УДК 614.21:004.738.1WWW:004.057.2
DOI https://doi.org/10.32782/2786-7684/2024-2-28

Сімон Кирило Ігорович,
аспірант кафедри соціальної медицини,
громадського здоров'я, організації та
управління охороною здоров'я,
Дніпровський державний медичний університет
ORCID ID: 0000-0003-4155-5873
SCOPUS ID: 59139664000
м. Дніпро, Україна

Підходи до оцінки відповідності вебсайтів закладів охорони здоров'я сучасним цифровим стандартам

Вступ. Цифрова репрезентація закладів охорони здоров'я (ЗОЗ) є необхідністю в умовах цифровізації системи охорони здоров'я. Якість вебсайтів ЗОЗ є критично важливою, оскільки вони відіграють значну роль у наданні пацієнтам доступу до медичних та/або телемедичних послуг, інформації про фахівців, а також дозволяють зручно взаємодіяти із закладом. Керівникам ЗОЗ важливо навчитися оцінювати якість вебсайтів свого закладу, щоб дбати про імідж закладу в умовах зростаючої конкуренції в медичній сфері та більш ефективно задовольняти потреби пацієнтів.

Мета. Розробка критеріїв для оцінки вебсайтів ЗОЗ щодо їх відповідності сучасним стандартам та вимогам пацієнтів на основі міжнародного та національного досвіду з подальшою інтеграцією результатів в практичну діяльність та освітній процес для підвищення цифрової грамотності медичних працівників.

Матеріали та методи. Було проаналізовано законодавчі акти, нормативні документи, наукові публікації та аналітичні матеріали, що регламентують функціонування вебсайтів медичних установ у різних країнах. Особлива увага приділялась захисту персональних даних, доступності інформації та технічним стандартам, оскільки ці пункти є елементами забезпечення кібербезпеки та безбар'єрності цифрового простору.

Результати. Було створено чеклист для оцінки вебсайтів ЗОЗ, який включає вимоги до їх інформаційного наповнення та технічної реалізації. Серед критеріїв оцінки зазначені такі важливі аспекти, як наявність актуальної інформації про заклад, контактні дані фахівців, перелік послуг, можливість запису на прийом онлайн, безпека вебсайту та його адаптивність для різних пристроїв.

Значна увага приділялася обговоренню важливості забезпечення доступності вебсайтів для людей з обмеженими можливостями, а також наявності резервних каналів комунікації у разі надзвичайних ситуацій оскільки вони є елементами реалізації стратегії створення безбар'єрного простору. Окрім цього наголошується на важливості використання безпечних протоколів передачі даних та недопущенні інтеграції реклами третіх сторін на сайтах, з метою попередження витоку чутливої інформації.

Висновки. Проведений аналіз дозволив визначити ключові аспекти якості вебсайтів ЗОЗ. Їх було оформлено в чеклист, який вже можна використовувати на практиці в освітньому та науковому процесі. Впровадження даного чеклисту в навчальний процес допоможе здобувачам медичної освіти отримати навички оцінки вебсайтів ЗОЗ з точки зору їх зручності та відповідності сучасним стандартам. В підсумку це сприятиме підвищенню якості надання медичних послуг та розбудові надійної системи цифрової охорони здоров'я.

Ключові слова: цифровізація охорони здоров'я, цифрові стандарти, телемедицина, здобувачі медичної освіти, вебсайти, заклади охорони здоров'я, захист персональних даних, кібербезпека.

Simon Kyrylo Ihorovych, PhD Student at the Department of Social Medicine, Public Health and Health Care Management, Dnipro State Medical University**,** ORCID ID: 0000-0003-4155-5873**,** SCOPUS ID: 59139664000**,** Dnipro, Ukraine

Approaches to assessing the compliance of the websites of healthcare institutions with modern digital standards

Introduction. The digital representation of healthcare institutions (HCIs) is a necessity in the context of the digitalization of the healthcare system. The quality of HCI websites is critically important, as they play a significant role in providing patients with access to medical and/or telemedicine services, information about specialists, and allow for convenient interaction with the institution. It is important for HCI managers to learn how to assess the quality of their websites in order to maintain the institution's image amid growing competition in the healthcare sector and more effectively meet patients' needs.

Objective. The development of criteria for assessing HCI websites in terms of their compliance with modern standards and patient requirements, based on international and national experience, with the further integration of the results into practical activities and the educational process to enhance the digital literacy of healthcare professionals.

