає в плануванні та здійсненні цілеспрямованої рухової діяльності (праксис).

Вирішення проблеми:

відтворення (імітація) когнітивної функції праксис за допомогою спеціальних виконавчих механізмів, таких як:

- маніпулятори, які оснащені всіляким інструментом;
- механічні «руки» і «ноги»;
- пристрої, що виконують функції просторового переміщення і пересування;
- тактильні, слухові і оптичні сенсори тощо.

3. Проблеми правового регулювання надання послуг роботами зі штучним інтелектом

Робоче визначення терміну:
«робот» – це інтеграція ШІ з деякою технічною системою, що створює можливості для об'єктивізації в реальному світі результатів реалізації штучним інтелектом певних когнітивних функцій.

Ми повинні з'ясувати, як найкращим чином інтегрувати роботів в соціальні, правові та культурні рамки нашого суспільства, як врахувати інтереси людей з різних культурних традицій, які не будуть дивитися на нашу роботу з широким діапазоном припущень, міфів і оповідань, що стоять за ними.
[Світові експерти з технологій, промисловості, мистецтва, права та соціальних наук, 2010 р.]

В умовах настання нової епохи в розвитку людства, коли все більш складні роботи, боти, андроїди та інші прояви штучного інтелекту, схоже, стануть каталізаторами нової індустріальної революції, яка, ймовірно, не залишить без уваги жодного прошарку суспільства, для законодавчої влади життєве важливим є вираховування юридичних та етичних наслідків.

Європарламент пропонує:

- розглянути наслідки правового рішення щодо створення в довгостроковій перспективі особливого юридичного статусу для роботів, наприклад, для найскладніших автономних роботів (роботів з супер AI – авт.).

- визначити цей статус як статус електронних осіб, відповідальних за нанесення будь-якого збитку, який вони можуть заподіяти, та, можливо, застосування статусу електронної особи у випадках, коли роботи будуть приймати автономні рішення або іншим чином взаємодіяти з третіми особами самостійно.

Класифікація та визначення

Робот = штучний інтелект + технічна система

1 гіпотеза
Роботи, зокрема, з штучним інтелектом:
- лише допомагають здійснювати звичайні суспільні відносини;
- суб'єкти – традиційні юридичні і фізичні особи;
- можна і без роботів, хоча менш ефективно.

Висновок.
Роботи не можуть виступати стороною суспільних відносин

2 гіпотеза
Роботи-андроїди або андроїди:
- самостійно оцінюють свої дії та дії інших суб'єктів;
- самостійно формують або змінюють мету та зміст своїх дій;
- враховують вплив непередбачуваних мінливих обставин;
- підпадають під вплив своїх емоцій та свідомості.

Висновки:
- роботи – людиноподібні суб'єкти з еквівалентними КФ;
- роботи здійснюють людиноподібні дії;
- роботи можуть виступати стороною суспільних відносин;
- роботи можуть виступати суб'єктом правовідносин

Роботи

простий робот (**simple robot**) – інтеграція прикладного AI та технічної системи, що дозволяє реалізовувати одну або кілька когнітивних функцій людини в процесі здійснення конкретного виду діяльності, пов'язаної, як правило, з однорідними об'єктами, що мають матеріальне або нематеріальне вираження.

робот-андроїд (**robot android**) – інтеграція загального AI та технічної системи, що дозволяє реалізовувати безліч когнітивних функцій в процесі здійснення будь-якого виду діяльності без участі людини, пов'язаної з різноманітними об'єктами, що мають матеріальне або нематеріальне вираження.

андроїд (**android**) – інтеграція супер ШІ та технічної системи, що дозволяє реалізувати повну безліч когнітивних функцій без участі людини в процесі здійснення будь-якої раніше відомої або невідомої діяльності, пов'язаної з різними відомими або раніше невідомими об'єктами, що мають матеріальне або нематеріальне вираження.

Важливе зауваження

Певний вид діяльності – конкретний набір КФ:
- фізична особа набуває потрібні якості конкретного набору КФ;
- AI програмується на наявність конкретного набору КФ.

Гіпотеза

Якщо робот з ШІ має КФ еквівалентні КФ фізичної особи, то робот з ШІ є правовим еквівалентом фізичної особи.
- правоздатність – це визнана державою загальна для будь-якого суб'єкта права потенційна можливість мати юридичні права і обов'язки;
- дієздатність – реальна персоніфікована для кожного суб'єкта права здатність своїми самостійними, усвідомленими діями отримувати для себе юридичні права і обов'язки, здійснювати їх та виконувати;
- деліктоздатність – це здатність кожного суб'єкта права нести персональну юридичну відповідальність за скоєне ним правопорушення (делікт).

Судово-психіатрична експертиза

- проводяться дослідження КФ фізичної особи;
- дослідження ґрунтуються на комплексному застосуванні психопатологічних, патопсихологічних, нейропсихологічних і інструментальних методів;

- оцінка КФ – це визначення наявності когнітивних порушень, їх тяжкості, якісних характеристик, гостроти розвитку, динаміки їх частоти і впливу на здатність суб'єкта до довільної регуляції своєї поведінки.

Діагностичні стандарти Міжнародної класифікації психічних розладів ч. 1 ст. 7 Закону України «Про психіатричну допомогу»

Висновки судово-психіатричної експертизи

Фізична особа не здатна свідомо і самостійно приймати і реалізовувати рішення, які є адекватними ситуації, усвідомлювати свої дії та керувати ними, оскільки встановлено факт наявності у неї когнітивних порушень, тобто встановлено факт наявності критичного зниження характеристик і показників когнітивних функцій.

Проблеми судово-психіатричної експертизи
(за наслідками наукової дискусії психіатричної спільноти)

Методи і методики повинні містити:
- порушення для кожної конкретної КФ повинні мати ознаки, критерії, характеристики, показники;
- опис алгоритму визначення інтегральних оцінок за певними критеріями стану показників для досліджуваної сукупності когнітивних функцій, які були б релевантними правовому поняттю «обмежена дієздатність» з урахуванням відповідності юридичному і психологічному критеріям.

Висновок
Дієздатність фізичної особи залежить від характеристик і показників когнітивних функцій.

Особливості правосуб'єктності

Твердження 1.

Правосуб'єктність фізичної особи (правоздатність, дієздатність і деліктоздатність) презюмується, не обмежена та не вимагає доказів. Виключення за законом.

Твердження 2.

Правосуб'єктність робота з ШІ (правоздатність, дієздатність і деліктоздатність) потребує доведення як правового еквівалента фізичної особи.

План досліджень щодо визначення дієздатності робота з AI як правового еквівалента фізичної особи

Формування теоретико-методологічних положень проведення експертиз для:

1. окремих КФ людини, які реалізуються в роботах з AI;
2. окремих видів і типів КФ людини, які реалізуються в роботах з AI;
3. конкретної діяльності, яка реалізуються за допомогою робота з AI з відповідним набором КФ;
4. конкретних видів і типів діяльності, які реалізуються за допомогою робота з AI з відповідним набором КФ;
5. робота з супер AI, який здатний реалізувати будь-яку наперед невідому діяльність.

Запропонований підхід базується на наступних принципах

1. Принцип правової еквівалентності фізичної особи (правові інститути: представництва, повіреного, управителя тощо).

2. Принцип презумпції правоздатності та дієздатності повнолітньої фізичної особи.

3. Принцип доведення необхідності обмеження дієздатності повнолітньої фізичної особи.

4. Принцип формування вичерпних вимог щодо спеціальної та галузевої правоздатності та дієздатності.

5. Принцип еквівалентності когнітивних функцій фізичної особи і штучного інтелекту.

6. Принцип визнання робота з ШІ як правового еквівалента фізичної особи.

7. Принцип доказового визнання дієздатності робота з ШІ. Проблема створення системи правового забезпечення застосування роботів з AI – це проблема здійснення ідентифікації правосуб'єктності роботів з AI в процесі самостійного надання послуг і проведення робіт в інтересах юридичних і фізичних осіб.

Фактично, це проблема визначення можливості роботів з AI бути суб'єктом правовідносин в рамках традиційної системи права.

Загальний висновок

Визнання обґрунтованості справедливості запропонованої викладеної гіпотези дозволить вирішити правові проблеми, пов'язані з роботами з AI:

- в рамках традиційної системи права,
- з використанням всього багатовікового досвіду її функціонування,
- шляхом формування теоретико-методологічних основ та розроблення практичних рекомендацій зі створення відповідної системи правового забезпечення.

Перелік контрольних питань:

- У чому полягає відмінність між загальним, прикладним та супер штучним інтелектом?
- Які є принципи розробки роботів? Чи існує нормативний документ, який встановлює ці принципи?
- Які положення розкриті в стратегії «Штучний інтелект для Європи»?
- Як співвідносяться поняття інтелект та штучний інтелект?
- Чому ступінь автономії штучного інтелекту пов'язана із можливістю відтворювати когнітивні функції людини?
- Чим займається Експертна група високого рівня з питань штучного інтелекту?

Тест https://forms.gle/WxjRgHKhMp1bbsqB

9. Розумні контракти та інші застосування технологій блокчейн

1. Базова місія технології блокчейн в сучасному цифровому світі
2. Використання блокчейн-технологій юридичними особами
3. Правові проблеми застосування блокчейн-технологій в різних сферах суспільних відносин

1. Базова місія технології блокчейн у сучасному цифровому світі

Технології блокчейн усувають необхідність в звичних економічних, правових і політичних інститутах, які в економіці виконують роль посередників довіри, замінюючи довіру доказами (Р. Меллон).

