УДК 338.23
DOI: https://doi.org/10.32782/2415-8801/2020-3.13

Новойтенко І.В.
кандидат економічних наук,
доцент кафедри економіки і права,
Національний університет харчових технологій

Малиновський В.В.
старший викладач кафедри технології
хлібопекарських і кондитерських виробів,
Національний університет харчових технологій

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ЯК БІЗНЕС-ТРЕНД

У статті проаналізовано регулювання захисту персональних даних фізичних осіб відповідно до нормативних актів України, Європейського Союзу, США. У результаті проведеного аналізу визначено методи збереження персональних даних із використанням шифрування, токенізації та найвищого рівня захисту за замовчуванням. Розглянуто сутність файлів cookie, за допомогою яких персональні дані збираються. Підкреслено необхідність вивчення політики конфіденційності, яка розкриває інформацію про обсяг персональних даних, що збираються, мету збору та передачі отриманих даних третім сторонам, терміну їх зберігання, права клієнтів дозволити/відкликати дозвіл на їх обробку. Установлено, що переважна більшість сайтів автоматично збирає та зберігає інформацію щодо доменного імені, IP-адреси, виду браузера та операційної системи, дати і часу відвідування сайту, переглянутих сторінок.

Ключові слова: *персональні дані, захист даних, політика конфіденційності, файли cookie.*

PERSONAL DATA PROTECTION AS A BUSINESS TREND

Novoitenko Iryna, Malynovskyi Vitalii
National University of Food Technology

The regulation of personal data protection was analyzed in the article according to the low of Ukraine, the European Union and the United States of America. The relevance of the study is sharing information to consumers in order to use the resources of the online environment consciously, improving their competency of collection, processing and transmission of personal data and demonstrating their ability to influence on this process. The maintenance of General Data Protection Regulation was researched. The rule of personal data protection based on using encryption, tokenization and the highest protection level by default. The essence of cookie file and the structure of Privacy Policy were investigated. The assignment of cookie file is collecting personal data. The main role of Privacy Policy is acquainting the user with the amount of personal data collection, the target of its action, the target of transferring information to third parties, the retention period, the right of customers to allow / revoke permission to use their personal data. The majority of sites automatically collect and store information about the domain name, IP address, type of browser and operating system, date and time of site visiting, details about viewed pages. Personal data collection usage is behavioral targeting. Information owners save every movement of individual activity on web site, such as search inform, purchases in online stores. It helps interested person to form a portrait of the individual taking into account his habits and preferences. Such information can be further used for various purposes, which start for advertising goods / services, informing about events / news and goes to predictive programming of person's behavior in certain situations. This is a reason to attribute personal data to the new modern world currency, which value is significantly underestimated. The size of penalties for data protection violations was determined. The largest penalties of Federal Trade Commission to the famous international companies were considered. The need to read the Privacy Policy before using the Internet resource was emphasized.

Keywords: *personal information, data protection regulation, Privacy policy, cookie files.*

Постановка проблеми. Зростання масштабів кібератак на державні установи та органи місцевого самоврядування, суб'єктів господарювання у сфері охорони здоров'я, торговельні майданчики та соціальні мережі зумовлює регулювання відносин захисту персональних даних та посилення відповідальності суб'єктів за виток такої інформації. Слід зазначити, що захист персональних даних є актуальним питанням і для українських експортерів, бізнес-інтереси яких спрямовані на європейський та американський ринки у зв'язку з прийняттям європейського регламенту GDPR та дією американського CCPA.

Аналіз останніх досліджень і публікацій. За даними праць зарубіжних та вітчизняних науковців Г. Гонсалеса Фустера, Р. Коха, Б. Волфорда, В. Головченко, Б. Томашевського, Р. Прус та за результатами аналізу звіту Світового економічного форуму «Глобальні ризики 2020», до глобальних ризиків на наступні десять років відносять кібератаки та руйнування інформаційної інфраструктури, які поряд зі зміною клімату, застосуванням зброї масового знищення, екстремальною погодою, водною кризою, втратою різноманітних видів біосфери, інфекційними захворюваннями, природними катаклізмами та екологічними катастрофами, спричиненими людською поведінкою, формують ТОП-10 найбільш вагомих ризиків для життєдіяльності по всьому світу [1].