Materials and Methods. Legislative acts, regulatory documents, scientific publications, and analytical materials regulating the functioning of healthcare institution websites in various countries were analyzed. Particular attention was paid to data protection, information accessibility, and technical standards, as these are elements of ensuring cybersecurity and barrier-free access to the digital space.

Results. A checklist for evaluating HCI websites was created, which includes requirements for both their informational content and technical implementation. Among the evaluation criteria were important aspects such as the availability of up-to-date information about the institution, contact details of specialists, a list of services, the ability to book appointments online, website security, and adaptability for different devices.

Significant attention was given to discussing the importance of ensuring website accessibility for people with disabilities, as well as the availability of backup communication channels in emergency situations, as these are elements of a strategy to create a barrier-free environment. Additionally, emphasis was placed on the importance of using secure data transmission protocols and preventing the integration of third-party advertisements on the websites to avoid the leakage of sensitive information.

Conclusions. The analysis identified key aspects of HCI website quality, which were compiled into a checklist that can already be used in practice in both educational and scientific processes. The implementation of this checklist in the educational process will help medical students develop the skills to evaluate HCI websites in terms of their user-friendliness and compliance with modern standards. Ultimately, this will contribute to improving the quality of healthcare services and building a reliable digital healthcare system.

Key words: healthcare digitalization, digital standards, telemedicine, medical students, websites, healthcare institutions, data protection, cybersecurity.

Вступ. Цифрова репрезентація закладів охорони здоров'я (ЗОЗ) є необхідністю в умовах цифровізації системи охорони здоров'я і одним з основних шляхів реалізації цього є створення власного сайту [1].

Якість сайтів ЗОЗ важлива, оскільки вони є ключовим джерелом інформації яка дозволяє пацієнтам отримати доступ до медичних та/або телемедичних послуг, записатися на прийом, ознайомитися з актуальними новинами закладу та дізнатися про його фахівців [2]. Це особливо актуально в умовах сучасних пандемій, коли значна частина консультацій і навіть діагностичних послуг може надаватися дистанційно за допомогою телемедичних технологій [3].

Високоякісний сайт ЗОЗ який надає всю необхідну інформацію у зручному форматі дбаючи при цьому про безпеку та приватність своїх користувачів сприяє підвищенню довіри до медичного закладу, зручності для пацієнтів та ефективності комунікації.

Керівникам ЗОЗ важливо навчитися оцінювати якість сайту власного ЗОЗ, щоб дбати про імідж закладу в умовах зростаючої конкуренції в медичній сфері та більш ефективно задовольняти потреби пацієнтів. Інформаційне наповнення та функціонал вебсайту є факторами, які можуть вплинути на вибір пацієнта між кількома медичними установами, особливо якщо мова йде про дистанційні послуги або зручність доступу до інформації про фахівців та послуги [4].

Метою дослідження є розробка критеріїв для оцінки вебсайтів ЗОЗ щодо їх відповідності сучасним стандартам та вимогам пацієнтів на основі міжнародного та національного досвіду з подальшою інтеграцією результатів в практичну діяльність та освітній процес для підвищення цифрової грамотності медичних працівників**.**

Методологія та методи дослідження. Дослідження було проведено шляхом аналізу нормативно-правової бази, що регулює діяльність вебсайтів медичних установ у різних країнах. Основними джерелами інформації стали законодавчі та нормативні акти, офіційні документи урядів та міжнародних організацій (наприклад: data.europa.eu, ontario.ca, ema.europa.eu, eur-lex.europa.eu, gov.au, rada.gov.ua), а також наукові публікації та аналітичні матеріали.

Пошук і збір даних здійснювалися з використанням відкритих джерел, таких як державні реєстри, правові бази даних та вебсайти відповідних міністерств охорони здоров'я (наприклад: moz.gov.ua, nszu.gov.ua, hhs.gov, cms.gov, healthdata.gov, nhs.uk); наукометричні бази (PubMed, Google Scholar). Ключовими критеріями для аналізу були вимоги до захисту персональних даних, забезпечення доступності інформації для пацієнтів та технічні стандарти вебсайтів, оскільки ці пункти є елементами забезпечення кібербезпеки та безбар'єрності цифрового простору.

Методи аналізу включали порівняння законодавства різних країн, зокрема в частині вимог до функціонування вебсайтів медичних установ, з метою виявлення спільних рис і відмінностей. Зібрані дані було систематизовано та інтерпретовано для подальшого узагальнення результатів.