Блокчейн – нова технологія, яка усуває необхідність третіх осіб для забезпечення довіри до фінансових, договірних та виборних дій (Світовий економічний форум в Давосі, 2015 р.).

Блокчейн – це послідовна база даних інформації, яка захищена методами криптографічного доказу і пропонує альтернативу класичним фінансовим книгам (David Yermack, 2017 р.)

Блокчейн – публічна база всіх здійснених транзакцій різного типу в рамках єдиної системи, які шикуються певним чином і з них формується ланцюжок блоків.

Блокчейн – це мережа, що складається з елементів (комп'ютери/ суб'єкти), які називаються вузлом, кожен з яких містить (зберігає) інформацію у формі ланцюжка блоків (книги).

Новий блок одним з вузлів в мережі поміщається в оновлену версію книги (реєстру, бази даних), в якій містяться всі попередні блоки.

Потім цей новий блок передається до всіх інших вузлів мережі технології блокчейну для оновлення версій їх книг (реєстрів, баз даних).

Всі блоки блокчейну пов'язані один з одним криптографічним методом таким чином, що внести зміни окремо в будь-який з них неможливо.

Кожен блок містить повний набір транзакцій, здійснених з моменту закінчення формування попереднього блоку мережі до моменту складання останнього блоку, розмір якого збільшується пропорційна збільшенню кількості попередніх транзакцій.

Повідомлення про транзакції включає відомості про публічну адресу одержувача, вартість транзакції та криптографічний цифровий підпис, наявність якого доводить достовірність транзакції.

Для перевірки цілісності та достовірності інформації, що передається та зберігається, застосовується криптографічне перетворення для вирахування хэш-функції.

Криптографічне перетворення за одним алгоритмом одного и того повідомлення різними учасниками блокчейн об'єднання призводить до однакового результату.

Для будь-якого обсягу інформації, будь-то одна буква або весь текст Т. Шевченка «Кобзар», існує унікальний і неповторний хеш – короткий символьний рядок.

Причому, якщо в тому ж «Кобзарі» змінити хоча б один символ, додати один лише знак,– хеш зміниться кардинально.

Наприклад, це буде:
ef3c82303f3896044125616982c715e77574
cd1f84c34c6b2e64167d2fde766

Якщо додати лише знак оклику в кінці тексту, то буде
a6123e137d1d7f0aad800cdbc0918a65bb
7a 778a607cb993043d99718ec5a9e1

Технології блокчейн мають наступні основні властивості в рамках певної мережі блокчейн, що об'єднує деяку обмежену сукупність суб'єктів:

- можливість зберігання інформації щодо кожної транзакції суб'єкта у вигляді незалежних записів;
- можливість зберігати для кожної транзакції різноманітну інформацію, наприклад, про права власності, звіти по кредитуванню, якість товарів і так далі;
- реєстр транзакцій не зберігається в певному місці, а розподіляється на всі комп'ютери (суб'єктів-членів РСД) по всьому світу;
- наявність вільного доступу у суб'єктів до всього реєстру (книги) транзакцій.

На думку експертів,
блокчейн буде застосовуватися в самих різних областях, такі як:

- грошові перекази,
- мікроплатежі,
- розумні контракти (або смарт-контракти),
- ідентифікація фізичних об'єктів і активів,
- державне управління,
- оборона і безпека,
- міжнародна діяльність тощо.

В цілому, передбачається, що в майбутньому технології блокчейн можуть стати драйвером радикальних змін в широкому спектрі галузей, бізнес-моделей, соціальних і операційних процесів.

До тестування та впровадження технологій блокчейн приступили в ряді країн і багато великих корпорацій.

2. Використання блокчейн-технологій юридичними особами

Проблеми сучасної економіки

- глобалізація економічних, виробничих, інформаційних, фінансових та інших відносин;
- зростання міжнародної конкуренції, тобто конкуренції на національних локальних ринках окремих країн гравців локальних ринків з інших країн світу;
- залежність бізнесу від невизначеності і волатильності попиту на продукцію або послуги;
- важливість знань про особливості конкретних юрисдикцій не тільки в цілому інших держав, але, навіть, їх окремих регіонів;
- прискорення темпів протікання і розвитку всіх процесів в соціумі, і, перш за все, в економіці;
- необхідність різкого збільшення швидкості та підвищення якості реакції на виклики.

Проблема довіри

Проблема довіри загострюється на першому етапі «глобалізації» суспільних відносин тоді, коли в якості еквівалента товару стали масово використовуватися національні «гроші», специфічні для кожного державного (квазідержавного) утворення.

Наявність різних еквівалентів створювало ризики шахрайства при здійсненні транзакцій, що зажадало формування довірчих механізмів обміну цими еквівалентами.

Функцію забезпечення довіри при обміні еквівалентів стали виконувати треті особи – посередники при обміні національних «валют» – міняйли, які обслуговували будь-якого учасника ринку.

Природно, за свою послугу міняйли стягували певну плату, що і становило частину транзакційних витрат, обумовлених наявністю ієрархічного зв'язку між покупцями (продавцями) і такою інституцією як міняйли.

Це був локальний в просторі обмін: «товар» – «гроші»«товар».

Світова реакція щодо необхідності зміцнення довіри

1. Прогрес, досягнутий в здійсненні рішень та подальшої діяльності за підсумками Всесвітньої зустрічі на вищому рівні з питань інформаційного суспільства на регіональному та міжнародному рівнях. (доповідь Генерального секретаря ООН, 2017 р.);

2. «Економіка побудови довіри в Інтернеті: запобігання спотворенню даних». (глобальний звіт ISOC, 2016 р.);

3. Політична основа для відкритого і надійного Інтернету. Підхід для зміцнення довіри у відкритому середовищі. (звіт ISOC, 2016 р.).

ISOC – Товариство Internet (некомерційне професійне об'єднання, що забезпечує технічний розвиток глобальної мережі і залучення нових користувачів в наукових, промислових і громадських колах шляхом випуску регулярних інформаційних бюлетенів та організації форумів, 1992 р.)

ЄС вважає, що технологія блокчейн при правильному використанні може забезпечити значні переваги європейській промисловості, європейській економіці та європейському суспільству в цілому.

Єврокомісія буде підтримувати розвиток блокчейн технологій політично, законодавчо та регуляторно.

Технологія блокчейн дозволяє людям та організаціям, які можуть не знати або довіряти одне одному, колективно домовлятися та постійно записувати інформацію без посередництва уповноваженого органу.

Створюючи довіру до даних способами, які раніше були неможливими, блокчейн може змінити спосіб обміну інформацією та здійснення транзакцій в Інтернеті.

Законодавчого визначення терміну «блокчейн» в ЄС поки що немає. Але проміжне розуміння подається.

Блокчейн це:

- це послідовність блоків, що містять дані, записи, що зберігаються у формі блоків.

- своєрідна база даних, яка спільно використовується мережею комп'ютерів, де записи постійно додаються як «блоки», і цей «ланцюг» не можна будь-яким чином порушити чи змінити.

- це постійний перевірений запис.

Декларацію Про співпрацю в рамках Європейського блокчейн-партнерства з 10.04.2018 р. до 16.10.2019 р. підписали всі держави-члени ЄС.
Підписанти Декларації вважають:

- блокчейн – це технологія сприяння довірі користувачів, яка дозволяє обмінюватися он-лайн інформацією, узгоджувати та реєструвати транзакції перевірним, безпечним та постійним способом.
- технологія блокчейн вже успішно апробована, переважно у фінансових послугах, і стане більш оперативною та інтегрованою у зростаючу кількість цифрових послуг, таких як регулятивна звітність, енергетика та логістика в найближчі роки.

Мета співпраці:

- реалізація потенціалу послуг на базі блокчейна на користь громадян, суспільства та економіки;
- розбудова Європейської інфраструктури блокчейн-сервісів (EBSI)
- надання транскордонних публічних послуг по всій території ЄС за допомогою технології blockchain.

Європейська інфраструктура блокчейн-сервісів

З 2021 року розробка та впровадження Європейська інфраструктура послуг блокчейн (European Blockchain Services Infrastructure, EBSI) фінансуватиметься на рівні ЄС у рамках Програми цифрової Європи.

EBSI складається з однорангової мережі взаємопов'язаних вузлів, що працюють на інфраструктурі служб на основі блокчейну.

Кожен член Європейського блокчейн-партнерства (EBP) – 27 держав-членів ЄС, Норвегія, Ліхтенштейн та Європейська комісія – буде мати принаймні один вузол.

Це дозволить державним (а зрештою і приватним) організаціям розробляти додатки, які підключаються до інфраструктури EBSI та використовують її.

Плани на початковий набір випадків використання EBSI

- нотаріальне діяльність: для створення надійних цифрових аудиторських записів, автоматизації перевірок відповідності процесів, що залежать від часу, і доведення цілісності даних;

- дипломи: повернення громадянами контролю при управлінні їхніми освітніми показниками; істотне зменшення витрат на перевірку та підвищення довіри до справжності;

- європейська самосуверенна ідентичність: впровадження загальної можливості самосуверенної ідентичності, що дозволяє користувачам створювати та контролювати власну ідентичність через кордони, не покладаючись на централізовані органи влади, та забезпечуючи відповідність нормативній базі eIDAS.

