СЛОВО МОЛОДОМУ НАУКОВЦЮ

Марія Уланська
студентка 3-го курсу
НЮУ імені Ярослава Мудрого
Староста наукового гуртка
з цивільного права НЮУ
імені Ярослава Мудрого
під керівництвом проф. І. В. Спасибо-Фатєєвої
(2023–2024 н. рік)
Голова комітету науки та іноземних мов
Ради студентського самоврядування
факультету юстиції НЮУ імені Ярослава Мудрого
(2023–2024 н.р.)

УДК 347.2:347.4:347.7
DOI: https://doi.org/10.69724/2786-8834-2024-1-1-233-254

ПРАВОВИЙ ПОГЛЯД НА ФУНКЦІОНУВАННЯ ТЕХНОЛОГІЙ «ІНТЕРНЕТ РЕЧЕЙ» ТА «РОЗУМНИЙ БУДИНОК»

Уланська Марія. Правовий погляд на функціонування технологій «інтернет речей» та «розумний будинок»

Анотація

В статті досліджено рівень правового врегулювання в світі, відносно нового об'єкту цивільно-правових відносин – технологій інтернету речей (Internet of Things або IoT), безпосередньо розумного будинку. Встановлено, що в різних країнах існує достатньо регулятивних документів стосовно IoT, захисту даних та інш. Але водночас важливими є: 1) відмінності між IoT і штучним інтелектом, 2) сутність технології розумного будинку не тільки як сукупності різних пристроїв, а й цілісного «організму». Логічним постає висновок про те, що наявного наразі стану врегулювання окремо приладів IoT або принципів штучного інтелекту, недостатньо для високого, лаконічного і доречного рівня встановленого правового контролю над функціонуванням smart houses.

Враховуючи аналіз судової практики та нормативно-правових актів різних країн в індустрії технологій, до юридичного науково-практичного простору вноситься пропозиція для розробки спочатку загальних принципів функціонування розумних будинків, а згодом створення нової бази норм права. Зміст юридично важливих принципів функціонування технології розумного будинку автором статті вбачається у наступному: 1) фундаментальні принцип інформаційної безпеки для

всеможливих систем розумного будинку; 2) охорона персональних даних; 3) громадська довіра; 4) повага до приватного життя; 5) науково-практична визначеність.

Ключові слова: інтернет речей, розумний будинок, штучний інтелект, об'єкт правовідносин, нерухомість, право інтелектуальної власності, принципи функціонування.

Сучасний світ безперервно розвивається. Одним з підтверджень цього є поява, становлення, вдосконалення феномену IoT (Internet of Things) – інтернету речей, основною метою якого є комплексний розвиток цифрових технологій. IoT утворює система зв'язків між комп'ютерами, приладами, додатками інтернету речей, датчиками і т.д. Усі складові такої системи IoT мають п'ять основних властивостей: 1) підключеність до мережі, 2) здатність оперативного збору даних, 3) можливість обміну інформацією, 4) аналіз отриманих даних, 5) функціонування задля покращення показників ефективності. Сьогодні реалізованим IoT є розумний дім.

Технологія «розумний будинок» – це система для автоматизованого контролю й керування інженерним устаткуванням будинків[1]. Така система покликана забезпечувати комфорт, безпеку і ресурсозбереження для всіх користувачів[2]. Цю технологію також називають терміном «розумна побутова техніка», тобто система, що функціонує автоматично та може бути запрограмовано за допомогою комп'ютера, який застосовується до будівель або резиденцій[3]. Особливістю системи розумного будинку є можливість управління нею, всім обладнанням і технікою, від налаштувань освітлення до різних побутових приладів, у дистанційному форматі за допомогою смартфона або інших гаджетів[4] .

Те, що в минулому здавалося чимось неймовірним, наразі набуло матеріального вираження у якості автоматизації інженерних систем. Розумні будинки революціонізують спосіб взаємодії з житловим простором. Такий новий вид нерухомості має низку суттєвих переваг, зокрема: 1) сприяння енергозбереженню та екологічності завдяки можливості відстежувати та контролювати споживання енергії внаслідок встановлення розумних термостатів, сонячних панелей, розумних систем освітлення та інш.; 2) зручність і комфорт, зокрема завдяки можливості дистанційного контролю різних аспектів власниками своїх розумних будинків; 3) забезпечення розширених функцій безпеки завдяки, наприклад, камерам відеоспостереження, датчикам руху та інтелектуальним замкам; 4) комфорт, який забезпечується високим

---

1 Дерев'янко Ю. В., Краснікова О. Л. Дослідження можливостей «інтелектуального будинку». *Право і Безпека*. 2010. No 1. С. 223–226. URL:https://cutt.ly/DbmPI09; Fathur Zaini Rachman. Smart Home Berbasis IoT. *Snitt Politeknik Negeri Balikpapan*. Vol 2. 2017

2 Дужак І. О. Розумний будинок. *Автоматизація технол. і бізнес-процесів*. 2013. No 13–14. С. 31–33. http://journals.uran.ua/atbp/article/download/32920/29533

3 Pratama, B., & Jasmine, R. Smart Home Appliances Regulation and Principles. *Proceedings of the 4th International Conference on Indonesian Legal Studies, ICILS 2021, June 8–9 2021, Semarang, Indonesia*. https://doi.org/10.4108/eai.8-6-2021.2314344

4 ibid

рівнем технологічного розвитку, оснащенням приладами, які дозволяють створювати додатковий час для людей та нові можливості для споживачів, які мають вади, пов'язані зі здоров'ям, що за звичайних обставин могли б значним чином впливати на їх побут; 5) свобода приватного життя, яке власник розумного будинку може реалізувати на свій власний розсуд в залежності від робочого графіку, вподобань до навколишнього світу та інш.

Ринок розумних будинків завдяки технологічним перевагам, новаторству та багатьом іншим чинникам, стрімко зростає[5], у зв'язку з чим правові питання, проблеми стосовно цієї сфери набувають актуальності та необхідності вирішення.

Правові питання, суміжні із функціонуванням розумних будинків

Право нерухомості – традиційна сфера регулювання для правових систем всього світу. Проте коли мова йде про розумні будинки слід пам'ятати про те, що цей інститут не обмежується суто поняттям нерухомості і відповідними межами регулювання, адже не менш важливою складовою виступають численні технологічні «розумні» складові систем освітлення, опалення, безпеки та інш. Якщо рівень врегулювання правового статусу нерухомості досить високий, достатньо досліджений і регламентований, то друга частина розумних будинків є дещо невизначеною і має достатньо прогалин, уникнення яких у правовому просторі є необхідним.

1. Право власності на дані

Перед тим, як визначити правовий режим права власності на дані, слід ідентифікувати місце їх збереження. Слушну думку висловлює українська юридична компанія Legal IT Group, порівнюючи систему розумного будинку з людським організмом: 1) «мозок» – центральна частина мережі, що керує налагодженим функціонуванням технології; 2) «органи чуття» – датчики для розпізнавання руху, тепла та інших показників, що потім направляють відповідні дані у «мозок»; 3) «органи життєдіяльності» – пристрої, які виконують завдання, відштовхуючись від отриманої датчиками інформації; 4) «руховий апарат» – пристрої для активізації діяльності системо розумного будинку, зокрема, пульт дистанційного керування та інш.; 5) «зоровий і слуховий апарат» – відеокамери, колонки, мікрофони, медіаобладнання, проектори та інш[6] .

