

разом, щоб забезпечити етичне, стійке та гуманне використання штучного інтелекту.

### Список використаних джерел

1. Буковська О.А. До проблеми правового регулювання штучного інтелекту// Збірник матеріалів хі наукових читань, присвячених пам'яті академіка В.В. Копейчикова (м. Київ). <http://elar.naiau.kiev.ua/bitstream/123456789/17794/1> (дата звернення: 05.06.2023).
2. Стець В.В. Україна у сучасному міжнародному просторі // Матеріали Міжнародної наук.-практ. конференції "Україна у сучасному міжнародному просторі" URL: <http://dspace.op.edu.ua/jspui/bitstream/123456789/12143/1/09> (дата звернення: 05.06.2023)
3. Шкурупій О.В., Дейнека Т.А., Туль С.І. Глобальна діджиталізація: переваги, загрози та роль людини в епоху штучного інтелекту : Наукове забезпечення соціально-економічних і управлінських засад розвитку, правового регулювання, провайдингу екоінновацій та енергоефективних технологій в умовах глобалізації в аграрній і суміжних сферах: колективна монографія; за редакцією Ю.В. Самойлик. Полтава : ТОВ НВП «Укрпромторгсервіс», 2021. С. 23-34 <http://dspace.puet.edu.ua/handle/123456789/11226> (дата звернення: 05.06.2023)

УДК 004.056

**Осадчук К.Д.** здобувач вищої освіти

*Вінницького національного технічного університету*

*Науковий керівник Шелепало Г.В. , к.ф.м.н. доцент кафедри захисту інформації Вінницького національного технічного університету*

### **КІБЕРБЕЗПЕКА НА ПРИКЛАДІ ДЕРЖАВИ В СМАРТФОНІ (ДІЯ)**

У наш час, коли інформаційні технології домінують у будь-якій сфері нашого життя, кібербезпека стає найважливішим питанням. Особливо це

застосування мобільних додатків, які використовують мільйони людей з всього світу. Один із таких додатків – «Дія», що надає доступ до послуг державних органів України через мобільний телефон. Однак, на жаль, зі зростанням популярності додатка «Дія», зростає і його вразливість до кібератак. Тому важливо знати, як організувати свою кібербезпеку під час використання цього додатку та які заходи здійснюють його розробники, щоб мінімізувати можливість ризиків.

#### Результати дослідження

Сучасні смартфони стали невід'ємною частиною нашого повсякденного життя. Вони забезпечують нам доступ до інформації, комунікацію, фінансові транзакції та багато інших функцій. Однак, зростаюча кількість ризиків у кіберпросторі ставить під загрозу безпеку наших особистих даних та державної інфраструктури.

Держава повинна відігравати ключову роль у створенні кібербезпеки на рівні смартфонів. Національні уряди повинні розробляти та впроваджувати ефективні стратегії кібербезпеки, враховуючи потенційні загрози та ризики. Наприклад, створення законодавства, спрямованого на захист особистих даних громадян, регулювання використання шифрування та інших технологій безпеки.

Держави повинні також співпрацювати з виробниками смартфонів, щоб впроваджувати кращі практики кібербезпеки на рівні апаратного та програмного забезпечення. Регулярні оновлення програмного забезпечення та патчі для виправлення вразливостей допоможуть у запобіганні кібератак та злому.

У зв'язку зі стрімким розвитком електронного урядування, важливо захиститися від проникнення зловмисників у додатки та інформаційні системи. Дослідження кібербезпеки мобільного додатку «Дія» може бути важливим кроком у напрямку забезпечення захисту електронних систем в Україні. Дана робота досліджує захист додатку від потенційних загроз, таких як злам

користувацьких акаунтів, крадіжка особистих даних та інші атаки на безпеку додатку.

Розробники додають нові функції чи публічні служби майже щомісяця. Відтепер доступний Цифровий паспорт та запущено онлайн-платформу для підприємців «Дія.Бізнес». Проектом керує Міністерство цифрової трансформації на чолі з Михайлом Федоровим. У розробці додатку «Дія» брали участь 35 волонтерів-експертів із найбільшої ІТ-аутсорсингової компанії в Україні EPAM Systems.

Цифрова держава безперечно має багато плюсів, таких як, онлайн-сервіс державних послуг, також містить портал з допомоги малому та середньому бізнесу, онлайн-платформа для розвитку цифрової грамотності тощо.