Відповідно до результатів дослідження (Університет Мериленду), хакери атакують кожні 39 секунд, у середньому 2 244 рази на добу [2]. Успіх атакам забезпечують легко розпізнавані логіни і паролі. Так, на першому місці за поширеністю логіну розташовано Root (у перекладі з англ. «корінь»), на другому місці – admin, далі розташувалися test, guest, info, user, adm, administrator, oracle. Серед легкодоступних та розповсюджених паролей виявилися такі: 123456, password, 1234, 12345, 123, test, 1. Отже, використання вищезазначених логінів і паролей слід уникати для запобігання швидкому несанкціонованому доступу до даних, що зберігаються на персональному комп'ютері.

Середньостатистичний період виявлення джерела атаки у 2019 р. становив 206 днів. У вартісному виразі середньостатистичні збитки компанії від витоку інформації оцінюються у $3,92 млн, для компанії зі США – $8,19 млн. Найдорожчою індустрією для атаки є охорона здоров'я, середній розмір збитків організації у цій сфері оцінюється у розмірі $6,45 млн) [3].

Постановка завдання. Для розкриття теми статті поставлено завдання дослідити стан захисту персональних даних, визначити загрози, заходи безпеки та відповідальність.

Виклад основного матеріалу дослідження. Із метою захисту персональних даних Європейський Парламент ухвалив Регламент про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних (General Data Protection Regulation – GDPR (EU) 2016/679). Положення регламенту є обов'язковими для виконання суб'єктами, які працюють із персональними даними осіб із території ЄС та Європейської економічної зони, з 25 травня 2018 р. [4].

Фізичним особам, які перебувають на території ЄС (не лише громадянам ЄС), гарантується захист права контролю, що передбачає отримання дозволу для збору, обробки, передачі іншим суб'єктам їхніх персональних даних. Із уведенням у дію цього Регламенту організація, що збирає та/або обробляє, та/або зберігає персональні дані, зобов'язана повідомити фізичну особу, дані якої збираються, про суб'єктів, які обробляють дані, та суб'єктів, яким передають дані, їхню мету та причини цих дій.

Дія Регламенту GDPR розповсюджується також на організації, зареєстровані поза ЄС, які здійснюють обробку, передачу або зберігання персональних даних осіб, які перебувають на території країн ЄС.

Відповідно до Європейського регламенту, кожна організація має затвердити політику конфіденційності, у якій зазначають перелік персональних даних, що збираються, мету їх обробки, права власників розпоряджатися своїми даними, порядок відповідей на скарги.

Персональними даними, відповідно до GDPR, є будь-яка інформація про фізичну особу, за допомогою якої особу ідентифіковано чи можна ідентифікувати. До персональних даних фізичної особи відносять: літери (ім'я, прізвище особи), числа (ідентифікаційний код особи, номер водійських прав), фотографії, звукозаписи (запис телефонної розмови з оператором), відеозаписи (запис із камер відеоспостереження), якщо за їх допомогою можна ідентифікувати особу [5].

Збір персональних даних фізичних осіб в онлайн-середовищі здійснюється шляхом використання файлів cookie. Вони дають змогу зберігати налаштування вебсайту під зручні для користувача параметри, а саме налаштування мови, налаштування конфіденційності, ідентифікатор користувача та пароль. Це дає змогу уникнути повторного введення/налаштування параметрів під час кожного наступного відвідування Інтернет-ресурсу. На сайтах електронної комерції файли cookie зберігають вміст кошика для покупок і параметри користувача для швидкого оформлення замовлення.

Основною метою збору персональних даних фізичних осіб є поведінковий таргетінг. Власники інформації щодо переглянутих фізичною особою сайтів, пошукових запитів, покупках в Інтернет-магазинах формують портрет особистості з урахуванням її звичок та вподобань. Така інформація в подальшому може бути використана з різною метою, щонайменше – для рекламування товарів/послуг, інформування про заходи/новини з метою прогнозного програмування поведінки особи у певних ситуаціях.

Більшість Інтернет-ресурсів містить файли cookie і повідомляє користувача про їх використання одразу із завантаженням вебсайту.