- довірений обмін даними: для безпечного обміну даними між органами влади в ЄС, починаючи з ідентифікаційних номерів ПДВ IOSS щодо ПДВ та імпортуючи єдине вікно для митних та податкових органів.

Крім того, буде друга черга: 1) фінансування МСП; 2) використання європейського номера соціального страхування для полегшення транскордонного доступу до соціальних служб; 3) сприяння управлінню транскордонними процесами запиту на притулок.

Нормативно-правова база для блокчейну

Цифровий Євро

Європейська комісія та Європейський центральний банк (ЄЦБ) продовжують свою діяльність щодо забезпечення потужного та енергійного європейського сектору цифрових фінансів та добре інтегрований платіжний сектор, який відповідає новим платіжним потребам у Європі.

Беручи до уваги цифровізацію, швидкі зміни в платіжному середовищі та появу крипто-активів ЄЦБ вивчає можливість випуску цифрових євро, як доповнення до рішень щодо готівки та платежів, що надаються приватним сектором.

Після завершення публічних консультацій 12 січня 2021 р. та періоду підготовчої роботи ЄЦБ розгляне питання, чи розпочинати цифровий євро-проект до середини 2021 року.

Такий проект відповів би на ключові дизайнерські та технічні питання та забезпечити ЄЦБ необхідними інструментами, щоб бути готовим випустити цифровий євро, якщо таке рішення приймається.

Служби ЄЦБ та Європейської комісії є спільними при розгляді на технічному рівні широкого кола політичних, правових та технічних питань, які випливають з можливого введення цифрового євро з урахуванням їх відповідних мандатів та незалежність, передбачені Договорами.

Закон ЄС про крипто-активи

Директива 2014/65 / ЄС Європейського Парламенту та Ради від 15 травня 2014 року про ринки фінансових передувала появі крипто-активів та DLT. Це може перешкодити інноваціям.

Єврокомісія 24.09.2020 р. запропонувала пілотний режим для ринкової інфраструктури, яка бажає спробувати торгувати та здійснювати розрахунки з фінансовими інструментами у формі крипто-активів. Режим PILOT допускає звільнення від існуючих правил і дозволяє регуляторам та компаніям тестувати інноваційні рішення, використовуючи блокчейни.

Для криптовалюти, яка не кваліфікується як «фінансові інструменти», такі як комунальні токени або платіжні токени, запропоновано конкретну нову систему, яка замінить усі інші правила ЄС та національні правила, що регулюють випуск, торгівлю та зберігання таких крипто-активів.

Такий ринок регулювання криптоактивів підтримуватиме інновації, одно- часно захищаючи споживачів та цілісність бірж криптовалют

Загальноєвропейська регуляторна пісочниця для блокчейну

Пісочниця – це об'єднання, яке об'єднує регуляторів, компанії та технічних експертів для тестування інноваційних рішень та виявлення перешкод, що виникають при їх застосуванні.

Європейське блокчейн-партнерство планує створити загальноєвропейську регуляторну пісочницю у співпраці з Європейською комісією для випадків використання в Європейській інфраструктурі блокчейн-сервісів (European Blockchain Services Infrastructure, EBSI), і поза EBSI, включаючи портативність даних, простір даних B2B, смартконтракти та цифрову ідентичність (Self Suvereign Identity) у галузі охорони здоров'я, навколишнього середовища, мобільності, енергетики та інших ключових галузях.

Стандарти блокчейну

Стандарти – важливий ключ до успіху будь-якої технології, що зароджується, зокрема, технологій блокчейн.

Правильні стандарти мають забезпечити взаємодію, створити довіру та допомогти забезпечити простоту використання технології, а отже, підтримати її розвиток та шлях до масового впровадження.

Європейські організації зі стандартизації (European Standardisation Organisations): до основних організацій, що стосуються блокчейну, належать Європейський інститут телекомунікаційних стандартів (**ETSI**),

Європейський комітет зі стандартизації (**CEN**), Європейський комітет з електротехнічної стандартизації (**CENELEC**);

Наднаціональні та галузеві організації: до основних глобальних організацій, що мають відношення до стандартів блокчейну, належать Міжнародна організація зі стандартизації (International Organization for Standardization, ISO) та Міжнародний телекомунікаційний союз (International Telecommunication Union, ITU).

Національні органи зі стандартів: більшість національних органів, що займаються стандартами інформаційних технологій (IT), також працюють або, як очікується, будуть працювати над темами блокчейн.

Органи відкритих стандартів: включають Інститут інженерів з електротехніки та електроніки (Institute of Electrical and Electronics Engineers, IEEE), Організацію вдосконалення структурованих інформаційних стандартів (OASIS) та Робочу групу з питань Інтернет-інженерії (IETF).

INATBA: Міжнародна асоціація довірених блокчейн-додатків також сприяє обговоренню стандартів на європейському та глобальному рівнях.

Застосування стандартів технологій блокчейну спрямовано на забезпечення наступного.

- Взаємодія: забезпечення можливості безперешкодного обміну даними за умови використання різних протоколів і платформ блокчейну та DLT.
- Управління: найкраща практика та стандарти управління блокчейновими проектами, а також створення консорціумів блокчейнів, що працюють на децентралізованих платформах.
- Ідентифікація: просування спільної системи ідентифікації та / або сумісної ідентичності серед різних блокчейнових протоколів та платформ.
- Безпека: Забезпечення безпечної роботи різних вузлів, мереж та служб Розумні контракти: Підтримка найкращих практик та стандартів для забезпечення надійної та безпечної технології смарт-контрактів.

Обсерваторія та форум ЄС з блокчейну

У лютому 2018 р. Європейська комісія у співпраці з Європейським парламентом запустила Observatory & Forum Blockchain.

Ця ініціатива патронується Генеральним директоратом комунікаційних мереж, контенту та технологій Європейської Комісії (DG CONNECT).

Інформація та погляди, які викладені на цій платформі належать авторам і не відображають офіційного погляду Комісії.

Комісія не гарантує точність даних, що містяться в цій платформі.

Ні Комісія, ні будь-яка особа, яка діє від імені Комісії, не можуть нести відповідальності за використання інформації, що може міститись у цій платформі.

Напрями активності Observatory & Forum Blockchain

- розбудова Карти основних існуючих ініціатив у Європі та за її межами;
- моніторинг розробок, аналіз тенденцій та розв'язання проблем;
- формування центру знань на blockchain;
- сприяння європейським акторам та зміцнення європейської взаємодії з кількома зацікавленими сторонами;
- платформа для Європи з комунікацій щодо обговорення проблем blockchain;
- призив до спільних дій, заснованих на конкретних випадках використання blockchain, що мають європейський інтерес.

Загальний висновок щодо політики ЄС з розвитку технологій блокчейну.

В цілому на рівні вищих інституцій Євросоюзу є розуміння важливих перспектив широкого застосування блокчейн технологій.

Одночасно, адекватно оцінені виклики, які можуть мати місце при використанні децентралізованих технологій.

Єврокомісія вживає енергійних заходів щодо всебічного та комплексного опрацювання проблеми застосування блокчейн технологій в Євросоюзі.

3. Правові проблеми застосування блокчейн-технологій в різних сферах суспільних відносин

Правове забезпечення широкого застосування технологій блокчейн потребує вирішення певної низки проблем, зокрема, в рамках інформаційного права:

- Систему правового регулювання застосування технологій блокчейн доцільно розробляти в парадигмі максимальної інтеграції в традиційну національну правову систему.

- Для низки публічних додатків технологій блокчейн задля зниження ризиків необхідно визначення правового режиму мережі блокчейн, її реєстру і записів транзакцій, формування правових вимог до їх форми і змісту.

- Визначення юрисдикції дій з реєстром мережі блокчейн, в тому числі, при наявності транскордонних транзакцій.

- Дослідження особливостей правовідносин, пов'язаних з технологіями блокчейн, юридичних прав, обов'язків і відповідальності сторін.

- Дослідження проблеми визначення юридичних ризиків та обмежень використання технологій блокчейн в різних сферах застосування.

- Формування правових механізмів нагляду, встановлення відповідальності за порушення прав суб'єктів мережі блокчейн і відшкодування завданих збитків або при наявності помилок в комп'ютерній програмі.

- Вирішення правовими засобами проблеми наявності неповної спостережливості з боку суб'єктів мережі блокчейн всіх прихованих дій програмного забезпечення, що реалізує ту чи іншу функцію технології блокчейн, що може привести до небажаного збитку.

- Розробка правових механізмів верифікації суб'єктів мережі блокчейн (в разі необхідності), які здійснюють транзакцію, на момент її здійснення.

- Вирішення протиріччя між законодавчими вимогами обмеження доступу до персональних даних та іншої чутливої інформації суб'єктів мережі блокчейн, яка може міститися в реєстрі цієї мережі, і відкритістю інформації для всіх суб'єктів по всіх транзакціях та їх зберіганням в кожному вузлі мережі блокчейн.

- Установити правову регламентацію забезпечення, перевірки і сертифікації (при необхідності) кібербезпеки як програмного забезпечення, що підтримує функціонування мережі блокчейн, так і програмно-апаратних платформ, на яких розміщується це програмне забезпечення.

- Розробка пропозицій щодо процесуальних особливостей розгляду у суді суперечок, пов'язаних з мережами блокчейн.