Виклад основного матеріалу дослідження. За результатами опрацювання нормативно-правової бази визначено, що закордонне законодавство регламентує лише деякі параметри, наприклад такі як безбар'єрність урядових сайтів (і в деяких випадках сайтів ЗОЗ) для людей з обмеженими можливостями [5–9]. В Україні також спостерігається прогрес в цьому напрямку, що виражається у «Національній стратегії зі створення безбар'єрного простору в Україні на період до 2030 року», де в розділі «Аналіз поточного стану та визначення ключових проблем» вказано, що: «Цифрові публічні сервіси (вебсайти, додатки, цифрові послуги) недостатньо адаптовані для всіх груп населення, а тому потребують розроблення та впровадження відповідних стандартів» [10], але на жаль зважаючи на воєнні дії дані процеси відбуваються повільніше, ніж планувалося.

За кордоном [11–13], як і в Україні [14, 15] законодавчо регламентуються параметри безпеки та приватності зберігання чутливих (в тому числі медичних) даних громадян, але їх аналіз потребує по-перше спеціальних технічних компетенцій якими не володіють медичні працівники, по-друге адміністративного доступу до сайту, тому ці аспекти не розглядалися. Особлива увага приділялася безпековим аспектам, які можна оцінити самостійно не маючи спеціальної технічної освіти.

На основі аналізу інформації в інтернет-просторі стосовно стандартів розробки вебсайтів [16, 17], в тому числі вебсайтів ЗОЗ [18, 19], а також публікацій де оцінювали інформаційне наповнення сайтів ЗОЗ [2, 20] було складено чеклист який містить пункти для оцінки сайтів ЗОЗ (табл. 1) за шкалою від 0 (абсолютно не реалізовано) до 10 (повністю реалізовано) для кожного пункту.

Чеклист можна доповнювати та оновлювати в залежності від різних умов та з плином часу, але на момент публікації були враховані майже всі найважливіші пункти для оцінки сайтів ЗОЗ, що дозволяє використовувати чеклист на практиці з освітньою та/або науковою метою.

Зазначений чеклист було впроваджено в навчальний процес при проведенні модулю з «Організації та економіки ОЗ». Здобувачам надавалися пояснення щодо кожного пункту чеклиста, особливо деталізовано було пояснено технічні моменти. Для прикладу наведено пояснення для деяких пунктів чеклисту стосовно технічної реалізації, які надавалися здобувачам:

1) «Адреса електронної пошти (або контакти в популярних месенджерах) ЗОЗ» цей пункт має сенс

Таблиця 1

Чеклист для оцінки сайтів ЗОЗ

Параметр	Оцінка
I. Змістовне наповнення:	
1. Загальні відомості про ЗОЗ:	
1) Повна назва ЗОЗ	
2) Точна адреса ЗОЗ	
3) Керуючі органи ЗОЗ	
4) Структурні підрозділи ЗОЗ	
2. Контактна інформація ЗОЗ:	
1) Дні та години роботи ЗОЗ	
2) Схема під'їзду до ЗОЗ	
3) Контактні телефони ЗОЗ	
4) Контактні телефони технічної підтримки сайту	
5) Адреса електронної пошти (або контакти в популярних месенджерах) ЗОЗ	
3. Діяльність та послуги ЗОЗ:	
1) Ліцензія на медичну діяльність	
2) Інформація про можливість, порядок, обсяг та умови отримання пацієнтами безкоштовної медичної допомоги	
3) Перелік, ціни та правила надання платних медичних послуг	
4. Медичний персонал (основні надавачі послуг):	
1) ПІБ	
2) Посада	
3) Освіта (кваліфікація, диплом)	
4) Дні та години роботи	
5. Правила прийому пацієнтів:	
1) Внутрішній порядок	
2) Правила запису на перший прийом	
3) Умови амбулаторного лікування	
4) Умови та терміни госпіталізації (за наявності стаціонару)	
5) Наявність відповідей на інші часті запитання	
6) Правила прийому громадян керівником організації	
6. Права та обов'язки пацієнтів:	
1) Права та обов'язки громадян у сфері ОЗ	
2) Контакти регіональних органів ОЗ	
3) Контакти органів з нагляду у сфері ОЗ та захисту прав споживачів	
4) Контакти антикорупційних органів	
II. Вимоги до технічного рішення:	
1. Зрозумілість інформації:	
1) Інформація наведена державною мовою	
2) Граматична та орфографічна коректність тексту	
3) Відсутність дублюючої інформації	
2. Маркери актуальності контенту:	
1) Дата першої публікації інформації на необхідних сторінках	
2) Дата останнього оновлення інформації на необхідних сторінках	
3. Відгуки пацієнтів	
1) Наявність відгуків на власному сайті	
2) Наявність відгуків на сайтах третіх сторін (має бути активне посилання)	
4. Новини закладу	
1) Наявність відповідного розділу на сайті	
2) Актуальність (регулярна оновлюваність) відповідного розділу на сайті	
3) Можливість отримувати новини закладу зручним способом, а не тільки на сайті (розсилка e-mail; канал YouTube, Telegam, Viber; RSS-стрічка)	
5. Відсутність на сайті реклами третіх сторін	
6. Доступність всієї інформації без реєстрації на сайті	
7. Ідентифікація сайту ЗОЗ у вебпросторі	
1) Відповідність адреси сайту назві закладу	