Перш ніж надати згоду залишитися на сайті, який використовує файли cookie, пропонуємо ознайомитися з політикою їх використання.

Файли cookie залежать від браузера і, по суті, є текстовими файлами, що містять інформацію, яку браузер користувача зберігає в певній папці. Деякі вебсайти надсилають файли cookie на сервер комп'ютера [6].

На сайті компанії з юридичної підтримки IT-бізнесу legalitgroup.com користувача одразу повідомляють про мету використання файлів cookie: для персоналізації контенту і реклами, надання доступу до функцій соціальних мереж і для аналізу їх трафіку. Одразу зазначено, що legalitgroup.com поширює інформацію про використання сайту своїм партнерам із соціальних мереж, рекламним партнерам і партнерам по аналітиці, які, своєю чергою, можуть поєднувати цю інформацію з іншими даними про користувача, отриманими раніше

під час користування їхніми послугами. Детальну інформацію про використання файлів cookie наведено в політиці конфіденційності та захисту даних [5].

Установлені на комп'ютері антивірусні програми зазвичай ідентифікують cookie-файли як низькоризиковані, даючи їм змогу зберігатися у папці на комп'ютері користувача.

Незалежно від операційної системи Windows, MacOS або Linux та незалежно від виду браузера Safari, Firefox, Internet Explorer, Chrome чи будь-якого іншого браузера файли cookie можна виявити на персональному комп'ютері за допомогою пошуку cookie, гіпертексту чи http. Оскільки переважна більшість користувачів здебільшого використовує один і той самий браузер на комп'ютері, cookie може фіксувати майже всі онлайн-дії користувача.

У контексті безпеки персональних даних особливої уваги потребують дії користувачів Інтернет-ресурсів із використанням загальнодоступного Wi-Fi-з'єднання (перебуваючи у кав'ярні, торговельному центрі, спортклубі, аеропорті тощо). Якщо вебсайти не вимагають від браузерів шифрування інформації про файли cookie перед її передачею, ризик витоку інформації може призвести до негативних наслідків.

Використання мобільних пристроїв та мобільного Інтернету знижує ризик неправомірного використання персональних даних порівняно з використанням незахищеного з'єднання персонального комп'ютера з Інтернетом. По-перше, існують десятки різновидів мобільних пристроїв із різними операційними системами, що використовують різні мобільні веббраузери та мобільні додатки із власними параметрами безпеки. По-друге, бездротові цифрові сигнали складніше перехопити та зламати, ніж незашифровані файли http у незахищеній мережі Wi-Fi. Звичайно, коли незашифрована інформація потрапляє до дротового Інтернету, існує ризик її перехоплення та зловживання, але цей ризик є значно меншим порівняно з використанням публічного трафіку точки доступу до Wi-Fi.

Згідно з Регламентом ЄС про захист персональних даних, принцип захисту даних передбачений за замовчуванням. Компанії зобов'язані впроваджувати технічні та організаційні заходи захисту даних із використанням шифрування та анонімізації, а також контролювати доступ до даних персоналу та підрядників. Для реалізації цієї норми Регламенту потрібно підписати угоду про нерозголошення інформації (Non-disclosure agreement) із кожним працівником, упровадити і контролювати дотримання політики обробки даних у межах компанії.

Аналітичний огляд Європейського регламенту GDPR, українського Закону «Про захист персональних даних», Каліфорнійського регламенту Consumer Privacy Act 2018 (CCPA, що набрав чинності 01.01.2020) дає підстави стверджувати, що предметом регулювання цих трьох нормативних актів є правові відносини, пов'язані із захистом та обробкою персональних даних [5; 7].

Каліфорнійський регламент CCPA захищає персональні дані осіб – резидентів штату Каліфорнія. До суб'єктів обробки даних відносяться компанії, які відповідають одному з трьох критеріїв: 1) річний дохід перевищує 25 млн; 2) поодинці або спільно з іншими купує, отримує для комерційних цілей інформацію не менш як 50 тис споживачів, домогосподарств або пристроїв; 3) одержує понад 50% щорічних доходів від продажу особистої інформації споживачів. Каліфорнійський регламент орієнтований на врегулювання відносин з акцентом у сфері продажу персональних даних.