Технології блокчейн створюють потенційну можливість за участю або без участі людини дистанційно укладати і виконувати договори на основі використання інформаційно-комунікаційних технологій.

Така реалізація технології блокчейн отримала назву розумні контракти (РК).

М. Сабо (1997 р.):
- розумні контракти відповідно до договірного права, мають величезні перспективи;
- використання ШІ (штучного інтелекту) значно посилить можливості РК;
- проблема практично на досліджена.

Приклад реалізації розумних контрактів

Мережа біткойну як всесвітня пірінгова криптовалютна цифрова платіжна система, яка використовує однойменну розрахункову одиницю і однойменний протокол передачі даних.

Уявлення про РК – два основних підходи:

- розумні контракти – це коли суспільні відносини регулюються програмним забезпеченням (комп'ютерним кодом);

- розумні контракти – це коли при реалізації суспільних відносин використовується програмне забезпечення у відповідності до певних домовленостей або положень закону.

Комп'ютерний код – новий Закон.

1. Алгоритми створюються людьми, які відображають в них своє розуміння порядку або правил реалізації певних дій, але розуміння, яке детермінується відомими закономірностями економіки, соціології, математики, фізики, механіки, металообробки, електроніки, робототехніки тощо.

2. Люди (програмісти) створюючи програмне забезпечення, керуються певними алгоритмами реалізації якихось дій (обчислень, обробки даних, функціонування технічних виробів, поведінки людей тощо).

3. Для випадку суспільних відносин – це алгоритми соціальних регуляторів, насамперед, правові норми.

Висновок.

Оскільки програмні засоби для РК створюються людьми або під керівництвом людей, то підхід, який базується на твердженні – «суспільні відносини регулюються програмним забезпеченням», принципово спотворює сприйняття ролі та місця комп'ютерних кодів в суспільних відносинах.

Розумний контракт – це набір обіцянок, зазначених в цифровій формі, включаючи протоколи, в якій сторони виконують ці обіцянки»

(Історично перше визначення – Н. Сабо)

Аналіз дефініцій визначень РК

Розумний контракт – це:
- набір обіцянок, зазначених в цифровій формі;
- набір правил;
- договір, який існує в формі програмного коду, що імплементовано на платформі блокчейн;
- договір, який самостійно виконується у разі настання заздалегідь визначених в ньому обставин;
- набір комп'ютерного коду, який використовується для формулювання, перевірки і виконання договору;
- програмні коди, в які вбудовуються умови контракту і які працюють в мережі і є еквівалентною заміною контракту, що «виконується» комп'ютером;
- угоди, що виконуються автоматизовано за допомогою комп'ютерних програм, реалізація яких відбувається без людського впливу.

Дефініція в інтересах правових досліджень.

Розумні контракти – інноваційна форма контрактів, укладення, виконання та припинення яких відбувається за участю або без участі людини, але з використанням мережевих комп'ютерних програмних та/або програмно-апаратних засобів, що мають взаємозв'язок з фізичними або цифровими об'єктами за допомогою оракулів.

Відмінною рисою цього визначення є те, що:
- розумний контракт – еквівалент традиційного контракту, який за допомогою ІКТ може укладатися, виконуватися і припинятися за участю або без участі людини;
- участь людини може проявлятися навіть в простому ініціюванні виконання розумного контракту;
- інваріантне до типу використовуваних технологій і до типу використовуваних мов програмування.

Дефініція в інтересах правових досліджень.

Оракул – це інтерфейс для забезпечення інформаційного обміну (обміну даними) між розумним контрактом (програмним забезпеченням РК) та зовнішніми джерелами / отримувачами інформації.

Оракул може бути виконаний як:
- програмне рішення;
- апаратне рішення.

Основні вимоги до оракулів:
- достовірність
- повнота
- інформації, що надається

Переваги РК
1. Висока швидкість – використання смарт-контрактів, дозволяє значно прискорити бізнепроцеси.
2. Ефективність – для повторюваних, однотипних контрактів.
3. Достовірність – принцип побудови блокчейн-ланцюжків виключає внесення змін до його тексту змін, не санкціонованих усіма сторонами контракту.
4. Спостережність – прозорість і простота звітності про вчинені транзакції.
5. Економічність – зменшення транзакційних витрат завдяки виключенню посередників, зменшення витрат людської праці.
6. Надійність – мінімізація ризику виникнення механічної помилки в процесі виконання контракту, можливість відновлення даних у разі їх втрати, висока стійкість проти кіберзагроз.
7. Універсальність – можливість застосування в найрізноманітніших сегментах людської діяльності.

Деякі дослідники в результаті юридичного аналізу доходять такого висновку:
В реальному житті складно розглядати інтелектуальний контракт як розумний, так і як контракт тому, що в даний час це просто автоматизований комп'ютерний код.

Проблема визначення правових механізмів для розумних контрактів:

- визнання «тексту» договору, викладеного в комп'ютерному коді, еквівалентним письмовій формі;

- визнання систем верифікації сторони контракту, які використовуються в мережевих комп'ютерних програмних та/або програмно-апаратних засобах, еквівалентними законодавчо схваленим системам ідентифікації суб'єктів за допомогою електронного або електронно-цифрового підпису;

- визначення місця укладення контракту з урахуванням можливої різної національної юрисдикції і мобільності сторін договору, наприклад, якщо сторона договору перебуває на борту літака, що летить;

- нотаріального посвідчення та державної реєстрації розумних контрактів.

Чотири функціональних властивості звичайних контрактів

1. Спостережність – здатність сторін спостерігати за виконанням контракту іншою стороною.

2. Верифікованість – здатність сторін контракту довести арбітру, що контракт був виконаний або порушений, або здатність арбітра визначити це іншими способами.

Спостережність та верифікованість – важливо для своєчасної індикації навмисних чи ненавмисних порушень.

3. Секретність (privity) – принцип, згідно з яким знання та контроль за змістом і виконанням контракту повинні розподілятися між сторонами лише в тому обсязі, наскільки це необхідно для виконання цього контракту.

4. Здатність до виконання – реалістичність виконання контракту, що мінімізує необхідність в додаткових заходах для забезпечення виконання контракту.

Бар'єри впровадження розумних контрактів

Контракти, що викладені природньою мовою, завдяки багатій семантиці дозволяють моделювати життєві ситуації з досить високим ступенем абстракції.

Високий ступінь абстракції – недолік, а не перевага, оскільки є причиною виникнення невизначеності при виконанні контрактів, що призводить до виникнення суперечок.

Абстракція закладається, наприклад, завдяки застосуванню таких висловів:
- «відповідають прийнятим стандартам»,
- «відповідно до прийнятих правил»,
- «сумлінна практика»,
- «розумний строк» тощо.

Висновок.

Необхідно створення систем автоматизації програмування розумних контрактів, зрозумілих для використання юристами без наявності спеціальної освіти в програмуванні.

Для цього необхідно провести дослідження з розробки:
- предметно-орієнтованих на юридичну сферу надвисокорівневих мов програмування з високим рівнем абстракції;
- засобів програмування природньою мовою з використанням штучного інтелекту.
- Необхідність зміни умов розумного контракту або його скасування.

Причини необхідності змін можуть бути різними: від зміни умов до змін законодавства.

В умовах використання блокчейн технологій існує проблема, яка пов'язана з неможливістю зміни інформації що була раніше записана у блокчейн.

А загальні комп'ютерні програми потребують значної переробки.

Доцільна розробка алгоритмів, досить гнучких до зміни умов, але це вимагатиме при реалізації застосування інноваційних підходів.

Розгляд спору в суді, як і в багатьох інших випадках, потребує наявність тексту РК, викладеного природньою юридичною мовою.

Таким чином, необхідна правова регламентація трансляції (перекладу) комп'ютерної програми, що містить опис розумного контракту, природньою юридичною мовою.

Висновок.

Правові механізми регулювання такої трансляції можуть бути аналогічні існуючим правовим механізмам здійснення перекладу з іноземних мов.

Діяльність, пов'язана з розумними контрактами, завжди буде пов'язана з вирішенням проблем:
- інтерпретації в лексиці програм, «зрозумілих» обчислювальним машинам, положень правового регулювання;
- відповідності алгоритмів програмного забезпечення алгоритмам правового регулювання.

Завдання, що стоять перед правою наукою і практикою

1. Інтеграція системи правового регулювання застосування розумних контрактів, що буде розроблятись, в традиційну національну правову систему.

2. Визначення юридичного статусу розумного контракту, формування правових вимог до його форми і змісту.

3. Визначення юрисдикції розумних контрактів, в тому числі, за наявності транскордонних транзакцій.

4. Дослідження особливостей правовідносин, пов'язаних з розумними контрактами, юридичних прав, обов'язків і відповідальності його сторін.

5. Дослідження проблеми визначення юридичних ризиків та обмежень використання розумних контрактів в різних сферах застосування.

6. Формування правових механізмів нагляду, встановлення відповідальності за порушення умов розумного контракту

і відшкодування завданих збитків або за наявності помилок в комп'ютерній програмі.

7. Формування правових вимог щодо забезпечення достовірності індикації та фіксації подій або явищ в реальному світі, факт наявності яких є причиною для здійснення певних дій сторін при виконанні розумного контракту.

8. Розв'язання правовими засобами проблеми наявності неповної можливості для учасників договору спостерігати за всіма прихованими діями програмного забезпечення розумного контракту, що може призвести до небажаного збитку.