Безперечно, дана розробка має допомагати українцям захистити свої дані. Тобто застосунок може допомогти кіберполіції викривати незаконні дії, які вчиняють, використовуючи додаток.

Наприклад, так Кіберпол спільно з Мінцифрою викрили в Харкові угруповання, яке займалося масовою підробкою ПЛР-тестів та COVID-сертифікатів. Шахраї працювали близько року і встигли виготовити понад 40 тисяч підроблених ПЛР-тестів та близько 500 підроблених сертифікатів. Щомісячний прибуток зловмисників сягав 4 мільйони гривень [1].

Додаток базується на технології підтягування даних із різних державних реєстрів, про це розказав в інтерв'ю Мстислав Банік [2]. Тобто при додаванні документів вони не зберігаються у коді програми, а підтягуються, що дає більш надійний захист, оскільки державні реєстри також мають захист даних.

До прикладу, так була спроба підробити додаток, але, оскільки хакер не знав роботу коду програми, у нього нічого не вийшло. Тобто зловмисник самостійно розробив застосунок зі схожим дизайном. У фейковій програмі можна було створити будь-який документ — від паспорта до сертифіката про вакцинацію від COVID-19. Фейковий застосунок не мав нічого спільного із

застосунком Дія, адже в розробки не було доступу до жодного з держреєстрів. Під час першої його перевірки можна викрити підробку [3].

«Дія» є гарним додатком для збереження документів та виконання певних дій, але сказати, що додаток є повністю надійним, не можливо. Щоб детально пояснити «що не так із додатком», можна навести невеликий перелік помилок:

1. Істотні дефекти архітектури програми «Дія».
2. Можливі шахрайства з використанням «Дії».
3. Ризики дистанційного несанкціонованого проникнення в смартфон («злом») зі встановленим додатком «Дія».
4. Немоżliвість самотійно заблокувати свій обліковий запис у «Дії» (опція Opt- Out).
5. Ризики відсутності доступу до програми «Дія» через відсутність доступу до інтернету.
6. Відсутність у публічному доступі документації на програму «Дія».
7. Відсутність публічного доступу до вихідного коду програми «Дія».
8. Відсутність інформації про зовнішні незалежні аудити безпеки програми «Дія».
9. Можливість необмеженого клонування документів у додатку «Дія».

Наприклад, перший пункт даного переліку означає, що при створенні програми було порушено один із базових принципів у галузі електронної ідентифікації – розмежування інструментів ідентифікації за рівнями довіри.

Для цього можна використовувати банківські системи, що активно застосовують онлайн-банки. Тобто виконується процес диджиталізації.

Диджиталізація – це процес переведення різноманітної інформації у всіх її формах — текстовій, звуковій, графічній – у цифровий формат, зрозумілий сучасним гаджетам.

У своїй роботі [4] автори описали основні чинники активної діджиталізації, які є характерними для банківського сектору України:

- конкуренція за клієнтів та сегменти ринку;

- стрімкий розвиток соціальних мереж та цифровізація соціальних й адміністративних послуг;
- посилення важливості реагування на кіберризики та зовнішнє шахрайство;
- зростання обсягів інформації та швидкості її обробки [4].

Безперервний розвиток цифровізації дозволяє використовувати для ідентифікації користувача високого рівня довіри, яким має бути власник цифрового паспорта, BankID – програмним інструментом із середнім рівнем довіри.

BankID – це спосіб електронної автентифікації громадян за допомогою їхніх даних в банку, де вони обслуговуються. Щоразу, коли особа хоче скористатися електронною послугою, портал формує електронний запит до банку, де особа є клієнтом, для отримання її персональних даних. Це може бути ППП, паспорт, ІНН, адреса, електронна пошта та інші дані – залежно від порядку надання конкретної електронної послуги. На підставі отриманих даних і проводять електронну автентифікацію особи. BankID має нижчий рівень довіри, ніж електронний цифровий підпис, та може застосовуватися не для всіх електронних послуг – лише найменш ризикових [5].

Проте неодноразово було доведено, що BankID у нинішньому вигляді не створює достатньої безпеки та вразливий для примітивних атак. У будь-яких обставинах електронний ідентифікаційний документ, наприклад, електронний паспорт для виїзду за кордон, має бути захищений виключно засобами найвищого рівня довіри, чого не можна сказати про чинну програму «Дія».