Регламентом GDPR регулюються відносини щодо обробки даних неповнолітніх осіб: до 13 років такі дії проводити заборонено, від 13 до 16 років – за наявності згоди батьків або опікунів на таку дію. У Бельгії, Естонії і Греції встановлено 13-річний вік особи для обробки її персональних даних за згодою батьків або опікунів.

Регламентом CCPA передбачено отримання згоди особи на продаж інформації про неї, якщо вона не досягла 16 років, та отримання згоди її батьків або опікунів, якщо їй не виповнилося 13 років.

За порушення положень Регламенту GDPR контролюючим органом накладається адміністративна відповідальність у вигляді більшої суми: штрафу в розмірі 20 млн євро або 4% річного доходу, отриманого за минулий рік; за порушення положень обробки даних неповнолітніх – 10 млн грн або 2% річного доходу, отриманого за минулий рік.

В Україні за порушення законодавства про захист персональних даних у частині незаконного доступу до них або порушення прав фізичної особи передбачено штраф: на громадян – від 1 700 до 8 500 грн (від 100 до 500 неоподаткованих мінімумів доходів громадян); на посадових осіб, громадян – суб'єктів підприємницької діяльності – від 5 100 до 17 000 грн (від 300 до однієї тисячі неоподаткованих мінімумів доходів громадян) [8].

Серед найбільш масштабних порушень у сфері захисту персональних даних слід відзначити претензії Федеральної комісії з торгівлі (США) до Uber виплатити штраф у розмірі $148 млн (2016 р.) унаслідок спричиненого хакерською атакою витоку інформації щодо 607 тис номерів водійських посвідчень, десятки мільйонів електронних адрес та номерів телефонів споживачів [9].

У 2018 р. було накладено штраф на British Airways у розмірі $230 млн (1,5% річного доходу за 2017 р.) за неправомірний доступ шахрайського сайту (внаслідок хакерської атаки та переадресації) до персональних даних клієнтів щодо входу у систему, даних про їхні платіжні картки та бронювання подорожей, а також їхні імена та адреси [10].

Наступний масштабний штраф у розмірі $700 млн ($300 млн – штраф та $425 млн – компенсація збитків постраждалим особам) накладено на американське кредитне агенство Equifax за порушення безпеки даних, яке призвело до витоку персональних даних 150 млн осіб унаслідок хакерських атак [11].

У 2019 р. історичною та показовою подією світового рівня у сфері захисту персональних даних стало накладання штрафу на Facebook за неправомірну передачу персональних даних 87 млн користувачів (переважно американців) британській консалтинговій компанії Cambridge Analytica. Окрім цього, компанію Facebook звинуватили в обміні особистою інформацією користувачів зі сторонніми додатками, завантаженими Facebook-«друзями», без отримання згоди користувачів. Федеральна комісія з торгівлі США (FTC) зобов'язала Facebook реструктурувати політику конфіденційності, створивши незалежний комітет із питань конфіденційності та позбавивши генерального директора контролю над рішеннями, що стосуються конфіденційності [12].

Висновки з проведеного дослідження. Для забезпечення безпеки персональних даних в онлайн-серед-

овищі завжди слід читати політику конфіденційності. Вона може бути довгою і складною для розуміння, але тільки прочитавши її, зрозумілими є рівень захищеності персональних даних, рівень безпеки і контролю над їх передачею, мета використання інформації та надання її третім сторонам. Якщо користувача інформують про використання cookie-файлів без роз'яснення мети, а інформація щодо політики конфіденційності сайту є незрозумілою, потрібно уникати активності на таких сайтах та відвідувати інші, з більш чіткою і прозорою політикою захисту персональних даних.

Ураховуючи кількість випадків витоку інформації, яка містить персональні дані, формуватиметься попит на Інтернет-ресурси та соціальні мережі, які зможуть забезпечити приватність інформації про фізичну особу та можливість ідентифікації лише за її згодою.

Список використаних джерел:

1. The global risks report 2020. URL: https://www.weforum.org/reports/the-global-risks-report-2020 (дата звернення: 21.08.2020).

2. Michael Cukier. Study: Hackers attack every 39 seconds. URL: https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds (дата звернення: 21.08.2020).