Сьогодні дискусійним питанням залишається правова природа цифрових об'єктів і визначення їх цифрового режиму[7]. Здебільшого погляди розділяються на дві

[5] Team, T. Why Smart Home Devices Are A Strong Growth Opportunity For Best Buy. Forbes. https://www.forbes.com/sites/greatspeculations/2017/07/05/why-smart-home-devices-are-a-strong-growth-opportunity-for-best-buy/

[6] Права розумного будинку. Юридичні фішки IOT. 2017, December 25. Legal IT Group. https://legalitgroup.com/prava-rozumnogo-budynku/

[7] Некіт К. Г. Цифрові дані та інформація як об'єкти права власності. *Цивілістичні проблеми ІТ-права*. 2021. Випуск 42. С. 38–43

групи, серед яких перша сконцентрована на усталеному цивілістичному підході, згідно з яким об'єкт права власності – річ, тобто предмет матеріального світу[8]. Зокрема О. В. Кохановська вважає, що «поняття право власності на інформацію ... не може застосовуватися до нематеріального блага особливого роду, яким є інформація»[9]. Водночас друга група цивілістичних досліджень спрямована на висвітлення доречності та актуальності можливості включення нематеріальних благ до об'єктів права власності. Наприклад, І. В. Спасибо-Фатєєва акцентує увагу на тому, що обмеження кола об'єктів виключно тілесними речами в аспекті традиційного права власності, не відповідає потребам цивільного обігу [10]. В. М. Брижко та О. А. Баранов підтримують позицію про розширення меж режиму права власності в умовах технічного прогресу[11]. Таким чином, реформування усталених уявлень про об'єкти право власності є актуальним питанням, особливо в умовах активного розвитку приладів IoT, систем розумного будинку, штучного інтелекту, взаємодія з якими нерозривно пов'язана з обертом інформації.

Дані, які збираються в розумну побутову техніку, є особистими даними користувача, а тому повинні бути захищені та не повинні витікати без згоди відповідного власника даних. Потенційно дискусійним питанням є не тільки коло об'єктів права власності в умовах технологічного прогресу, а й суб'єкт такого права. Уявімо, що об'єкт із технологією розумного будинку є предметом договору оренди, іпотеки та інш. Тоді виникає низка питань для подальших досліджень: 1) кого саме буде визначено «власником даних»? 2) За яких обставин, в якому випадку та за яких умов такий «власник даних» може бути змінений? 3) Чи доречне створення нових доктрин у цивілістичному просторі, зокрема «безпосереднього жильця розумного будинку», що буде сконцентроване на тому, що «власником даних» постає людина, яка проживає, розпоряджається, володіє і користується системою розумного будинку? 4) Як співвідносяться право власності на дані різних категорій та інші майнові права на розумний будинок як житловий об'єкт? та інш.

2. Конфіденційність даних. Кібербезпека, витік або злом даних

У контексті технології розумного будинку дані зазвичай поділяють на дві основні групи: дані адміністративного характеру та дані, якими керують пристрої системи розумного будинку [12].

---

8 ibid

9 Кохановська О. В. Цивільно-правові проблеми інформаційних відносин в Україні : автореф. дис.докт. юрид. Наук : 12.00.03. Київ, 2006. 39 с. URL:http://referatu.net.ua/referats/7569/165907

10 Некіт К. Г. Цифрові дані та інформація як об'єкти права власності. Цивілістичні проблеми IT-права. 2021. Випуск 42. С. 38–43; Спасибо-Фатєєва І. В. Трансформери власності в індивідуально-суспільному аспекті. *Вісник Академії правових наук України*. Харків : Право, 2006. No 1 (44). С. 91–100.

11 Некіт К. Г.

12 Pratama, B., & Jasmine, R.

Категорія даних	Адміністративні дані	Дані, якими керують пристрої системи розумного будинку
Приклади	імена, адреси, номери телефонів, електронні адреси, IP-адреси ...	звук, освітлення, поведінка та зображенн
Значення	Використовуються для додатків системи та інтеграції техніки, приладів з відповідним програмним забезпечення технології розумного будинку	Дані, що отримуються інаслідок щоденного використання побутової техніки системи

Актуальність проблеми конфіденційності даних, з якими взаємодіє розумний будинок, простежується у багатьох реальних конфліктах, які часто доходили до етапу розгляду в судовому порядку: *John Baker Orange v. Ring LLC; Ashley Lemay, Dylan Blakeley, Tania Amador, and Todd Craig* v. *Ring LLC; Doty v. ADT, LLC; конфліктні ситуації з компаніями Orvibo, IoT Wyze та інш.*

Юридично значна категорія конфіденційності даних нерозривно пов'язана з кібербезпекою та можливими проблемами у вигляді витоку або злому даних, адже останні поняття і процеси – перш за все вираження порушення конфіденційності. У зв'язку з цим, зазначені терміни доречно аналізувати разом.

Отже, безпека в аспекті технології розумного будинку стосується процесу захисту інформації та пристроїв, які її зберігають, від всеможливих загроз. Основна мета кібербезпеки – захист комп'ютерів, смартфонів, комп'ютерних мереж, а також загалом інформації як такої, що зберігається у відповідних гаджетах[13].

Першочергові складові безпеки інформації, інформаційної системи або технології – доступність, цілісність, конфіденційність[14]. Доступність інформації проявляється у можливості 1) власників розумних будинків здійснювати дозволені операції, 2) безпосередньо підсистем технології впроваджувати своєчасну взаємодію між пристроями-складовими системи. Категорія цілісності відображається у достатній кількості інформації щодо всіх встановлених у будинку приладів та сформованому єдиному механізмі управління. Конфіденційність є одною з основних складових гармонійного приватного життя людини, адже покликана унеможливити витік приватної інформації з технології розумного будинку.

Проте є важливим те, що перелічені вище категорії інформаційної безпеки є здебільшого теоретичними зазначеннями. Необхідним з правової точки зору буде визначення практичного стану функціонування технологій розумного будинку та визначення насправді вразливих етапів такого процесу. Іноземні науковці виокрем-

[13] Setiawan Awan dan Yulianto Erwin, Keamanan Dalam Media Digital. Bandung: Informatika Bandung. 2020

[14] Білова А. О., Онищенко В. В. Методи забезпечення безпеки розумного будинку. *Кібербезпека: освіта, наука, техніка.* 2019. No 2. С. 134–141. https://u.to/SnFMGw

люють наступні уразливі аспекти розумного будинку: 1) злом системи безпеки, 2) отримання мобільним додатком доступу до операцій, які не є необхідними для роботи, 3) отримання шкідливими програмами необмеженого доступу до конфіденційної інформації, що може призвести до її витоку[15].

Контроль над дотриманням конфіденційності інформації, кібербезпеки може здійснюватись шляхом 1) реалізації принципів функціонування штучного інтелекту, приладів IoT, технології розумного інтелекту загалом; 2) дотримання кожною країною конкретного нормативно-правового акту в індустрії IoT; 3) створення нового обов'язкового і узагальненого для технології розумного будинку в різних країнах нормативно-правового акту, адже дотримання норм низки укладених наразі регулятивних документів в певних країнах (Австралія, Індія, Японія, Сингапур, В'єтнам) є добровільним, що може ускладнювати процес

3. Відповідальність

Для визначення суб'єкта відповідальності в аспекті індустрії IoT, штучного інтелекту, розумного будинку, за порушення правових норм та прав користувачів конкретними технологіями спочатку необхідно звернутись до загального поняття та явища юридичної відповідальності. Таким чином, юридична відповідальність – застосування до винної особи примусових заходів за вчинене правопорушення.