Закінчення табл. 1

2) Можливість знайти сайт через пошукову систему в перших 5-ти позиціях пошукової видачі (за умови зазначення назви лікарні та міста де вона розташована та не рахуючи рекламні позиції)	
3) Відсутність дублікатів або старих версій сайту, які не дозволяють зрозуміти яке посилання обрати в пошуковій видачі	
8. Відсутність функціоналу, який не працює належним чином (неробочі посилання, неклікабельні кнопки, тощо)	
9. Можливість записатися на прийом онлайн	
10. Наявність мапи сайту	
11. Наявність пошуку по сайту	
12. Наявність версії для людей з вадами зору (якщо все і так добре видно, то немає необхідності в окремій версії)	
13. Розмір тексту та його контрастність з фоном зручні для сприйняття	
14. Швидкість завантаження сайту навіть при обмеженій швидкості інтернет-з'єднання	
15. Адаптивність сайту (сайт відображається однаково коректно на найбільш поширених типах пристроїв: смартфони, ПК, планшети)	
16. З'єднання з сайтом за допомогою захищеного протоколу HTTPS.	

розглядати окремо від «Контактні телефони ЗОЗ» оскільки це канали зв'язку принципово іншого типу. У випадку надзвичайних ситуацій (НС) певні канали зв'язку можуть бути повністю недоступними [21] і в цьому разі потрібно потурбуватися заздалегідь про резервні канали комунікації для того, щоб зменшити наслідки впливу НС [22].

2) «Можливість отримувати новини закладу зручним способом, а не тільки на сайті (розсилка e-mail; канал YouTube, Telegam, Viber; RSS-стрічка)» – знову ж таки, у випадку НС краще мати резервні канали комунікації. Окрім цього у випадку компрометації певних каналів (наприклад, через кібератаку) і використання їх з метою розповсюдження дезінформації люди зможуть дізнатися про компрометацію з інших каналів зв'язку і убезпечити себе від потенційно небезпечних дій які могли б бути вчинені у відповідь на піддавання дезінформації.

3) «Відсутність на сайті реклами третіх сторін» зменшує вірогідність витоку чутливих даних пацієнтів. Чому ж саме включення реклами третіх сторін на сайті ЗОЗ може бути шкідливою? Це пов'язано з тим, що рекламні мережі (РМ) вбудовують свій код (з ініціативи власника сайту) на цільовий сайт, який динамічно обирає яку рекламу показати користувачу (так званий «таргетинг») для максимізації вірогідності переходу за рекламним посиланням. Для підвищення ефективності таргетингу РМ необхідно знати про користувача якомога більше інформації. Реалізується це шляхом вбудовування коду РМ на максимальну кількість сайтів. На момент публікації Google's AdSense є найпопулярнішою РМ і вбудована на 48,3% всіх сайтів в мережі Інтернет [23], а її доля ринку серед інших РМ складає 99,1% [24]. Таким чином РМ мають можливість збирати всю інформацію при взаємодії користувача з усіма сайтами де вбудовано код цих РМ. Саме по собі накопичення даних користувачів у базі даних РМ не представляє загрози, але проблема в тому, що на цьому все не закінчується. Всі відомі РМ є комерційними компаніями, відповідно ставлять на перше місце власний прибуток, тому дані, які вони збирають потім перепродаються зацікавленим сторонам, якими в тому числі є дата-брокери (торговці даними), які в свою чергу займаються агрегацією персональних даних користувачів з різних джерел для формування якомога більш повного профілю, щоб потім перепродати їх ще дорожче тим, хто готовий за це заплатити (страхові компанії яким потрібно розраховувати вартість індивідуального страхового внеску, банки яким потрібно прийняти рішення про видачу кредиту або навіть шахраї які хочуть збільшити вірогідність успіху своїх злочинних схем використовуючи якомога більше персональних даних своїх потенційних жертв) [25, 26]. Таким чином на основі тематики сторінок які проглянув пацієнт і частоти їх перегляду можна опосередковано дізнатися певний обсяг інформації медичного характеру щодо цього пацієнта. Хочу нагадати, що медичні дані відносяться до чутливих і представляють чи не найбільший інтерес з боку шахраїв та хакерів [27].