3. Cost of a Data Breach Report highlights. URL: https://www.ibm.com/security/data-breach (дата звернення: 21.08.2020).

4. GDPR. Офіційний український переклад. URL: https://www.kmu.gov.ua/storage/app/media/uploaded-files/es-2016679.pdf.

5. GDPR імплементація, GDPR та персональні дані. URL: https://legalitgroup.com/shho-take-personalni-dani-za-gdpr/ (дата звернення: 21.08.2020).

6. Information about Website Cookies. URL: https://www.allaboutcookies.org (дата звернення: 21.08.2020).

7. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI-ВР, станом на 20.03.2020. *Законодавство України.* URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 21.08.2020).

8. Про адміністративні правопорушення : Кодекс України від 07.12.1984, станом на 13.08.2020. *Законодавство України.* URL: https://zakon.rada.gov.ua/laws/show/80731-10#Text (дата звернення: 21.08.2020).

9. Uber to pay 148 million in settlement over 2016 data breach. URL: https://www.bloomberg.com/news/articles/2018-09-26/uber-to-pay-148-million-in-settlement-over-2016-data-breach (дата звернення: 22.08.2020).

10. British Airways faces record $230 million fine over data theft. URL: https://www.reuters.com/article/us-iag-cybercrime-ico/british-airways-faces-record-230-million-fine-over-data-theft-idUSKCN1U30KD (дата звернення: 22.08.2020).

11. Equifax exposed $150 million Americans personal data. URL: https://edition.cnn.com/2019/07/22/tech/equifax-hack-ftc/index.html (дата звернення: 22.08.2020).

12. FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook. URL: https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions (дата звернення: 22.08.2020).

References:

1. The global risks report 2020. Kyiv. Available at: https://www.weforum.org/reports/the-global-risks-report-2020 (accessed 21 August 2020).

2. Michael Cukier. Study: Hackers attack every 39 seconds. Kyiv. Available at:https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds (accessed 21 August 2020).

3. Cost of a Data Breach Report highlights. Kyiv. Available at: https://www.ibm.com/security/data-breach (accessed 21 August 2020).

4. GDPR. Ofitsiinyi ukrainskyi pereklad. Kyiv. Available at: https://www.kmu.gov.ua/storage/app/media/uploaded-files/es-2016679.pdf.

5. GDPR implementatsiia, GDPR ta personalni dani. Kyiv. Available at: https://legalitgroup.com/shho-take-personalni-dani-za-gdpr/ (accessed 21 August 2020).

6. Information about Website Cookies. Kyiv. Available at: https://www.allaboutcookies.org (accessed 21 August 2020).

7. Pro zakhyst personalnykh danykh: Zakon Ukrainy vid 01.06.2010 №2297-VI-VR stanom na 20.03.2020/ Baza danykh «Zakonodavstvo Ukrainy» / VR Ukrainy. Kyiv. Available at: https://zakon.rada.gov.ua/laws/show/2297-17#Text (accessed 21 August 2020).

8. Pro administratyvni pravoporushennia: kodeks Ukrainy vid 07.12.1984 stanom na 13.08.2020/ Baza danykh «Zakonodavstvo Ukrainy» / VR Ukrainy. [Elektronnyi resurs]. Kyiv. Available at: https://zakon.rada.gov.ua/laws/show/80731-10#Text (accessed 21 August 2020).

9. Uber to pay 148 million in settlement over 2016 data breach. Kyiv. Available at: https://www.bloomberg.com/news/articles/2018-09-26/uber-to-pay-148-million-in-settlement-over-2016-data-breach (accessed 22 August 2020).

10. British Airways faces record $230 million fine over data theft. Kyiv. Available at: https://www.reuters.com/article/us-iag-cybercrime-ico/british-airways-faces-record-230-million-fine-over-data-theft-idUSKCN1U30KD (accessed 22 August 2020).

11. Equifax exposed $150 million Americans personal data. Kyiv. Available at: https://edition.cnn.com/2019/07/22/tech/equifax-hack-ftc/index.html (accessed 22 August 2020).

12. FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook. Kyiv. Available at: https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions (accessed 22 August 2020).

E-mail: inovoitenko@ukr.net