9. Розробка правових механізмів верифікації сторін контракту, що здійснюють транзакцію, на момент її здійснення.

10. Розв'язання протиріччя між законодавчими вимогами обмеження доступу до персональних даних та іншої чутливої інформації сторін контракту, яка в ньому може міститися, і відкритістю інформації за всіма транзакціями для всіх учасників публічної децентралізованої мережі блокчейнів і її зберіганням в кожному вузлі блокчейн-ланцюжка.

11. Правова регламентація забезпечення кібербезпеки як програмного забезпечення, що підтримує використання розумних контрактів, так і програмно-апаратних платформ, на яких розміщується це програмне забезпечення.

12. Розробка пропозицій стосовно процесуальних особливостей розгляду в суді суперечок, пов'язаних з розумними контрактами.

Загальні висновки

1. Розумні контракти – створюють умови для реалізації на практиці переваг технологій Інтернету речей.

2. Розумні контракти – інноваційна форма контрактів, укладення, виконання та припинення яких відбувається з використанням мережевих комп'ютерних програмних та/або програмно-апаратних засобів, що мають взаємозв'язок з фізичними або цифровими об'єктами, за участю або без участі людини, що вимагає проведення системних і комплексних правових досліджень в рамках цивільного, фінансового, інформаційного права тощо.

3. Доцільно орієнтуватися на стратегію максимально можливого використання правових механізмів традиційної системи права з необхідним удосконаленням або розвитком окремих правових положень.

До створення нових правових конструкцій слід вдаватися тільки в тому випадку, коли в існуючому законодавстві не знаходиться навіть віддаленої аналогії.

Перелік контрольних питань:

1. Охарактеризуйте технологію блокчейн, вирішення яких правових проблем вона може забезпечити?
2. В чому суть централізованої системи довіри?
3. В чому суть розподіленої системи довіри?
4. Навіщо створено загальноєвропейську регуляторну «пісочницю» для блокчейну?
5. Дайте характеристику розумному контракту
6. У яких сферах доцільно використовувати технологію блокчейн та розумних контрактів.
7. Сформулюйте переваги, недоліки та ризики використання блокчейн технологій

Тест https://forms.gle/MCoZjxYc9UaXF9LB9

10. Економіка результату, Інтернет речей і право

1. Поняття та основні засади економіки результату
2. Стратегія і методи реалізації економіки результату
3. Соціальна трансформація та перехід до економіки результату

1. Поняття та основні засади економіки результату

Економіка результату – це новий світ, де підприємства конкурують за їх здатність надавати результати:
- важливі для їх клієнтів,
- мають кількісні показники,
- в певному місці та у визначений час.

Результат – задоволення потреб та інтересів людини.
Кількісна оцінка результату – міра відповідності задоволенню потреб та інтересів людини.

Економіка результату
- виробляється лише те и стільки, скільки замовляють та споживають;
- споживається все, що виробляється;
- велика економія ресурсів;
- люди отримують лише те, що задовольняє їх потреби та інтереси;
- потреби та інтереси людей максимально задовольняються;
- якість життя людей значно покращиться.

Основні засади Економіки результату

Базова мета бізнес діяльності
- задоволення потреб та інтересів людини;
- отримання прибутку;

Базові вимоги до результату бізнес діяльності
- має бути доставлений або наданий в зазначений час і в будь-яке місце на планеті;
- має характеристики і параметри релевантні потребам та інтересам споживача

Базові вимоги щодо реалізації Економіки результату:
- розуміння потреб споживачів та контекстів, у яких будуть використовуватися товари та послуги;
- мати кількісну оцінку результату у режимі реального часу.

Виконати ці вимоги для масштабування – неможливо в умовах сучасної реальної економіки.

2. Стратегія і методи реалізації економіки результату

Стратегія

Умови реалізації принципу Економіки результату:

- кооперація великої кількості економічних акторів;
- кооперaційні зв'язки ситуативні;
- суб'єкти різної державної юрисдикції;
- локація суб'єктів не передбачувана;
- організація кооперації в режимі реального часу тощо.

Фундаментальний вплив на економічні відносини мають особливості сучасного процесу розвитку цивілізації:
- швидке зростання темпів і масштабів глобалізації;
- глобалізуються – відносини: транснаціональних корпорацій, міждержавні, середнього та малого бізнесу різної юрисдикції, міжособистісні;
- світова логістична інфраструктура – дозволяє швидко переміщувати товари, капітали, послуги та людей в будь-яку точку планети;
- високі темпи і масштаби проникнення ІКТ та інтернет-технологій в усі сфери людської активності;
- глобалізація інформаційних процесів стала необхідною для глобалізованого людства і можливою, завдяки використанню ІКТ та мережі Інтернет.

Сучасна економічна наука

Проблема: недостатня релевантність моделей глобальної/національної економіки, недосконалі економічні моделі, проблеми стратегічного прогнозування та планування на макро- та мікроекономічному рівні

Сучасна реальна економіка на має можливості для забезпечення реалізації принципу відповідних економічних, фінансових, логістичних, технологічних та правових умов.

Вихід є – це Інтернет речей! Чому?

Рішення приймаються та виконуються в режимі реального часу на основі:

- збору і обробки величезної кількості даних;
- ідентифікації всіх суб'єктів та об'єктів, що беруть участь в процесах;
- застосування спеціальних математичних алгоритмів, зокрема алгоритмів штучного інтелекту.

Два методи реалізації стратегії Економіки результату

1. Залученість до життя споживача – виробник має багато знати про конкретного споживача.

Реалізація – функціональний таргетинг.

.2 Залученість до виробничого процесу – споживач сам визначає характеристики необхідного товару або послуги.

Реалізація – Індустрія 4.0 (індустріальний IoT.)

Функціональний таргетинг – наукова інтерпретація та апроксимація отриманих результатів обробки великих даних про людину з використанням положень:

- соціології,
- соціальної психології та психології особистості, з урахуванням освітніх, ментальних, культурних і релігійних особливостей особистого досвіду тощо окремої людини.

Функціональний таргетинг – це методи, способи і механізми збору та обробки неструктурованої інформації про людину (споживача) з різних джерел, що дозволяють з високою достовірністю визначити якісні та кількісні характеристики її потреб та інтересів, недоліки та переваги її життєвих обставин, патерни її поведінки для подальшого формування індивідуальних пропозицій товарів та послуг з метою максимально повного вирішення проблемних ситуацій споживача.

Функціонально таргетована економічна діяльність – це діяльність з доставки результатів роботи, товару та послуги в потрібне місце та час з параметрами і характеристиками релевантними запитами і інтересам конкретного споживача.

Економіка результату – це функціонально таргетована економічна діяльність суб'єктів ринку, які забезпечують на основі ситуаційної взаємодії (інтеграції) з будь-якими іншими суб'єктами ринку задоволення потреб будь-якого конкретного споживача.

3. Соціальна трансформація та перехід до економіки результату

Економіка результату – це людиноцентристська економіка з:

- величезним ресурсозберігаючим та інноваційним потенціалом,
- зі зміненою природою екосистем коопераційної взаємодії конкуренції, з глобальною соціо-технологічною базою (IoT).

Реалізація стратегії розвитку такої економіки зажадає проведення масштабних соціальних і цифрових трансформацій.

Соціальна трансформація – це перетворення, зміна або корекція мети функціонування, структури і функцій суспільства, в тому числі, методів, способів і механізмів реалізації цих функцій, для нейтралізації або сприяння дії зовнішніх і внутрішніх впливів на його подальший розвиток.

Перехід до Економіки результату – проведення масштабної соціальної трансформації:

1) необхідна умова – перетворення, зміна або корекція:
   - мети функціонування органів публічної влади, бізнес структур у всіх сегментах економічної діяльності;
   - світогляду, системи цінностей, способу життя споживачів, а також оволодіння ними відповідними знаннями та навичками;

2) зміна інституційної структури і функцій системи публічного управління і регулювання в економічній сфері;

3) еволюційне створення сегментноорієнтованих об'єднань економічних акторів для гнучкого формування кооперації;

4) вдосконалення правового забезпечення, створення нових механізмів реалізації функцій публічного управління і регулюванн;

5) правове забезпечення формування предметно орієнтованих екосистем кооперaційної взаємодії економічних акторів різної галузевої приналежності, зокрема, в умовах різної державної юрисдикції та із мінімальними транзакційними витратами;

6) проведення масштабного реінжинірингу колишніх і створення нових бізнес-моделей і бізнес-процесів в економічній діяльності.

Зв'язок Економіки результату і права

В економіці результату заради задоволення інтересів конкретної людини відбувається конвергенція (злиття, інтеграція) процесів і результатів автономних в минулому економічної діяльності різних виробників.

Подібно має відбуватись конвергенція законодавства різних галузей, яке буде застосовуватись до різних за змістом економічних процесів, що будуть відбуватись одночасно в інтересах конкретного споживача в різних юрисдикціях.

Крім того, має вирішуватись велика правова проблематика застосування технологій IoT, зокрема, що стосується Робототехніки, Штучного Інтелекту, Хмарних технологій, Великих даних, Кібербезпеки тощо.

Ми знаходимось на порозі великої синергії 3-х фундаментальних явищ сучасності
- Економіки результату
- Цифрових трансформацій (IoT, ШІ, роботи, Big Data, Інтернет)
- Трансформації системи права

Місія розвитку цивілізації: покращення якості життя на основі підвищення ефективності

Перелік контрольних питань:

1. Охарактеризуйте головні риси притаманні економіці результату.
2. У чому відмінність економіки результату від сучасної економіки.
3. Які є методи для реалізації стратегії економіки результату.