Висновки. Дослідження на тему підтверджує важливість застосування ефективних заходів створення кібербезпеки в сучасному світі, де використання смартфонів стає все поширенішим. На основі дослідження можна зробити кілька висновків.

По-перше, зростаюча залежність суспільства від смартфонів і цифрових технологій створює нові виклики у сфері кібербезпеки. Зловмисники активно

використовують ці можливості для здійснення кібератак, крадіжок інформації та порушення приватності користувачів.

По-друге, захист державних інформаційних систем та особистих даних громадян є критично важливим завданням для кожної держави. У світлі зростаючих загроз кібербезпеці, держави повинні звернути особливу увагу на розробку імунітету до кібератак, на встановлення строгих стандартів безпеки та регулювання використання смартфонів у державних структурах.

По-третє, успішна кібербезпекова політика вимагає не лише застосування технічних заходів безпеки, але й підвищення освіченості користувачів щодо загроз кібербезпеці. Регулярні навчання і свідоме використання смартфонів допоможуть уникнути багатьох загроз і забезпечити захист інформації.

Також важливо зазначити, що кібербезпека є глобальною проблемою, оскільки кіберзагрози можуть походити з будь-якої точки світу. Тому співпраця між державами на міжнародному рівні є необхідною для обміну інформацією, розробки спільних стратегій та координації дій у випадку кібератак.

Отже, кібербезпека на прикладі держави в смартфоні є складною проблемою, яка вимагає комплексного підходу та спільних зусиль з боку держави, громадськості та міжнародного співтовариства. Тільки шляхом поєднання технічних заходів, правового регулювання, співпраці та освіти можна забезпечити ефективний захист від кіберзагроз і зберегти безпеку та приватність у цифровому світі.

### **Список використаних джерел**

1. Прес-служба Міністерства. Мінцифра та Кіберпол викрили злочинне угруповання, які підробили 40 тисяч ПЛР-тестів та COVID-сертифікатів. Міністерство цифрової трансформації України.URL: <https://thedigital.gov.ua/news/mintsifra-ta-kiberpol-vikrili-zlochinne-ugrupovannya-yaki-pidrobili-40-tisyach-plr-testiv-ta-covid-sertifikativ> (дата звернення: 24.05.2023).

2. Розмова. Мстислав Банік: «ДІЯ це не сервіс роздачі повісток» Розмова, 2023. YouTube. URL: <https://www.youtube.com/watch?v=UkE5Ez5JKEY> (дата звернення: 24.05.2023).

3. Прес-служба Міністерства. Мінцифра та Кіберпол викрили розробника фейкової копії застосунку Дія. Міністерство цифрової трансформації України. URL: <https://thedigital.gov.ua/news/mintsifra-ta-kiberpol-vikrili-rozrobnika-feykovogo-zastosunku-diya> (дата звернення: 24.05.2023).

4. Копилова О., Пічугіна Ю., Гончар К. Діджиталізація банківського сектору України: виклики та перспективи. Економіка та суспільство. 2023. № 50. URL: <https://doi.org/10.32782/2524-0072/2023-50-47>

5. BankID НБУ. Національний банк України. URL: <https://bank.gov.ua/ua/bank-id-nbu> (дата звернення: 24.05.2023).

**Кривенков М.О.,**

здобувач вищої освіти Вінницького державного педагогічного  
університету імені Михайла Коцюбинського  
науковий керівник **Самборська О.Ю.**, к.е.н., доц., доцент кафедри  
фундаментальних і приватно-правових дисциплін

## **ФОРМУВАННЯ ПРАВОВОЇ КУЛЬТУРИ АПАРАТУ СУДУ ЯК ЧИННИК РОЗВИТКУ ПУБЛІЧНОЇ ВЛАДИ**

Гармонізація всієї правової системи України з правовою системою Європейського Союзу (ЄС) має особливе значення в сучасній правовій системі. Це стосується і питання вдосконалення законодавства про державних службовців та правового регулювання правової культури працівників апарату суду.

У країнах ЄС інформація про стандарти поведінки міститься в спеціальних законодавчих актах, які часто називають кодексами поведінки