Також для деталізації цього питання проаналізуємо суб'єкт відповідальності у справах *John Baker Orange v. Ring LLC; Ashley Lemay, Dylan Blakeley, Tania Amador, and Todd Craig* v. *Ring LLC; Doty v. ADT, LLC, де відповідачами виступали компанії Ring та ADT. Звідси можна побачити, що у контексті функціонування технології розумного будинку, за порушення несуть відповідальність здебільшого юридичні особи, діяльність яких сконцентрована в технологічній індустрії smart houses.*

4. Право інтелектуальної власності та технологія розумного будинку

Не основним як для об'єкта нерухомості, але все ж таки юридичним питанням стосовно розумного будинку є його співвідношення із правом інтелектуальної власності, що характеризується комплексним характером. Перш за все це обумовлено тим, що система розумного будинку складається з багатьох пристроїв, кожен з яких є самостійним об'єктом правової охорони в контексті авторського чи патентного права[16].

Технологія розумного будинку загалом як пристрій може набувати статусу як винахід або корисна модель, за умови дотримання вимог ЗУ «Про охорону прав

[15] E. Fernandes, J. Jung, A. Prakash Security Analysis of Emerging Smart Home Applications. 2016 IEEE Symposium on Security and Privacy. http://iotsecurity.eecs.umich.edu/img/Fernandes_SmartThingsSP16.pdf; V. Sivaraman, D. Chan, D. Earl, and R. Boreli, «Smart-phones attacking smart-homes,» in Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks. ACM, 2016. http://www2.ee.unsw.edu.au/~vijay/pubs/conf/16wisec.pdf

[16] Тарасенко Х. Ю. Об'єкти інтелектуальної власності в системі розумного будинку. http://tspartners.lviv.ua/articles/objekty-intelektualnoji-vlasnosti-v-systemi-rozumnogo-budynku-smart-hauz/

на винаходи і корисні моделі»[17]. З іншого боку, якщо опис такого винаходу або корисної моделі презентувати у вигляді, наприклад, проекту, письмової чи електронної форми, буде застосовуватись охорона згідно зі ст.6 ЗУ «Про авторське право і суміжні права», зокрема, як ілюстрації, карти, плану, креслення, ескізу[18]. Також важливою частиною співвідношення технології розумного будинку та права інтелектуальної власності є умови правомірного використання при формуванні конкретного об'єкту пристроїв, що вже винайдені та наявні на ринку. Таким чином, слушним є 1) використання доктрини вичерпання прав[19], висвітленої у п.5 ст.12 ЗУ «Про авторське право і суміжні права» , п.3 ст.31 ЗУ «Про охорону прав на винаходи і корисні моделі», ч.3 п.6 ст.16 ЗУ «Про охорону прав на знаки для товарів і послуг»[20] або 2) укладання ліцензійного чи іншого договору для отримання дозволу на комерційне використання конкретних пристроїв.

5. Технологія штучного інтелекту та автоматизованого управління в розумному будинку

Сфера розумного будинку останнім часом майже нерозривно пов'язана із штучним інтелектом[21].

Штучний інтелект – це функція, яка дозволяє комп'ютеру, серед іншого, автоматично виконувати певні дії за людину. Такі можливості виконувати завдання зазвичай обумовлені даними, які попередньо були зібрані та відібрані за допомогою низки методів машинного навчання[22]. У свою чергу «Інтернет речей» – це технологія, яка дозволяє підключеним до Інтернету пристроям і приладам налагоджено взаємодіяти між собою та з користувачами. Таким чином, ними пристроями IoT можна керувати дистанційно, передавати дані про свій поточний стан за допомогою команди або відповідати на голосові команди[23]. У контексті безпосередньо розумного будинку пристрої IoT надають дані штучному інтелекту, які останній вико-

---

17 Про охорону прав на винаходи і корисні моделі. Закон України від 15.12.1993. URL:https://zakon.rada.gov.ua/laws/show/3687–12#Text (дата звернення 22.10.2023)

18 Про авторське право і суміжні права. Закон України від 01.12.2022. https://zakon.rada.gov.ua/laws/show/2811–20?find=1&text=%D0%B5%D1%81%D0%BA%D1%96%D0%B7#w1_2 (дата звернення 20.10.2023)

19 Тарасенко Х. Ю.

20 Про охорону прав на знаки для товарів і послуг. Закон України від 15.12.1993. https://zakon.rada.gov.ua/laws/show/3689–12#Text (дата звернення 12.10.2023)

21 Kopytko, V., Shevchuk, L., Yankovska, L., Semchuk, Z., & Strilchuk, R. Smart Home and Artificial Intelligence as Environment for the Implementation of New Technologies. *Path of Science*. 2018. Vol 4(9), 2007–2012. https://doi.org/10.22178/pos.38–2

22 Kopytko, V., Shevchuk, L., Yankovska, L., Semchuk, Z., & Strilchuk, R.; Pekka Ramula. What AI and IoT Can Do For Smart Homes. https://www.linkedin.com/pulse/httpswwwonpassivecomreg5f3lanprn4obqpvqidkkzw3d3d-peter-ramula?utm_source=share&utm_medium=member_ios&utm_campaign=share_via

23 Pekka Ramula.

ристовує для реалізації певних функцій. На відстані розумні пристрої з інтеграцією технологій штучного інтелекту та IoT реагують на голосові команди користувача або попередньо запрограмовану штучним інтелектом команду[24]. Також слід брати до уваги здатність штучного інтелекту навчатися та у перспективі – передбачати бажання користувача розумного будинку. Тому подальша інтеграція IoT та штучного інтелекту в розумний будинок сьогодні не втрачає своєї актуальності, адже є підґрунтям забезпечення високотехнологічного рівня життя.

Важливим питанням є контроль над штучним інтелектом в побуті людини, у зв'язку з чим низка країн вже визначилися з регулятивними принципами у цій сфері. США: довіра громадськості до ШІ; участь громадськості; наукова доброчесність та якість інформації; оцінка та управління ризиками; вигоди та витрати; гнучкість; справедливість та недискримінація; розкриття інформації та прозорість; безпека та захист; міжвідомча координація[25]. Принципи Великої Британії стосовно штучного інтелекту: довіра користувача; повага до приватного життя; безпека та захист[26]. Основні аспекти, на які орієнтується Китай: налагодженість праці; чесність і справедливість; інклюзивність та єдність; повага до приватного життя; безпека і контрольованість; спільна відповідальність причетних до встановлення штучного інтелекту фізичних осіб; відкрита співпраця; компетентний у технологічних питаннях уряд. ОАЕ першочергово звертає увагу на наступні принципи функціонування штучного інтелекту: етика, кібербезпека, гуманність та інклюзивність[27].

6. Договори стосовно розумних будинків

Повернемось до усталеного правила, згідно з яким право власності на нерухоме майно відповідно до договорів купівлі-продажу, міни, ренти та довічного утримання виникає у набувача з моменту нотаріального посвідчення та державної реєстрації цих договорів.

Звідси логічною є важливість встановлення істотних умов договору стосовно розумного будинку. Ціна і строк дії договору визначаються в кожному конкретному випадку індивідуально. Надважливим є саме предмет договору, який розширюється за межі регулювання суто нерухомості у прийнятному наразі для юридичної спільноти вигляді.

Таким чином, до предмету договору у сфері технології розумних будинків на постійній основі повинні входити: 1) які розумні об'єкти або прилади включені до будинку (чи вимагає якийсь із них щомісячну плату за управління згідно з контрактом, який порядок передачі таких приладів, що може спричинити

[24] ibid.