4) «З'єднання з сайтом за допомогою захищеного протоколу HTTPS» дозволяє впевнитися, що жоден з тих, хто фізично передає дані у ланцюжку від користувача до сайту не зможе розшифрувати їх зміст і відповідно використати його проти користувача. В останні роки ситуація щодо захищеності з'єднання значно покращилась: від 26,9% у 2018 р. до 84,9% у 2024 р. [28], але до сих пір знаходяться сайти які нехтують цим важливим елементом забезпечення приватності своїх користувачів. Захист з'єднання особливо важливий при наданні телемедичних послуг за допомогою сайту, оскільки якщо мова йде про онлайн-консультації, то при відсутності захисту зловмисники можуть отримати доступ до даних голосу і відеозображення як пацієнта так і лікаря, що значно розширить спектр можливих векторів атаки.

Після надання здобувачам пояснень по кожному пункту їм було надано завдання для самостійного аналізу будь-якого сайту ЗОЗ на території України за даним чеклистом. Після виконання завдання проводилося обговорення за результатами проведеної оцінки. Таким чином здобувачі отримали навички, які дозволяють оцінювати сайти ЗОЗ з точки зору їх зручності, інформаційної наповненості та відповідності сучасним стандартам.

Висновки з дослідження. Проведений аналіз дозволив виявити ключові аспекти якості сайтів ЗОЗ, зокрема безбар'єрність, інформаційне наповнення і безпека та приватність користувачів. Їх було оформлено в чеклист, який можна використовувати на практиці в освітньому та науковому процесі. Запропоновані критерії можуть бути використані для вдосконалення сайтів ЗОЗ, а також для підвищення рівня цифрової грамотності медичних працівників та здобувачів на різних рівнях медичної освіти. Впровадження цих навичок у навчальний процес сприяє формуванню у здобувачів відповідальності за цифрову присутність свого медичного закладу та його репутацію в онлайн-середовищі. В підсумку це сприятиме підвищенню якості надання медичних і телемедичних послуг та розбудові надійної цифрової системи охорони здоров'я.