Тест https://forms.gle/Rsq8DFrWy9ZTyzJm

11. Методичні рекомендації

11.1 Програма курсу (Силабус)

11.2 Методичні рекомендації до семінарських занять та самостійної роботи

11.1 Програма курсу (Силабус)

Силабус навчальної дисципліни

Рівень вищої освіти	Другий (магістерський)
Галузь знань	08 Право
Спеціальність	081 Право
Освітня програма	Право
Статус дисципліни	Вибіркова (факультативна)
Форма навчання	Дистанційна (змішана)
Обсяг дисципліни	4 кредити ЄКТС / 120 годин
Семестровий контроль/ контрольні заходи	Залік
Розклад занять	1 лекція 1 раз на тиждень/ 1 семінар 1 раз на тиждень
Мова викладання	Українська
Інформація про керівника курсу / викладачів	Лектор: доктор юридичних наук, професор Баранов Олександр Андрійович e-mail: baa_1@ukr.net Практичні / Семінарські: кандидат юридичних наук, старший викладач Дубняк Марія Вікторівна e-mail: euliot20@gmail.com
	Практичні / Семінарські: кандидат юридичних наук, старший викладач Головко Ольга Михайлівна e-mail: euliot20@gmail.com

Програма навчальної дисципліни

Опис навчальної дисципліни, її мета, предмет вивчання та результати навчання

Метою навчальної дисципліни є формування у студентів теоретичних та практичних навичок, підвищення правової культури та ерудиції, оволодіння ними передовим досвідом Євросоюзу у правовому регулюванні застосування Інтернету речей (IP, Internet of Things, IoT).

Що будемо вивчати.

Теорію та практику інформаційного законодавства Євросоюзу в одній із найсучасніший та найскладнішій сфері суспільства – сфері застосовування Інтернету речей. Складність обумовлена тим, сфера насичена застосуванням складних Інтернет та комп'ютерних технологій, тому студентам будуть надаватись необхідні загальні технічні знання.

Навчання базується на аналізі документів ЄС найвищого рівня: стратегій, концепцій, регламентів та директив тощо дотичних до сфери IoT. Зокрема, це стосується таких питань як: основи та принципи функціонування IoT, ризики та бар'єри впровадження, правове забезпечення кібербезпеки критичної інфраструктури, захисту персональних даних, верифікації та ідентифікації суб'єктів, використання великих даних та хмарних технологій, застосування роботів та штучного інтелекту, розумних контрактів, технологій блокчейну тощо.

Чому це цікаво

Практично в кожній сфері діяльності сучасні суспільні відносини реалізуються з використанням Інтернет технологій. Тому з однієї сторони юристи мають знати особливості правового регулювання таких суспільних відносин, а з іншого – вміти максимально використовувати переваги застосування Інтернет технологій в професійної діяльності. Дана навчальна дисципліна є вкладом у формування важливої конкурентної переваги сучасного юриста – це знання правових систем передових держав, особливо, у сферах які стали локомотивом всебічного розвитку суспільства.

Такою проривною сферою світ сьогодні визнає широкомасштабне застосування технологій IoT (сотні млрд доларів інвестицій, понад 40 передових держав мають національні стратегії розвитку IoT). Беззаперечно, це відноситься до Євросоюзу – одного із лідерів як розвитку світової економіки, так і розбудови Єдиного цифрового ринку 27 держав-членів та застосуванню IoT практично у всіх сферах соціальної активності. Саме Євросоюз створив найбільш системне та ефективне законодавство у сфері проектування, впровадження та застосування технологій IoT.

Опанування навчальної дисципліни дозволить досягнути наступне:

- підвищити правову культуру та ерудицію, оволодіти передовим досвідом у правовому регулюванні суспільних відносин в ЄС у сфері застосування Інтернету речей;
- набути знання, уміння і навички:
  - аналізу питань про розвиток, ризики та бар'єри впровадження IP, загальні проблеми впровадження та застосування Інтернету речей;
  - розуміння положень Європейського права щодо кібербезпеки критичної інфраструктури IP, захисту персональних даних, верифікації та ідентифікації суб'єктів та об'єктів IP,
  - з'ясування напрямів вирішення правових проблем застосування базових технологій IP, використання великих даних та хмарних технології, регулювання застосування роботів та штучного інтелекту, розумних контрактів та інших випадків застосування технологій блокчейна;
- здобути навички виявлення проблем, що виникають, шляхів їх розв'язання, а також покращення творчого креативного мислення та самовдосконалення професійного рівня на прикладі проведення порівняльно-правового аналізу на прикладі європейського і національного законодавства,
- сформувати навички прийняття рішень щодо правових проблем, опанування навиків формування та обґрунтування власної правової позиції;
- виховувати відданості ідеям істини, справедливості та законності, почуття відповідальності юриста перед людиною, суспільством і державою, а також сформувати почуття нового в соціальному розвитку, розуміння неминучості впливу цього на необхідність вдосконалення та оновлення системи правового регулювання та законодавства.

Основні завдання навчальної дисципліни

Після засвоєння навчальної дисципліни студенти мають продемонструвати такі результати навчання:

- **ЗНАТИ:**
  - Особливості правового регулювання суспільних відносин в частині застосування Інтернет технологій відповідно до законодавства Євросоюзу.
  - Теорію та практику права щодо проектування, створення та застосування окремих складових технологій IoT.

- **УМІТИ:**
  - Визначати правовий режим даних, що збираються, накопичуються та використовуються в технологіях IoT,
  - Формувати правові вимоги щодо забезпечення кібербезпеки критичних елементів IoT.
  - Пропонувати можливі правові механізми регулювання застосування роботів із штучним інтелектом, хмарних технологій та технологій блокчейну.

Пререквізити та постреквізити дисципліни (місце в структурно-логічній схемі навчання за відповідною освітньою програмою)

Попередні дисципліни: інформаційне право, цивільне право, господарське право.

Зміст навчальної дисципліни

Денна форма навчання

Назви розділів і тем		Лекції	Семінари	СРС
Розділ 1. Введення в предметну сферу Інтернету речей				
1.	Загальні питання Інтернету речей.	2		
2.	Політика Євросоюзу щодо розвитку Інтернету речей, системні ризики та перешкоди впровадження.		2	8
3.	Соціальне підприємництво та IoT.	2		
4.	Застосування технологій IoT із значним соціальним ефектом.		2	8

Розділ 2. Загальносистемні правові проблеми впровадження Інтернету речей					
5.	Загальні проблеми безпеки впровадження та застосування Інтернету речей.		2		
6.	Інфраструктурні, технологічні, техногенні та інформаційні аспекти безпеки при застосуванні IoT.			2	8
7.	Кібербезпека та критична інфраструктура Інтернету речей.		2		
8.	Правові проблеми забезпечення кібербезпеки IoT.			2	8
9.	Особливості захисту персональних даних.		2		
10.	Правові виклики забезпечення захисту персональних даних в умовах застосування IoT.			2	8
11.	Електронні довірчі послуги		2		
12.	Верифікація та ідентифікація суб'єктів та об'єктів. (директива ЄС).			2	8
Розділ 3. Законодавче регулювання застосування базових технологій Інтернету речей.					
13.	Правові проблеми застосування базових технологій Інтернету речей.		2		
14.	Екстериторіальність використання технологій хмарних обчислювань.			2	8
15.	Правове регулювання застосування роботів та штучного інтелекту.		2		
16.	Правосуб'єктність роботів із штучним інтелектом.			2	8
17.	Переваги та бар'єри застосування технологій блокчейна.		2		
18.	Правові умови застосування розумних контрактів.			2	8
	МКР		-	-	4
	Залік:		-	-	4
	Всього годин:	120	20	20	80

Навчальний контент

Методика опанування навчальної дисципліни (освітнього компонента)
Опанування дисципліни здійснюється на засадах проблемного методу навчання, тобто шляхом виявлення проблемних питань і вирішення їх на основі інтерактивної дискусії. Для підвищення рівня з'ясування змісту дисципліни інформація надається також через зоровий канал сприйняття за допомогою презентацій.

З метою розвитку професійних здібностей майбутніх юристів широко застосовуються такі форми: розв'язання практично спрямованих кейсів, на основі судової практики; доповідь підготовленого есе за актуальними проблемами; обговорення як між окремими студентами, так і між групами; спланованої та спонтанні дискусії; ділові ігри з ролями із реального життя юристів, розробки проектів певних документів.

Всі ці форми потребують від студентів розвитку вмінь щодо дослідницької діяльності, яка притаманна для будь-якій юридичної професії. Тому в процесі викладання приділяється увага подальшому розвитку когнітивних навичок в частині пошуку інформації, зокрема нормативно-правової, її аналізу, виявлення правових проблем, визначення можливих шляхів їх вирішення, складання необхідних документів для їх вирішення.

Пошук та вирішення правових проблем в процесі колективної роботи здійснюється на основі особистісно-орієнтованих (розвиваючих) технологіях, які гуртуються на активних формах і методах навчання («мозковий штурм», «аналіз ситуацій» дискусія кейс-технологія, проектна технологія і ін.).