[25] Pratama, B., & Jasmine, R.

[26] Pratama, B., & Jasmine, R.

[27] ibid

розкриття інформації); 2) конкретні характеристики розумних об'єктів в залежності від підсистеми, до якої входять (клімат контроль, музичний супровід, вентиляція, опалення, пожежна сигналізація, газовий контроль, контроль використання електрики, системи водопостачання, контроль освітлення і вологості, сигналізація від неправомірного проникнення в будинок та інш.); 3) час і порядок переходу розумних об'єктів у власність, отримання доступу до технології розумного будинку.

Технологія розумного будинку, її окремі складові та реальність.

Розумні будинки наразі є не такими ідеальними, якими здаються з першого погляду. Підтвердженням цьому є низка конфліктів щодо конкретних аспектів функціонування даної технології.

John Baker Orange v. Ring LLC (United States, 2019). Позивач John Baker Orange подав до Центрального окружного суду Каліфорнії колективний позов проти компанії Ring та її материнської компанії Amazon[28] [20] за наступні чинники: недбалість, втручання в приватне життя, порушення неявної гарантії комерційної придатності, порушення неявного контракту, неправомірне збагачення та порушення Закону про недобросовісну конкуренцію в Каліфорнії [29][20, 21].

Загальне позиціонування продукції компанії Ring представлене у якості технологій розумних систем безпеки з підтримкою Wi-Fi. Основний предмет спору – камери компанії Ring, які, за думкою позивача, не відповідають початковим обіцянкам постачальника. Причиною цьому стала пом'якшена безпека, що призвела до злому камер Ring користувачів їхніми зловмисниками, які, у свою чергу, отримали доступ до системи відео та мікрофонів, котрі згодом використовувалися з метою вторгнення у приватне життя позивачів [21][30]. Невідомий протиправно отримав доступ до двосмугового динаміку камери, через який спілкувався з дітьми позивача (віком 7,9,10 років), заохочував підійти ближче до камери і т.д, після чого змінив пароль та підключив двофакторну аунтефікацію. Важливим нюансом є те, що позивач встановлював пароль середньої складності, не знаючи про той факт, що доступна двофакторна автентифікація, і тому вважав, що компанія Ring не надає користувачам достатні заходи безпеки для запобігання злому системи.

Таким чином, компанія Ring не змогла забезпечити захист своїх камер від кібератак та вимагала лише базовий пароль, не пропонуючи і не заохочуючи дво-

[28] John Baker Orange v. Ring LLC and Amazon.com, INC. https://www.documentcloud.org/documents/6593079-JOHN-BAKER-ORANGE-v-RING-LLC-and-AMAZON-COM–INC

[29] John Baker Orange; Ring Sued in Class Action for Hacking Vulnerability. Law Street Media. (2019, December 30). https://lawstreetmedia.com/news/tech/ring-sued-in-class-action-for-hacking-vulnerability/

[30] Ring Sued in Class Action for Hacking Vulnerability. Law Street Media. (2019, December 30). https://lawstreetmedia.com/news/tech/ring-sued-in-class-action-for-hacking-vulnerability/

факторну автентифікацію. Крім того, у позові стверджувалося, що «Ring відомо, що хакерська спільнота розробила спеціальне програмне забезпечення для злому камер безпеки Ring», також ключовим моментом є подібні до обставин цієї позовної заяви випадки злому камер Ring багатьох користувачів[31] і попри це компанія всеодно демонструвала тільки бездіяльність. John Baker Orange вимагав відшкодування збитків, судового захисту за справедливістю, декларативного характеру розгляду справи та судової заборони.

Черговим прикладом, пов'язаним із витоком даних і пристроямиIoT[32], є справа *Ashley Lemay, Dylan Blakeley, Tania Amador, and Todd Craig* v. *Ring LLC (United States, 2019),* обставинами якої є неправомірне отримання хакерами доступу до камери в кімнаті дитини та подальша розмова з нею[33] .

Яскравим прикладом недостатньої врегульованості технологій є ситуація з китайською компанією *Orvibo*[34], яка виробляла на момент конфлікту (2019 рік) близько ста різних продуктів для розумного будинку та залишила незахищену базу даних Elasticsearch доступною онлайн через веб-інтерфейс без автентифікації. Згодом базу даних було захищено, але доступною вона була протягом 2 тижнів. «Поки база даних залишається відкритою, кількість доступних даних продовжує збільшуватися щодня. Це є масовим порушенням конфіденційності та безпеки з далекосяжними наслідками. Витік даних впливає на користувачів з усього світу», — зазначає дослідницька група, яка виявила порушення у діяльності компанії Orvibo[35] Дані, що були включені до порушення: адреси електрон-

[31] How Hackers Are Breaking Into Ring Cameras, Vice, December 11, 2009, https://www.vice.com/en_us/article/3a88k5/how-hackers-are-breaking-into-ring-cameras; Hackers are taking Control of Ring Cameras and using them to taunt both adults and children, Inc., https://www.inc.com/minda-zetlin/ring-camera-hacked-hackers- bitcoin-ransom-security.htm; Discord is a proprietary freeware voice over internet protocol application and digital distribution platform designed for video gaming communities, that specializes in text, image, video and audio communication between users in a chat channel. As of July 2019, there are over 250 million unique users of the software. https://en.wikipedia.org/wiki/Discord_(software) ; Inside the Podcast that Hacks Ring Camera Owners Live on Air, Vice, December 13, 2019, https://www.vice.com/en_us/article/z3bbq4/podcast-livestreams-hacked-ring-cameras-nulledcast ; Nulledcast: a podcast where hackers play live audio of themselves breaking into Ring cameras and tormenting their owners, BoingBoing, December 13, 2019, https://boingboing.net/2019/12/13/nulledcast.html; Ring camera hacking has become entertainment for some people, Slashgear, December 12, 2019, https://www.slashgear.com/ring-camera-hacking-has-become-entertainment-for-some-people-12603149/; Hackers are taking Control of Ring Cameras and using them to taunt both adults and children, Inc., https://www.inc.com/minda-zetlin/ring-camera-hacked-hackers- bitcoin-ransom-security.html;

[32] Lindsay D., Wilkinson G., Wright E. Regulation of Internet of Things Devices to Protect Consumers. June 2022. p. 152 https://accan.org.au/files/Grants/2022%20UTS%20IOT/ACCAN%20IoT%20Project%20Final%20Report_ 20622_Clean_Accessible.pdf

[33] Ashley Lemay, Dylan Blakeley, Tania Amador, and Todd Craig v. Ring LLC. https://www.classaction.org/media/lemay-et-al-v-ring-llc.pdf

[34] Report: Orvibo Smart Home Devices Leak Billions of User Records. VpnMentor. https://www.vpnmentor.com/blog/report-orvibo-leak/

[35] Exposed Orvibo database leaks two billion records. (2019, July 1). SC Media. https://www.scmagazine.com/news/exposed-orvibo-database-leaks-two-billion-records

них пошт; паролі; коди облікових записів; точні геолокації; IP-адреси; імена та прізвища; ідентифікатори; розумні пристрої; пристрої, які отримали доступ до облікового запису; розклад користувачів. З основних ризиків подібних несправностей бази даних користувачів різноманітних приладів розумного будинку можна виокремити: можливість зловмиснику легко знаходити паролі користувачів у зв'язку зі слабким алгоритмом хешування; здатність зловмисника при його бажанні назавжди заблокувати користувача з його облікового запису, змінивши спочатку пароль, а потім адресу електронної пошти. Однак Orvibo орієнтується не лише на окремі будинки, адже компанія також має різні профілі для офісів і готелів, що значно розширює межі кола користувачів групи ризику витоку, злому даних.