REFERENCES

1. Sobon M. Hospital Website as an Element of Digital Transformation – Comparative Analysis of 2014, 2018 and 2022. *Procedia Comput Sci*. 2023 Jan 1;225:693-702.
2. Bach MP, Seljan S, Jaković B, Buljan A, Zoroja J. Hospital Websites: From the Information Repository to Interactive Channel. *Procedia Comput Sci*. 2019 Jan 1;164:64-71.
3. Schultz M. Telehealth and Remote Patient Monitoring Innovations in Nursing Practice: State of the Science. OJIN Online J Issues Nurs [Internet]. 2023 May 4;28(2). Available from: https://ojin.nursingworld.org/table-of-contents/volume-28-2023/number-2-may-2023/special-topic-nursing-now/telehealth-and-remote-patient-monitoring/
4. Bujnowska-Fedak MM, Węgierek P. The Impact of Online Health Information on Patient Health Behaviours and Making Decisions Concerning Health. *Int J Environ Res Public Health*. 2020 Jan 31;17(3):880.
5. Accessibility of State and Local Government Websites to People with Disabilities [Internet]. Available from: https://archive.ada.gov/websites2.htm
6. Directive (EU) 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the accessibility of the websites and mobile applications of public sector bodies (Text with EEA relevance) [Internet]. OJ L Oct 26, 2016. Available from: http://data.europa.eu/eli/dir/2016/2102/oj/eng
7. Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services (Text with EEA relevance) [Internet]. OJ L Apr 17, 2019. Available from: http://data.europa.eu/eli/dir/2019/882/oj/eng
8. ADA.gov [Internet]. 2024. Guidance on Web Accessibility and the ADA. Available from: https://www.ada.gov/resources/web-guidance/
9. Review of the Information and Communications Standards: 2020 final recommendations report | ontario.ca [Internet]. Available from: http://www.ontario.ca/page/review-information-and-communications-standards-2020-final-recommendations-report
10. Ofitsiinyi vebportal parlamentu Ukrainy [Internet]. Pro skhvalennia Natsionalnoi stratehii zi stvorennia bezbariernoho prostoru v Ukraini na period do 2030 roku. Available from: https://zakon.rada.gov.ua/go/366-2021-%D1%80
11. Regulation – 2016/679 – EN – gdpr – EUR-Lex [Internet]. Available from: https://eur-lex.europa.eu/eli/reg/2016/679/oj
12. Rights (OCR) O for C. The Security Rule [Internet]. 2009. Available from: https://www.hhs.gov/hipaa/for-professionals/security/index.html
13. Rights (OCR) O for C. The HIPAA Privacy Rule [Internet]. 2008. Available from: https://www.hhs.gov/hipaa/for-professionals/privacy/index.html
14. Mykhailo Radutskyi: Kolehiia MOZ zatverdyla Stratehiiu rozvytku systemy okhorony zdorovia do 2030 roku [Internet]. Available from: https://www.rada.gov.ua/news/news_kom/233093.html
15. Shablony dlia vprovadzhennia kiberstandartiv u medychnykh zakladakh [Internet]. Available from: https://moz.gov.ua/uk/shabloni-dlja-vprovadzhennja-kiberstandartiv-u-medichnih-zakladah
16. Division (DCD) DC. Website Requirements Checklist [Internet]. 2015. Available from: https://www.hhs.gov/web/building-and-managing-websites/development-process-and-milestones/website-requirements-checklist/index.html
17. Digital Service Standard (DSS) | digital.gov.au [Internet]. Available from: https://www.digital.gov.au/policy/digital-experience/digital-service-standard
18. Acosta-Vargas P, Hidalgo P, Acosta-Vargas G, Salvador-Acosta B, Salvador-Ullauri L, Gonzalez M. Designing an Accessible Website for Palliative Care Services. In: Botto-Tobar M, Zambrano Vizuete M, Torres-Carrión P, Montes León S, Pizarro Vásquez G, Durakovic B, editors. Applied Technologies [Internet]. Cham: Springer International Publishing; 2020;371-83. Available from: https://doi.org/10.1007/978-3-030-42517-3_28
19. Acosta-Vargas G, Acosta-Vargas P, Jadán-Guerrero J, Salvador-Ullauri L, Gonzalez M. Improvement of Accessibility in Medical and Healthcare Websites. In: Nunes IL, editor. Advances in Human Factors and System Interactions [Internet]. Cham: Springer International Publishing; 2021;266-73. Available from: http://doi.org/10.1007/978-3-030-79816-1_33
20. Nematollahi M, Fallahnejad E, Niknam F, Nadri N, Khademian F. Evaluation of the structure of websites of educational hospitals of Fars province in 2016. *J Health Manag Inform*. 2015 Dec 22;3:132-7.
21. RBK-Ukraina [Internet]. Naibilsha khakerska ataka na telekom-infrastrukturu u sviti: holova 'Kyivstaru' nazvav tsili. Available from: https://www.rbc.ua/rus/news/naybilsha-hakerska-ataka-telekom-infrastrukturu-1702452541.html
22. RBK-Ukraina [Internet]. NBU rekomenduie bankam stvoryty rezervni kanaly zviazku pislia kiberataky na 'Kyivstar'. Available from: https://www.rbc.ua/rus/news/nbu-rekomendue-bankam-stvoriti-rezervni-kanali-1702538362.html
23. Historical yearly trends in the usage statistics of advertising networks for websites, October 2024 [Internet]. Available from: https://w3techs.com/technologies/history_overview/advertising/all/y

24. Market share yearly trends for advertising networks, October 2024 [Internet]. Available from: https://w3techs.com/technologies/history_overview/advertising/ms/y
25. Khto taki data-brokery i yak vony rozkryvaiut nashu personalnu informatsiiu [Internet]. Available from: https://kunsht.com.ua/articles/khto-taki-data-brokery-i-iak-vony-rozkryvaiut-nashu-personalnu-informatsiiu
26. Out of Control: How Consumers are Exploited by the Online Advertising Industry. Forbruker; 2020. 186 p.
27. American Hospital Association. HHS: EMRs still a top target for cyber criminals [Internet]. Available from: https://www.aha.org/news/headline/2023-04-13-hhs-emrs-still-top-target-cyber-criminals-0
28. W3Techs. Historical yearly trends in the usage statistics of site elements for websites [Internet]. Available from: https://w3techs.com/technologies/history_overview/site_element/all/y