2. Gottsegen G. Cloud Computing & Education. URL: https://builtin.com/cloud-computing/cloud-computing-and-education
3. The Main Benefits & Challenges of Cloud Computing in Education. URL: https://www.buchanan.com/benefits-cloud-computing-education/
4. Riddle J. Cloud Technologies in the Education System. URL: https://www.computer.org/publications/tech-news/build-your-career/cloud-technologies-in-the-education-system

Ключові слова: хмарні технології, хмарні послуги, хмарні сервіси, хмарне програмне забезпечення, онлайн-курси, онлайн-навчання.
Ключевые слова: облачные технологии, облачные сервисы, облачное программное обеспечение, онлайн-курсы, онлайн-обучение.
Key words: cloud technologies, cloud services, cloud software, online courses, online learning.

ЗАДЕРЕЙКО ОЛЕКСАНДР ВЛАДИСЛАВОВИЧ

Національний університет «Одеська юридична академія»,
доцент кафедри інформаційних технологій, кандидат технічних наук

МОДЕЛЬ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У ЄС

У травні 2018 року Європейський Союз (ЄС) переключився на оновлені правила обробки персональних даних, що були встановлені Загальним регламентом щодо захисту даних (Регламент ЄС 2016/679 від 27 квітня 2016 року або GDPR – General Data Protection Regulation) [1]. Даний регламент має пряму дію в усіх 28 країнах ЄС. Важливим нюансом GDPR є екстериторіальний принцип дії нових європейських правил обробки персональних даних.

Новий регламент надає резидентам ЄС інструменти для повного контролю над своїми персональними даними. З травня 2018 року посилилась відповідальність за порушення правил обробки персональних даних: по GDPR штрафи сягають 20 мільйонів євро або 4 % річного доходу суб'єкту бізнесу.

Термінологія, яка використовується в GDPR

Персональні дані (ПД) – будь-яка інформація, що відноситься до фізичної особи або «суб'єкту даних», яка може бути використана прямо або побічно для визначення фізичної особи:

- відбитки пальців, генетичні дані, біометричні дані, расова приналежність;
- інформація про будинок і роботу;
- сексуальна орієнтація і відомості про особисте життя;
- медичні записи, інформація про здоров'я;
- дані про сім'ю: релігійні погляди, філософські погляди;
- час проводження і хобі;
- політичні погляди;

- інтереси, захоплення;
- історія подорожей і дані про місцезнаходження;
- фінансова інформація;
- членство в профспілці;
- поведінкові моделі, які використовуються пристроєм.

Обробка ПД – будь-яка дія, що здійснюється з ПД з використанням або без використання засобів автоматизації, включаючи збір, запис, організацію, структурування, збереження, адаптацію або зміну, відновлення, консультацію, використання, розкриття при передачі, поширенні або забезпеченні доступності, угруповання або комбінацію, обмеження, стирання або знищення.

Суб'єкти ПД в ЄС – суб'єкти ПД, що знаходяться на території ЄС, наприклад, громадяни ЄС, резиденти ЄС, суб'єкти, які перебувають в ЄС на підставі віз, біженці.

Оператор ПД – фізична або юридична особа, державний орган, установа або інша особа, самостійно або спільно з іншими особами визначає мету та засоби обробки ПД.

Оброблювач ПД – фізична або юридична особа, державний орган, установа або інша особа, що обробляє ПД від імені оператора ПД.

Моніторінг може включати: – відстеження резидента ЄС в Інтернет; – використання методів обробки даних для профілювання окремих осіб, їх поведінки або їх відношення до чого-небудь (наприклад, для аналізу або прогнозування особистих переваг).

GDPR має екстериторіальну дію і застосовується до всіх компаній, які обробляють ПД резидентів і громадян ЄС, незалежно від місцезнаходження такої компанії. Філії, представництва іноземних організацій на території ЄС повинні будуть відповідати новим вимогам.

Принципи обробки даних по GDPR

Загальний підхід до обробки ПД сформульовано у вигляді наступних принципів:

1) законність, справедливість і прозорість;
2) обмеження мети;
3) мінімізація даних;
4) точність;
5) обмеження зберігання;
6) цілісність і конфіденційність;

Права суб'єкта даних (фізичної особи)

GDPR значно розширює права громадян і резидентів ЄС з контролю за їх ПД. Європейські користувачі мають право запитувати підтвердження факту обробки їх даних, місце і мету обробки, категорії оброблюваних ПД, яким третім особам ПД розкриваються, період, протягом якого дані будуть оброблятися, а також уточнювати джерело отримання організацією ПД та вимагати їх виправлення. Більш того, користувач має право вимагати припинення обробки своїх даних.

У GDPR також передбачено право на забуття, яке дає громадянам ЄС можливість видаляти свої особисті дані за запитом щоб уникнути їх розповсюдження або передачі третім особам.