Проблема витоку даних користувачів простежувалася також у діяльності компанії *IoT Wyze*.[36] .

Doty v. ADT, LLC, No. 20-cv-60972, 2020 U. S. Dist. LEXIS 245373 (S. D. Fla. Dec. 30, 2020). Позивачка володіє розумним будинком, в якому, зокрема, встановлені камери відеоспостереження як всередині, так і ззовні, та замки, керування якими можливе шляхом підключення до інтернету. Початок проблем – технік, який безпосередньо встановлював технологію розумного будинку, налаштував за собою віддалений доступ, завдяки чому згодом заходив до облікового запису близько 70 разів і завантажив записи з камер відеоспостереження. Потім позивачка подала колективний позов від свого імені та від імені всіх клієнтів, «до чиїх систем безпеки мав віддалений доступ співробітник або агент» відповідача «без дозволу клієнта»[37].

Отже, проблема кібербезпеки і конфіденційності даних користувачів залишається однією з основних у межах функціонування нового виду нерухомості – розумного будинку, з чого постає нагальне питання про розробку відповідної системи правового врегулювання і уникнення цієї прогалини.

Правове регулювання «smart house» та «IoT»

Нормативно-правові акти в індустрії IoT здебільшого стикаються з проблемами двох напрямків: 1) захист підключених до єдиної системи пристроїв від кіберзагроз і атак (IoT cybersecurity), 2) захист конфіденційності особистої інформації користувачів певної технології (IoT privacy)[38] .

[36] *C.* Budd. Wyze data leak. https://www.geekwire.com/2019/wyze-data-leak-key-takeaways-server-mistake-exposed-information-2–4 m-customers/

[37] Smart Homes and Liabilities: A Brave New World. The National Law Review. https://www.natlawreview.com/article/smart-homes-and-liabilities-brave-new-world

[38] IoT Cybersecurity: regulating the Internet of Things. Thales Group. 2021. https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/inspired/iot-regulations

Країна	Назва регулятивного документу	Основні моменти
Країни ЄС	The Cybersecurity Act[39]	– запровадження сертифікації кібербезпеки – посилення повноважень Агенства ЄС з кібербезпеки – переваги впровадження нової сертифікаційної системи: підвищення довіри громадян/кінцевих користувачів до цифрових продуктів, маркування «center secure", економія коштів та часу завдяки одноразовій сертифікації, підвищення обізнаності урядів
Країни ЄС	Directive 95/46/ЕС[40] [38]	– вплив вимірюють у всьому світі, адже дія поширюється на 500 млн людей[41] [35] – регулювання обробки персональних даних (автоматизованої та інш.) – зв'язок права на повагу до приватного життя та права на захист персональних даних[42] [52] – обов'язкові принципи обробки персональних даних: прозорість, законність, пропорційність – необхідність створення спеціального наглядового органу в кожній країні ЄС – порядок передачі даних третім країнам – робоча група із захисту осіб в контексті обробки персональних даних
Країни ЄС	The Directive on security of network and information systems[43] [39]	– спільний для всіх країн ЄС рівень безпеки мережевих та інформаційних систем – створення національних компетентних органів і груп реагування на інциденти комп'ютерної безпеки (CSIRT) – розвиток довіри між країнами ЄС, ефективне співробітництво

39 The Cybersecurity Act. Regulation (EU) 2019/881 of April 17 2019. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

40 The Cybersecurity Act. Regulation (EU) 2019/881 of April 17 2019. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

41 IoT Cybersecurity: regulating the Internet of Things. Thales Group. 2021. https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/inspired/iot-regulations

42 Hustinx, P. EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation. https://www.statewatch.org/media/documents/news/2014/sep/eu-2014-09-edps-data-protection-article.pdf

43 The Directive on security of network and information systems. EU 2016/1148. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

Країна	Назва регулятивного документу	Основні моменти
		– вимоги безпеки для операторів цифрових послуг Недоліки: низький рівень спільної ситуаційної обізнаності країн ЄС та відсутності спільного реагування на кризу, низький рівень кіберстійкості
США	IoT Cybersecurity Improvement Act [44][40]	– мінімальні стандарти безпеки для підключених пристроїв, які використовує федеральний уряд – уникнення прямого регулювання приватного сектора[45] – надання повноважень у сфері кібербезпеки Національному інституту стандартів і технологій (NIST)
США (штат Каліфорнія)	Senate Bill No. 327 – Information privacy: connected devices[46]	– вимоги безпеки для пристроїв IoT, підключених до мережі Інтернет (прямо чи опосередковано), за допомогою IP- або Bluetooth-адреси – вимога оснащено пристроїв «розумними функціями безпеки»[47], які покликані захищати пристрій IoT та його дані – спрямованість на пристрої IoT і основні методи кібератак – вимоги до паролей (неприпустимість функціонування приладів із «загальним» паролем, встановленим виробником за умовчанням, що мало ризиком підвищену уразливість приладів до кібератак)[48] .
США (штат Орегон)	House Bill 2395 [49]	Зміст подібний до Каліфорнійського закону[50]

[44] IoT Cybersecurity Improvement Act of 2020. https://www.congress.gov/bill/116th-congress/house-bill/1668

[45] IoT Cybersecurity: regulating the Internet of Things. Thales Group. 2021. https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/inspired/iot-regulations

[46] Senate Bill No. 327 – Information privacy: connected devices. SB-327. California State Senate. 28 September 2018z https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327

[47] IoT Cybersecurity: regulating the Internet of Things. Thales Group. 2021.

[48] ibid

[49] House Bill 2395. HB 2395. Oregon House of Representatives. 16 April 2019.

[50] Senate Bill No. 327

Країна	Назва регулятивного документу	Основні моменти
Австралія	Code of Practice – Securing the Internet of Things for Consumers[51]	– перший крок у підході уряду Австралії до підвищення безпеки пристроїв IoT – забезпечення безпеки IoT приладів для споживачів – рекомендований характер як мінімальні стандарти для IoT – для промислової аудиторії – 13 принципів кібербезпеки, 3 основні: дії щодо паролів за замовчуванням, розкриття вразливостей та оновлення безпеки системи приладів IoT
Бразилія	Requisitos de seguranza cibernйtica para equipamentos para telecomunicasxes[52]	– впровадження програми нагляду за ринком приладів IoT – основні критерії кібербезпеки: оновлення програмного забезпечення, віддалене управління, встановлення та експлуатація приладів, доступ до структури пристроїв, персональні дані
Канада	Personal Information Protection and Electronic Documents Act [53]	– визначення поняття персональні дані – регламентація прав суб'єктів-власників персональних даних
Китай	Guidelines for the Construction of IoT Basic Security Standard Systems (2021 Edition) [54]	– галузева стандартизація пристроїв – п'ять основних стандартів для системи приладів IoT: загальна безпека, безпека терміналу, безпека шлюзу (включають безпеку пристрою IoT gateway, безпеку обміну та обробки даних, безпеку зв'язку та інтерфейсу, безпеку фізичного середовища, безпеку компонентів, а також тестування та оцінку), безпека платформ

[51] Code of Practice – Securing the Internet of Things for Consumers. Code of Practice. Australian Government, Department of Home Affairs. October 2020. https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf

[52] Requisitos de segurança cibernética para equipamentos para telecomunicações. Act n 77, 5th of January 2021. Brazilian Agency of Telecommunications (Anatel). 5 January 2021. https://informacoes.anatel.gov.br/legislacao/atos-de-certificacao-de-produtos/2021/1505-ato-77