Звичайно буде забезпечуватись допомога в опануванні відповідних інформаційно-комунікаційних технологій для забезпечення проблемно-дослідницького характеру процесу навчання та активізації самостійної роботи студентів (електронні презентації власних есе та доповідей тощо).

Самостійна робота студента/аспіранта

До самостійної роботи студентів включається підготовка до аудиторних занять шляхом опанування матеріалів лекції та вивчення базової і додаткової літератури. Розв'язок кейсів та практичних задач, підготовка юридичних документів.

Рекомендований загальний час для підготовки до одного практичного заняття – 3 години.

Політика та контроль

№ з/п	Контрольний захід	%	Ваговий бал	Кількість	Всього
1	Доповіді на семінарських (опрацювання лекційного матеріалу)	50	7	7	49
2	Виконання практичних завдань	40	10	4	40
3	Модульна контрольна робота	10	11	1	11
	Всього				100

Теоретична частина включає в себе опрацювання студентами лекційного матеріалу та виступів з доповідями.

Критерії оцінювання:

Ваговий бал	Критерій оцінювання
6-7	Здобувачвиконавдодатковітворчізавдання (проаналізував наукові джерела, судову практику)
5	Здобувач опрацював матеріали лекцій, додаткову літературу, вільно володіє матеріалом, вірно відповідає на питання, підтримує дискусію.
4	Здобувач опрацював лише матеріали лекцій добре володіє матеріалом, вірно відповідає на питання.

Практична частина семінару включає в себе такі види робіт:

Ваговий бал	Критерій оцінювання
10	Презентація з доповіддю, виконання творчих завдань.
10	Письмовий аналіз юридичних документів.
10	Підготовка документів.
10	Письмове вирішення задач та кейсів.
10	Аналіз судової практики, аналітичних матеріалів.

Модульна контрольна робота

Ваговий бал	Критерій оцінювання
11	Виконується у формі тестових завдань.

Заохочувальні бали*:

Ваговий бал	Критерій оцінювання
10	підготування та опублікування тез доповіді статті в науковому фаховому виданні за тематикою курсу (у співавторстві, чи під науковим керівництвом викладачів)

* До рейтингу зараховується один із запропонованих видів заохочувальних балів, і не звільняє студента від обов'язку виконати умови допуску до іспиту.

Календарний рубіжний контроль

Метою проведення календарного рубіжного контролю є виявлення якості виконання графіка освітнього процесу студентами.

Критерій	Перший	Другий
Термін	8-й тиждень	14-й тиждень
Умови отримання позитивного результату	10 балів	40 балів

Семестровий контроль

Можливість отримання оцінки «автоматом»: так, для студентів, які виконали умови допуску до заліку і мають рейтинг ≥ 60 балів.

Обов'язкові умови допуску до заліку
Активна робота на всіх лекціях.
Активна робота не менш як на 7 семінарських заняттях, з них особиста активність (доповіді, захист творчих робіт, участь у дискусії) не менше 15 хв. кожного заняття.
Виконання 4 практичних робіт.
Поточний рейтинг RD ≥ 40

Залік проходить за умовами м'якого РСО (до поточного рейтингу додаються бали отримані на заліку).

Вид завдання	Статус	Бали
Он-лайн тестування в аудиторії	обов'язкове	60

Тест складається з 20 завдань різної складності і змісту, оцінюється у 3 бали кожне
20*3 = 60

Студент допускається на залік з мінімальним рейтингом RD ≥ 40. Отже, 40 (поточний рейтинг) + 60 (максимум за залік) = 100 балів.

Таблиця переведення рейтингових балів за університетською шкалою

Рейтингові бали	Оцінка за університетською шкалою
95-100	Відмінно
85-94	Дуже добре
75-84	Добре
65-74	Задовільно
60-64	Достатньо
Менше 60	Незадовільно
Невиконання умов допуску	Не допущено

Силабус складено

д.ю.н., професор Олександр БАРАНОВ

к.ю.н., ст. викладач Марія ДУБНЯК

к.ю.н., ст. викладач Ольга ГОЛОВКО

11.2 Методичні рекомендації до семінарських занять та самостійної роботи

І. Загальні організаційні питання.

В ЗВО формується група студентів на чолі зі старшим групи, який є комунікатором з організаційних питань з Менеджером проекту.

Кожна така група розділяється на семінарські групи, кількість студентів в яких визначається відповідно до методичних вимог проведення інтерактивних форм занять.

Лекційний потік може складатись із студентських груп одного чи декількох ЗВО.

Лекційні та семінарські заняття проводяться факультативно поза офіційним розкладом навчальних занять.

ІІ. Викладання лекційного семінару.

Викладання лекційного матеріалу здійснюється он-лайн за допомогою додатку «Хмарні конференції ZOOM».

Для участі в лекції необхідно перейти за посиланням, яке буде надано у відповідному каналі Телеграм (Telegram).

Для викладання лекції використовуються презентації, які підготовлені за допомогою програми PowerPoint для Windows.

Презентація кожної лекції буде надаватись студентам за допомогою програми Google Classroom.

Якість засвоєння матеріалів лекції буде ідентифікуватись за дві доби до відповідного семінарського заняття за допомогою он-лайн тестування.

III. Семінарські заняття

Проведення семінарських занять здійснюється он-лайн за допомогою додатку «Хмарні конференції ZOOM».

Перед семінарськими заняттями необхідно опанувати зміст викладеного лекційного матеріалу, а також зміст матеріалу який буде надано у вигляді відповідної презентації для самостійного опрацювання. Презентаційний матеріал семінару надається одночасно з наданням презентації попередньої лекції.

Якість засвоєння самостійно опрацьованих матеріалів семінару буде ідентифікуватись за дві доби до відповідного семінарського заняття за допомогою он-лайн тестування.

Крім того, для кожного семінару будуть надані окремі інструкції щодо підготовки питань до нього та методичні вказівки щодо його проведення.

Окремі інструкції до семінарського заняття надаються одночасно з наданням презентації попередньої лекції.

IV. Оформлення презентацій студентами

В процесі виконання деяких завдань до семінарів та їх публічного захисту виникне необхідність підготувати відповідну презентації.

Перший слайд такої презентації має бути зроблений за зразком, в якості якого рекомендується використовувати перший слайд будь-якої лекції.

Для оформлення інших слайдів в якості загального зразка оформлення рекомендується використовувати презентації лекцій.

Комунікації.

В якості комунікаційних каналів використовуються:

Телеграм (Telegram) – для оперативної комунікації, для розміщення посилань на ZOOM конференції:
- один загальний – для лекційного потоку;
- для кожної семінарської групи;

Google Classroom – для підтримки всього обсягу навчального процесу.

Крім того, проект «EULIOT» має загально доступні канали поширення інформації:
- веб-сайт;
- FB сторінка.

Загальні технічні вимоги.

1. Використовувати комп'ютер або iPad. Не використовувати – смартфони.
2. Мати відеокамеру, яка вмикається на весь час заняття.
3. Мати навички роботи з програмами Word, PowerPoint для Windows,
4. «Хмарні конференції ZOOM», Телеграм, Google Classroom.

Окрема інструкція

Правила користування платформою ZOOM під час проведення занять із навчальної дисципліни «Євроінтеграція: законодавство та Інтернет речей»

ШАНОВНІ СТУДЕНТИ!

Для плідної роботи на платформі Zoom з урахуванням особливостей он-лайн спілкування, нагадуємо Вам про певні технічні особливості:

Просимо всіх на початку лекції або семінару вимкнути мікрофони і тримати їх постійно вимкнутими.

Це позбавить наш он-лайн простір зайвих шумів та звуків. Просимо вмикати мікрофони лише у випадку власного виступу, за проханням викладача або для задавання питання.

Якщо у Вас неякісне Інтернет з'єднання, то радимо вимкнути і відео-зв'язок. В додатку ZOOM ця кнопка знаходиться поруч з кнопкою Вашого мікрофону.

1. Всі Ваші запитання до викладачів озвучте, піднявши руку в ZOOM. Викладач наддасть Вам слово. Крім того, після закінчення заняття викладач наддасть відповіді на всі Ваші запитання та коментарі.

2. Всі Ваші запитання з технічних моментів радимо писати у чат.

3. Якщо Ви плануєте робити пости про Вашу участь у заході в соціальних мережах, запрошуємо ставити посилання: #euliot

4. Анкета для студентів

ПІБ	так	ні
Курс інформаційного права		
Вміння користування ZOOM		
Вміння користування Телеграм (Telegram)		
Вміння користування Google Classroom		
Чи інстальована програма «Хмарні конференції ZOOM»		

Відповідальним за організацію навчального процесу зі сторони проекту є Менеджер проекту.

Формується лекційна група студентів на чолі зі старшим групи, який є комунікатором з організаційних питань з Менеджером проекту.

Література та нормативні акти

1. Alliance for Internet of Things Innovation (AIOTI) (European Commission 24 March 2015). URL: https://ec.europa.eu/digital-single- market/en/news/launch-alliance-internet-things-innovation.

2. Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures (ENISA, November 2017). URL: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot.

3. Commission staff working document Advancing the Internet of Things in Europe (Brussels, 19.04.2016). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016SC0110.

4. Communication from the Commission to the European Parliament and the Council. Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union (Brussels, 29.5.2019). URL: https://eur-lex.europa.eu/legal-content/EN/ TXT/?uri=COM:2019:250:FIN.

5. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A Digital Agenda for Europe. URL: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52010DC0245.