Однак, право на забуття поширюється не тільки на пошукові системи. Будь-яка компанія, що обробляє дані, повинна видаляти будь-чиї ПД за запитом, якщо це не суперечить інтересам суспільства або іншим фундаментальним правам громадян ЄС.

Право на переносимість даних

Право на переносимість даних є новацією в правилах обробки даних ЄС. Дане право полягає в тому, що компанії зобов'язані надавати безкоштовно електронну копію ПД іншої компанії на вимогу самого суб'єкта ПД.

Згода на обробку даних

GDPR встановлює високі вимоги щодо форми отримання згоди на обробку ПД. Згода особи на одну обробку її ПД даних має бути виражена у формі затвердження або у формі чітких активних дій користувача. Згода на обробку ПД буде недійсна, якщо у користувача не було вибору або не було можливості відкликати свою згоду без шкоди для самого себе. Якщо особа дала згоду на обробку своїх ПД, контролер повинен мати можливість продемонструвати це.

Згода також не може бути виражена у вигляді мовчання або бездіяльності особи. Інформація про порядок відкликання згоди на обробку ПД повинна бути розміщена таким чином, щоб особа могла легко її знайти.

Особливий захист дітей

Дитячі ПД заслуговують особливого захисту, адже вони менш інформовані про ризики, наслідки, гарантії і їх права щодо обробки ПД. Згода на обробку даних дитини має бути авторизована батьками (або законними представниками дитини). Віковий поріг для батьківської авторизації встановлюється державами-членами ЄС окремо (від 13 до 16 років).

Призначення відповідального за захист персональних даних

Ця вимога стосується компаній, які здійснюють регулярні та систематичні великомасштабні спостереження, моніторинг осіб (вище про нього згадувалося); або які здійснюють великомасштабну обробку спеціальних ПД, наприклад, медичні записи або відомості про кримінальну судимість.

У будь-якому випадку, будь-яка організація може добровільно призначити співробітника щодо захисту даних для управління процесами обробки ПД користувачів і контролю за дотриманням вимог GDPR. У такому випадку компанія повинна опублікувати інформацію про такого співробітника, а також направити її національному регулятору щодо захисту ПД відповідної країни ЄС.

GDPR – найважливіший законодавчий документ, який суттєво підвищує рівень захисту ПД суб'єктів в ЄС і за його межами. Він вимагає дуже уважного дотримання. Таким чином GDPR вносять ясність і послідовність правил, які повинні застосовуватися в області захисту даних на території ЄС. Їх дотримання відновлює довіру користувача-споживача до будь-яких суб'єктів бізнесу що використовують потенціал єдиного європейського цифрового ринку.

Список використаної літератури:

1. Загальний регламент про захист даних (GDPR). [Електронний документ]. – URL: https://gdpr-text.com/ua/
2. Регламент європейського парламенту і ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних. [Електронний документ]. – URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text

Ключові слова: персональні дані, GDPR, захист персональних даних в ЄС.
Ключевые слова: персональные данные, GDPR, защита персональных данных в ЕС.
Key words: personal data, GDPR, personal data protection in the EU.

ЧАНЫШЕВ РАШИД ИБРАГИМОВИЧ

Национальный университет «Одесская юридическая академия»,
доцент кафедры информационных технологий,
кандидат юридических наук, доцент

ВИРУСЫ-ШИФРОВАЛЬЩИКИ (RANSOMWARE), УГРОЗЫ И МЕРЫ ПРОТИВОДЕЙСТВИЯ

Примерно десять лет назад появилась новая разновидность вредоносных компьютерных программ – вирусы-шифровальщики («Ransomware»). Их возникновение стало возможным только после появления криптовалют, так как именно криптовалюты сделали безопасным механизм получения выкупа.

Вирусы-шифровальщики работают следующим образом: на управляющем атакой сервере C&C (Command and Control server) создается пара ключей ассиметричного шифрования. При этом публичный (открытый) ключ встраивается в тело вируса. После заражения вирусом очередного компьютера на управляющем сервере генерируется ключ для симметричного шифрования, с помощью которого происходит шифрование файлов на компьютере – жертве. Передача самого симметричного ключа осуществляется при помощи методов ассиметричного шифрования (например, RSA-256) – симметричный ключ зашифровывается на управляющем сервере с помощью приватного (закрытого) ключа, вирус на атакованном компьютере расшифровывает его с помощью встроенного в него публичного ключа, после чего происходит процесс шифрования.

После окончания шифрования вирус выводит на экран компьютера сообщение с требованием выкупа с оплатой при помощи одной из криптовалют, например биткойна. При этом обычно указывается срок, в течение которого должна быть произведена оплата («счетчик»).