[53] Personal Information Protection and Electronic Documents Act. PIPEDA. Office of the Privacy Commissioner of Canada. August 2020. https://www.priv.gc.ca/en/privacy-topics/technology/gd_iot_man/

[54] Guidelines for the Construction of IoT Basic Security Standard Systems (2021 Edition). IoT BSSS. Ministry of Industry and Information Technology (MIIT). 23 September 2021. https://www.miit.gov.cn/cms_files/filemanager/1226211233/attach/202110/6615b008ceb14cb789e20ca9badab163.pdf

Країна	Назва регулятивного документу	Основні моменти
Японія	IoT Security Safety Framework [55]	– основна мета: компіляція підходів до забезпечення надійності взаємних зв'язків між кіберпростором і фізичним простором
Королівство Саудівська Аравія	Internet of Things Regulatory Framework [56]	– розрізнення послуг IoT, що надаються через мобільні та фіксовані мережі або з використанням частот, звільнених від ліцензії – регулювання обладнання IoT, вагомість типу технології і діапазону частот – порядок управління даними
Сингапур	Cybersecurity labelling scheme [57]	– мета: підвищення рівня кібербезпеки IoT, покращення захисту кіберпростору Сингапуру – CLS – перший у своєму роді в Азіатсько-Тихоокеанському регіоні – оцінка пристроїв залежно від рівня кібербезпеки – має на меті допомогти виробникам виділитися серед своїх конкурентів і отримати стимул для розробки більш безпечних продуктів [58].
ОАЕ	Internet of Things Regulatory Policy[59]	– мета: скоординований, узгоджений, безпечний, захищений розвиток IoT в ОАЕ – методологія регулювання IoT – вимоги до радіо- та телекомунікаційного кінцевого обладнання – вимоги до постачальників послуг IoT – вимоги до ліцензіатів – обов'язковість дотримання одночасних взаємних зобов'язань

[55] IoT Security Safety Framework. IoT-SSF. Ministry of Economy, Trade and Industry (METI). 5 November 2020. https://www.meti.go.jp/policy/netsecurity/wg1/IoT-SSF_ver1.0_eng.pdf

[56] Internet of Things Regulatory Framework. IoT Regulatory Framework. Communication and Information Technology Commission. September 2019. https://www.cst.gov.sa/en/RulesandSystems/RegulatoryDocuments/Documents/IoT_REGULATORY_FRAMEWORK.pdf

[57] Cybersecurity labelling scheme. CSL. Cyber Security Agency of Singapore (CSA). October 2020. https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cybersecurity-labelling-cheme

[58] ibid

[59] Internet of Things Regulatory Policy. IoT Regulatory Policy. Telecommunications Regulatory Authority. 22 March 2018. https://tdra.gov.ae/-/media/About/regulations-and-ruling/EN/Regulatory-Policy---Internet-of-Things--IoT--pdf.ashx

Країна	Назва регулятивного документу	Основні моменти
В'єтнам	Decision No. 736/ QĐ-BTTTT on 31 May 2021 («Decision») Setting out the List of Baseline Requirements to Ensure Cyber Security for Consumer IoT Devices [60]	– перелік основних вимог до забезпечення інформаційної безпеки мережі для споживчих пристрої IoT (не використовувати спільні паролі за умовчанням; використовувати: керування звітами, безпечні з'єднання, безпечне зберігання персональних даних; запровадити цілісність програмного забезпечення, віддалену перевірку і оцінку системних даних, захист персональних даних споживачів пристроїв IoT та інш.)

Висновки

У сучасному світі різноманітні технології (штучний інтелект, IoT, розумний будинок) набирають більшої популярності з кожним новим днем. А тому, відповідно, потребують належного рівня правового врегулювання, що буде гарантом і надійним інструментом забезпечення налагодженого функціонування технологій та їхньої успішної інтеграції з побутом людини.

Розумні будинки стали значним прогресом у сфері нерухомості. Можна виокремити наступні тенденції для подальшого розвитку технології: 1) синтез штучного інтелекту з технологією розумного будинку (подальше впровадження сумісного і нерозривного розвитку явищ, реформування як системи розумного будинку, так і розумних приладів підсистем різних напрямків окремо); 2) домінування голосового керування системою; 3) покращений та більш детальний рівень управління енергією; 4) орієнтир на здоров'я та добробут мешканців (баланс режиму сну і фізичних вправ, показники чистоти повітря, рекомендації щодо правильного харчування та інш. В автоматизованому режимі); 5) зв'язок з іншими розумними будинками, розширена технологічна комунікація (існують гіпотези про можливість розширення впливу технологічного прогресу від «розумного будинк» до «розумних міст»)[61].

У цьому аспекті важливо зазначити, що в різних країнах дійсно достатньо регулятивних документів стосовно IoT, захисту даних та інш. Але водночас важливими є: 1) відмінності між IoT і штучним інтелектом, 2) сутність технології розумного будинку не тільки як сукупності різних пристроїв, а й цілісного «організму». Тобто можна зробити логічний висновок про те, що наявного наразі стану врегу-

[60] Decision No. 736/QĐ-BTTTT on 31 May 2021 («Decision») Setting out the List of Baseline Requirements to Ensure Cyber Security for Consumer IoT Devices. List of Baseline Cyber Security Requirements for Consumer IoT. Authority of Information Security (AIS). 31 May 2021. https://mic.gov.vn/Upload_Moi/VanBan/736QD.PDF

[61] The Rise of Smart Homes: Integrating Technology in Real Estate. *Vakilsearch*. 2023. https://vakilsearch.com/blog/rise-of-smart-homes/

лювання окремо приладів IoT або принципів штучного інтелекту, недостатньо для високого, лаконічного і доречного рівня встановленого правового контролю над функціонуванням smart houses.

Беручи до уваги аналіз судової практики та нормативно-правових актів різних країн в індустрії технологій, до юридичного науково-практичного простору вноситься пропозиція для розробки спочатку загальних принципів функціонування розумних будинків, а згодом створення нової бази норм права, що покривали б порушені у цій статті проблеми: право власності на адміністративні дані та дані зовнішнього світу, з якими безпосередньо взаємодіють пристрої всеможливих підсистем розумного будинку; конфіденційність даних; забезпечення кібербезпеки; протидія поширеному витоку або злому даних; відповідальність у разі протиправного функціонування розумного будинку; право інтелектуальної власності в технологічному світі; штучний інтелект як складова smart house: роль, переваги взаємодії прогресивних технологій.

Отже, можна виокремити наступні юридично важливі принципи функціонування технології розумного будинку як такої: 1) фундаментальні принцип інформаційної безпеки для всеможливих систем розумного будинку, зокрема системи Blockchain, IoT Argos і GHOST (багатошаровість, різноманітність, обмеження)[62]; 2) охорона персональних даних; 3) громадська довіра (в юридичному аспекті може бути забезпечена завдяки належному ступеню врегульованості розумного будинку, реальним діям для впровадження правових норм в реальність, справедливому порядку судового розгляду, діяльності компаній smart houses згідно з іншими принципами); 4) повага до приватного життя (принцип, що нерозривно пов'язаний із фундаментальними принципами інформаційної безпеки); 5) науково-практична визначеність (доопрацювання правових проблем навколо розумного будинку, перехід до усталеної думки стосовно можливості права власності користувачів на їхні дані, адаптація тріади права власності до технологічної індустрії, дотримання норм права інтелектуальної власності в індустрії smart houses).