6. Declaration Cooperation on a European Blockchain Partnership (Brussels 10 April 2018). URL: https://cysec-conf.com/wp-content/uploads/2019/12/Declaration-Cooperation-on-a-European-Blockchain-Partnership.pdf.

7. ENISA NCSS Good Practice Guide Designing and Implementing National Cyber Security Strategies (NOVEMBER 2016). URL: https:// www.enisa.europa.eu/publications/ncss-good-practice-guide.

8. Europe 2020. A strategy for smart, sustainable and inclusive growth. URL: https://eur-lex.europa.eu/legal-content/en/ ALL/?uri=CELEX%3A52010DC2020.

9. European blockchain strategy. Share. Build. Deploy (European Union, 2019). URL: https://ec.europa.eu/digital-single-market/en/news/european-blockchain-strategy-brochure.

10. European Parliament and of the Council Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32004R0460.

11. European Parliament and of the Council, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EU (General Data Protection Regulation). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

12. European Parliament and of the Council, Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Text with EEA relevance.). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1807.

13. European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (Strasbourg 16 February 2017). URL: https://www.europarl.europa.eu/ doceo/document/TA-8-2017-0051_EN.html.

14. European Parliament, Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (Strasbourg, 6 July 2016). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC.

15. Golovko O.M. Information policy of Ukraine: prospects and threats / Європейська традиція в міжнародному праві: реалізація прав людини : міжнародна науково-практична конференція; м. Братислава, Словацька Республіка, 6-7 травня 2016 р. С. 38-40.

16. Баранов О.А. Інтернет речей: теоретико-методологічні основи правового регулювання. Т.1: Сфери застосування, ризики і бар'єри, проблеми правового регулювання: монографія / О.А. Баранов; НДІІП НАПрН України – К.: Видавничий дім «АртЕк», 2018. – 344 с.

17. Баранов О. А. Правове забезпечення інформаційної сфери: теорія, методологія і практика : монографія / О. А. Баранов. – Київ : Едельвейс, 2014. – 497 с.

18. Баранов О.А. Інформаційне право України: стан, проблеми, перспективи / О.А. Баранов. – К. : Видавничий дім «СофтПрес», 2005. – 316 с.

19. Баранов О. А. Про тлумачення та визначення поняття «кібербезпека» / О. А. Баранов / Правова інформатика. – 2014. – № 2. – С. 54–62.

20. Баранов О.А. «Інтернет речей» як правовий термін / О.А. Баранов / Юридична Україна. – 2016. – № 5-6. – С. 96–103.

21. Баранов О.А. Захист персональних даних в сфері Інтернет речей / О.А. Баранов, В. М. Брижко / Інформація і право. – 2016. – № 2. – С. 15–31.

22. Баранов О. Віртуальність і правове регулювання / О.А Баранов / Публічне право.– 2017. – № 1. – С. 210-218.

23. Баранов О.А. Інтернет речей (IoT): правові моделі використання обмеженого радіочастотного ресурсу (частина I)/ О.А Баранов / Інформація і право. – 2017. – № 2. – С. 41-50.

24. Баранов О.А. Інтернет речей (IoT): правові моделі використання обмеженого радіочастотного ресурсу (частина II) / О.А Баранов / Інформація і право. – 2017. – № 3. – С. 73-84.

25. Баранов О.А. Інтернет речей і штучний інтелект: витоки проблеми правового регулювання / IT-право: проблеми та перспективи розвитку в Україні : збірник матеріалів II-ї Міжнародної науково-практичної конференції (Львів, 17 листопада 2017 р.). – Львів : НУ «Львівська політехніка», 2017. – 318 с. (С. 18-42).

26. Баранов О.А. Інтернет речей (IoT): правові проблеми застосування розумних контрактів / О.А Баранов / Інформація і право. – 2017. – № 4. – С. 26-40.

27. Баранов О.А. Інтернет речей (IoT) і блокчейн / О.А Баранов / Інформація і право. – 2018. – № 1. – С. 59-71.

28. Баранов О.А. Інтернет речей (IoT): мета застосування та правові проблеми / О.А Баранов / Інформація і право. – 2018. – № 2. – С. 31-44.

29. Баранов О.А. Інтернет речей (IoT): робот зі штучним інтелектом у правовідносинах / Юридична Україна. – 2018. – № 5-6. – С. 75–95.

30. Баранов О.А. Інтернет речей (IoT): регулювання надання послуг роботами зі штучним інтелектом / О.А Баранов / Інформація і право. – 2018. – № 4. – С. 46-70.

31. Baranov A. (2019) Internet of Things: Future Telecommunication. In: Ilchenko M., Uryvsky L., Globa L. (eds) Advances in Information and Communication Technologies. UKRMICO 2018. Lecture Notes in Electrical Engineering, vol 560. Springer, Cham ,<https://doi. org/10.1007/978-3-030-16770-7_1> Print ISBN 978-3-030-16769-1

32. Баранов О.А. Правові аспекти національних стратегій розвитку штучного інтелекту / Юридична Україна. № 7. – 2019. – С. 21-38. Закон України

Всі монографії розміщені у вільному доступі за адресою: https:// baa129. wixsite.com/baranov/books

33. Головко О.М. Дослідження поняття «кіберпростір» у вітчизняному законодавстві. Юність науки 2018: соціально-економічні та гуманітарні аспекти розвитку суспільства: Міжнародна науково-практична конференція студентів, аспірантів і молодих вчених (м. Чернігів, 11-12 квітня 2018р.): у 2-х ч. Чернігів: Черніг. нац. технол. ун-т, 2018. Ч. 2: С. 120-121.

34. Головко О.М. Закони функціонування інформаційного суспільства: філософсько-антропологічний вимір. Інформаційні технології і безпека : зб. Матер. XV Міжнар. наук.-практ. конф.; м. Київ, 21 жовтня 2015 р. К.: ІПРІ НАНУ, 2015. с. 50-53.

35. Головко О.М. Право людини на безпечне інформаційне середовище в контексті природних прав людини. Правова інформатика. 2014. № 4 (44). С. 79-85.

36. Головко О.М. Секс-футурологія: Інтернет речей у дії. Інтернет речей: проблеми правового регулювання та впровадження: Друга науково-практична конференція (Київ, 29 листопада 2018 р.). К.: КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2018. С. 64-65.

37. Головко О.М. Четверте покоління прав людини: безпековий аспект. Актуальні проблеми управління інформаційною безпекою держави: Наук.-практ. конф. (Київ, 30 березня 2018 р.). Київ: Нац. акад. СБУ, 2018. С. 42-44.

38. Дубняк М.В. Визначення та правовий статус технологічного контракту. Інформаційне право: сучасні виклики та напрями розвитку: Матеріали І науково-практичної конференції (18 жовтня 2018 р., м. Київ), Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорсько- го». К.: «Політехніка». 2018. С. 118-122. URL: http://ippi.org.ua/sites/ default/files/maket-6.pdf.

39. Дубняк М.В. Законодавче регулювання інформаційної взаємодії в органах місцевого самоврядування європейських країн. Міжнародний науково-практичний юридичний журнал «Legea si Viata». 2017. № 4. С. 31-35. URL: http://www.legeasiviata.in.ua/ archive/2017/4-2/9.pdf.

40. Дубняк М.В. Концептуальні підходи формування дисципліни «Правове забезпечення ІТ-бізнесу». Закарпатське юридичне читання. Матеріали X-ї Міжнародної науково-практичної конференції (19-21 квітня 2018 р., Ужгород). Ужгородський національ- ний університет ім. Ужгород: РІК-У, 2018. Т.1. стор. 379-382 (у співавторстві).

41. Дубняк М.В. Правове регулювання інформаційної взаємодії в процесі прийняття рішень як фактор забезпечення кібербезпеки. Кібербезпека та інтелектуальна власність: проблеми правового забезпечення: матеріали Міжнар. наук. практ. конф., 21 квітня 2017 р. Київський політехнічний інститут імені Ігоря Сікорського. К.: «Політехніка». 2017. С. 98-102. URL: http://ippi.org. ua/sites/ default/files/ch-1.pdf.

42. Дубняк М.В. Роль фіксації юридичних фактів під час виконання смарт-контрактів. Актуальні питання розвитку юридичної науки і практики: матеріали Міжнародної науково-практичної конференції (18 травня 2018 р.). У 2-х томах. Том 1. К., 2018, с. 307-308.

43. Правове регулювання бізнес-моделей стартап-проектів на основі хмарних технологій. Інтернет речей: проблеми правового регулювання та впровадження: матеріали II наук.-практ. конф. (29.11.2018, Київ). стор. 78-81.

44. Становлення і розвиток правових основ та системи захисту персональних даних в Україні: монографія / В.Г. Пилипчук, В.М. Брижко, О.А. Баранов, К.С. Мельник; за ред. В.М. Брижка, В.Г. Пилипчука. К.: ТОВ «Видавничий дім «АртЕк», 2017. 226 с.

Навчальне видання

Упорядники

Олександр БАРАНОВ

Ольга ГОЛОВКО

Марія ДУБНЯК

Європейська інтеграція: законодавство та Інтернет речей. Навчально-методичний посібник

Матеріали в авторській редакції.

Формат 60х84/16. Ум-друк. арк. 7,27
Наклад 150 прим. Зам. No 2111-09.

Видавець ТОВ «ДС День Печати»
м.Київ, Гродненський провулок, 6а;
e-mail: info@print-day.com