REFERENCES

List of legal documents

Legislation

1. The EU General Data Protection Regulation. The EU GDPR (Directive 95/46/EC). URL:https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?amp;from=EN&uri=CELEX%3A32016R0679 (in English)
2. The Directive on security of network and information systems. EU 2016/1148. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN (in English)
3. IoT Cybersecurity Improvement Act of 2020. URL:https://www.congress.gov/bill/116th-congress/house-bill/1668(in English)

[62] Albany, M., Alsahafi, E., Alruwili, I., & Elkhediri, S. A review: Secure Internet of thing System for Smart Houses. *Procedia Computer Science*. 2022. 201. 437–444. https://doi.org/10.1016/j.procs.2022.03.057

4. Senate Bill No. 327 — Information privacy: connected devices. SB-327. California State Senate. 28 September 2018z URL:https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327(in English)
5. House Bill 2395. HB 2395. Oregon House of Representatives. 16 April 2019. (in English)
6. Code of Practice — Securing the Internet of Things for Consumers. Code of Practice. Australian Government, Department of Home Affairs. October 2020. URL:https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf (in English)
7. Requisitos de seguranзa cibernйtica para equipamentos para telecomunicaзхes. Act n 77, 5th of January 2021. Brazilian Agency of Telecommunications (Anatel). 5 January 2021. URL:https://informacoes.anatel.gov.br/legislacao/atos-de-certificacao-de-produtos/2021/1505-ato-77 (in Portuguese)
8. Personal Information Protection and Electronic Documents Act. PIPEDA. Office of the Privacy Commissioner of Canada. August 2020. URL:https://www.priv.gc.ca/en/privacy-topics/technology/gd_iot_man/ (in English)
9. Guidelines for the Construction of IoT Basic Security Standard Systems (2021 Edition). IoT BSSS. Ministry of Industry and Information Technology (MIIT). 23 September 2021. URL:https://www.miit.gov.cn/cms_files/filemanager/1226211233/attach/202110/ 6615b008ceb14cb789e20ca9badab163.pdf (in English)
10. IoT Security Safety Framework. IoT-SSF. Ministry of Economy, Trade and Industry (METI). 5 November 2020. URL:https://www.meti.go.jp/policy/netsecurity/wg1/IoT-SSF_ver1.0_eng.pdf (in English)
11. Internet of Things Regulatory Framework. IoT Regulatory Framework. Communication and Information Technology Commission. September 2019. URL:https://www.cst.gov.sa/en/RulesandSystems/RegulatoryDocuments/Documents/IoT_REGULATORY_FRAMEWORK.pdf (in English)
12. Cybersecurity labelling scheme. CSL. Cyber Security Agency of Singapore (CSA). October 2020. URL:https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme (in English)
13. Internet of Things Regulatory Policy. IoT Regulatory Policy. Telecommunications Regulatory Authority. 22 March 2018. URL:https://tdra.gov.ae/-/media/About/regulations-and-ruling/EN/Regulatory-Policy---Internet-of-Things--IoT--pdf.ashx (in English)
14. Decision No. 736/QĐ-BTTTT on 31 May 2021 («Decision») Setting out the List of Baseline Requirements to Ensure Cyber Security for Consumer IoT Devices. List of Baseline Cyber Security Requirements for Consumer IoT. Authority of Information Security (AIS). 31 May 2021. URL:https://mic.gov.vn/Upload_Moi/VanBan/736QD.PDF (in English)
15. Pro okhoronu prav na vynakhody i korysni modeli. [On the Protection of Rights to Inventions and Utility Models.] Zakon Ukrainy [Law of Ukraine] vid 15.12.1993.

№ 3687-XII URL: https://zakon.rada.gov.ua/laws/show/3687−12#Text (accessed: 22.10.2023) (in Ukrainian).
16. Pro avtorske pravo i sumizhni prava. [On Copyright and Related Rights.] Zakon Ukrainy [Law of Ukraine] vid 01.12.2022. № 2811-IX URL: https://zakon.rada.gov.ua/laws/show/2811−20?find=1&text=%D0%B5%D1%81%D0%BA%D1%96%D0%B7#w1_2 (accessed: 20.10.2023) (in Ukrainian).
17. Pro okhoronu prav na znaky dlia tovariv i posluh. [On the Protection of Rights to Trademarks and Service Marks] Zakon Ukrainy [Law of Ukraine] vid 15.12.1993. № 3689-XII URL: https://zakon.rada.gov.ua/laws/show/3689−12#Text (accessed: 12.10.2023) (in Ukrainian).

Cases
18. John Baker Orange v. Ring LLC and Amazon.com, INC. URL:https://www.documentcloud.org/documents/6593079-JOHN-BAKER-ORANGE-v-RING-LLC-and-AMAZON-COM−INC (in English)
19. Ashley Lemay, Dylan Blakeley, Tania Amador, and Todd Craig v. Ring LLC. URL:https://www.classaction.org/media/lemay-et-al-v-ring-llc.pdf(in English)

Bibliography
Authored books
20. Setiawan Awan dan Yulianto Erwin, Keamanan Dalam Media Digital. Bandung: Informatika Bandung. 2020 (in English)
21. Lindsay D., Wilkinson G., Wright E. Regulation of Internet of Things Devices to Protect Consumers. June 2022. p. 152 URL:https://accan.org.au/files/Grants/2022%20UTS%20IOT/ACCAN%20IoT%20Project%20Final%20Report_20622_Clean_Accessible.pdf (in English)

Journal articles
22. Derev'ianko Yu.V., Krasnikova O. L. Doslidzhennia mozhlyvostei «intelektualnoho budynku» [Study of the possibilities of the «intelligent house»] (2010) 1. Pravo i Bezpeka. 223−226. URL: https://cutt.ly/DbmPIO9 (in Ukrainian).
23. Fathur Zaini Rachman. Smart Home Berbasis IoT. (2017) 2. *Snitt Politeknik Negeri Balikpapan*. Vol (in English)
24. Duzhak I. O. Rozumnyi budynok. [Smart home.] (2013) 13−14. Avtomatyzatsiia tekhnol. i biznes-protsesiv. 31−33. URL: http://journals.uran.ua/atbp/article/download/32920/29533 (in Ukrainian).
25. Nekit K. H. Tsyfrovi dani ta informatsiia yak ob'iekty prava vlasnosti. [Digital data and information as objects of property rights.] (2021) 42 Tsyvilistychni problemy IT-prava. 38−43 (in Ukrainian).

26. Spasybo-Fatieieva I. V. Transformery vlasnosti v indyvidualno-suspilnomu aspekti. [Transformers of property in the individual-social aspect.] (2006.) 1 (44). Visnyk Akademii pravovykh nauk Ukrainy. Pravo, 91–100. (in Ukrainian).
27. Bilova A. O., Onyshchenko V. V. Metody zabezpechennia bezpeky rozumnoho budynku. [Methods of ensuring the security of a smart home.] (2019) 2 Kiberbezpeka: osvita, nauka, tekhnika. 134–141. https://u.to/SnFMGw (in Ukrainian).
28. Kopytko, V., Shevchuk, L., Yankovska, L., Semchuk, Z., & Strilchuk, R. Smart Home and Artificial Intelligence as Environment for the Implementation of New Technologies. *Path of Science*. 2018. Vol 4(9), 2007–2012. URL:https://doi.org/10.22178/pos.38–2 (in English)
29. Pekka Ramula. What AI and IoT Can Do For Smart Homes. URL: https://www.linkedin.com/pulse/httpswwwonpassivecomreg5f3lanprn4obqpvqidkkzw3d3d-peter-ramula?utm_source=share&utm_medium=member_ios&utm_campaign=share_via(in English)
30. Ring Sued in Class Action for Hacking Vulnerability. Law Street Media. (2019, December 30). URL:https://lawstreetmedia.com/news/tech/ring-sued-in-class-action-for-hacking-vulnerability/ (in English)
31. Report: Orvibo Smart Home Devices Leak Billions of User Records. VpnMentor. URL:https://www.vpnmentor.com/blog/report-orvibo-leak/ (in English)
32. Exposed Orvibo database leaks two billion records. (2019, July 1). SC Media. URL:https://www.scmagazine.com/news/exposed-orvibo-database-leaks-two-billion-records (in English)
33. Smart Homes and Liabilities: A Brave New World. The National Law Review. URL:https://www.natlawreview.com/article/smart-homes-and-liabilities-brave-new-world (in English)
34. The Cybersecurity Act. Regulation (EU) 2019/881 of April 17 2019. URL:https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN (in English)
35. Albany, M., Alsahafi, E., Alruwili, I., & Elkhediri, S. A review: Secure Internet of thing System for Smart Houses. 2022. 201. *Procedia Computer Science*. 437–444. URL:https://doi.org/10.1016/j.procs.2022.03.057 (in English)

Conference papers

36. Pratama, B., & Jasmine, R. Smart Home Appliances Regulation and Principles. Proceedings of the 4th International Conference on Indonesian Legal Studies, ICILS 2021, June 8–9 2021, Semarang, Indonesia. URL: https://doi.org/10.4108/eai.8-6-2021.2314344 (in English)
37. E. Fernandes, J. Jung, A. Prakash Security Analysis of Emerging Smart Home Applications. 2016 IEEE Symposium on Security and Privacy. http://iotsecurity.eecs.umich.edu/img/Fernandes_SmartThingsSP16.pdf (in English)

38. V. Sivaraman, D. Chan, D. Earl, and R. Boreli, «Smart-phones attacking smart-homes,» in Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks. ACM, 2016. http://www2.ee.unsw.edu.au/~vijay/pubs/conf/ 16wisec.pdf (in English)

Theses

39. Kokhanovska O. V. Tsyvilno-pravovi problemy informatsiinykh vidnosyn v Ukraini [Civil and legal problems of information relations in Ukraine] (avtoref dys dokt. yuryd nauk, Kyivskyi natsionalnyi universytet imeni Tarasa Shevchenka, 2006) URL:http://referatu.net.ua/referats/7569/165907 (in Ukrainian).

Websites

40. How Hackers Are Breaking Into Ring Cameras, Vice, December 11, 2009, URL:https://www.vice.com/en_us/article/3a88k5/how-hackers-are-breaking-into-ring-cameras (in English)
41. Hackers are taking Control of Ring Cameras and using them to taunt both adults and children, Inc., URL: https://www.inc.com/minda-zetlin/ring-camera-hacked-hackers- bitcoin-ransom-security.htm (in English)
42. Team, T. Why Smart Home Devices Are A Strong Growth Opportunity For Best Buy. Forbes. URL: https://www.forbes.com/sites/greatspeculations/2017/07/05/why-smart-home-evices-are-a-strong-growth-opportunity-for-best-buy/ (in English)
43 Prava rozumnoho budynku. Yurydychni fishky IOT. [Smart home rights. Legal chips of IOT.] 2017, December 25. (Legal IT Group.) URL: https://legalitgroup.com/prava-rozumnogo-budynku/ (in Ukrainian).
44. Tarasenko Kh. Yu. Ob'iekty intelektualnoi vlasnosti v systemi rozumnoho budynku. [Intellectual property objects in the smart home system.] URL: http://tspartners.lviv.ua/articles/objekty-intelektualnoji-vlasnosti-v-systemi-rozumnogo-budynku-smart-hauz/ (in Ukrainian).
45. Discord is a proprietary freeware voice over internet protocol application and digital distribution platform designed for video gaming communities, that specializes in text, image, video and audio communication between users in a chat channel. As of July 2019, there are over 250 million unique users of the software. URL:https://en.wikipedia.org/wiki/Discord_(software) (in English)
46. Inside the Podcast that Hacks Ring Camera Owners Live on Air, Vice, December 13, 2019, URL: https://www.vice.com/en_us/article/z3bbq4/podcast-livestreams-hacked-ring-cameras-nulledcast (in English)
47. Nulledcast: a podcast where hackers play live audio of themselves breaking into Ring cameras and tormenting their owners, BoingBoing, December 13, 2019, URL:https://boingboing.net/2019/12/13/nulledcast.html (in English)
48. Ring camera hacking has become entertainment for some people, Slashgear, December 12, 2019, URL:https://www.slashgear.com/ring-camera-hacking-has-become-entertainment-for-some-people-12603149/ (in English)

49. Hackers are taking Control of Ring Cameras and using them to taunt both adults and children, Inc., URL:https://www.inc.com/minda-zetlin/ring-camera-hacked-hackers- bitcoin-ransom-security.html (in English)
50. C. Budd. Wyze data leak. URL:https://www.geekwire.com/2019/wyze-data-leak-key-takeaways-server-mistake-exposed-information-2–4 m-customers/ (in English)
51. IoT Cybersecurity: regulating the Internet of Things. Thales Group. 2021. URL:https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/inspired/iot-regulations (in English)
52. Cetome. Panorama of IoT cyber security regulations across the world. Cetome.com. URL:https://cetome.com/panorama (in English)
53 Hustinx, P. EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation. URL:https://www.statewatch.org/media /documents/news/2014/sep/eu-2014–09-edps-data-protection-article.pdf (in English)
54. arch.com/blog/rise-of-smart-homes/ (in English) The Rise of Smart Homes: Integrating Technology in Real Estate. *Vakilsearch*. 2023. URL:https://vakilse

Maria Ulanska
3rd year student
Yaroslav Mudryi National Law University,
Kharkiv, Ukraine
Head of the scientific club of the Civil Law of the Yaroslav Mudryi National Law University under the guidance of Prof. I. V. Spaso-Fateeva (2023–2024 academic year); Chairman of the Committee on Science and Foreign Languages of the Student Government Council of the Faculty of Justice of the Yaroslav Mudryi National Law University (2023–2024 academic year)

Ulanska Maria. Legal view on the functioning of the «internet of things» and «smart home» technologies

Abstracts.

The article examines the level of legal regulation in the world regarding a new object of civil law relations – Internet of Things (IoT) technologies, specifically, smart houses. It is established that in different countries there are sufficient regulatory documents on IoT, data protection, etc. But at the same time, the following are important: 1) the differences between IoT and artificial intelligence, and 2) the essence of smart home technology not only as a set of different devices, but also as an integral «organism».

It is logical to conclude that the current state of regulation of individual IoT devices or artificial intelligence principles is not sufficient for a high, concise and appropriate level of legal control over the functioning of smart homes.

Taking into account the analysis of judicial practice and regulations of different countries in the technology industry, the author proposes to develop, first, general principles of smart homes, and then to create a new framework of legal norms. The author sees the content of the legally important principles of smart home technology functioning as follows: 1) fundamental principles of information security for all kinds of smart home systems; 2) protection of personal data; 3) public trust; 4) respect for privacy; 5) scientific and practical certainty.

Keywords: Internet of Things, IoT, smart houses, artificial intelligence, object of legal relations, real estate, intellectual property rights, principles of operation.