Список використаних джерел

1. http://emsbi.ua/fzp-103-2
2. https://tzi.com.ua/bazalt-31.html
3. https://romsat.ua/products/telecommunication-equipment/ethernet-kommutator-switch/edge-core-ecs4120-28f/
4. https://e.huawei.com/kz/products/enterprise-networking/routers/ar-g3/ar2200

УДК 004.056.5

ДОСЛІДЖЕННЯ СИСТЕМ ЗАХИСТУ БАЗ ДАНИХ

Махняєва К. С., студ. гр КБ-161
Науковий керівник: **Гур'єв В. І.,** к.т.н., доцент
Національний університет «Чернігівська політехніка»

В результаті зростання кількості інформації значними темпами поширюється використання баз даних, а з цим і зростає кількість кіберзлочинців. Кожен день зламується велика кількість баз даних, і часто трапляється, що власник бази даних може не дізнатись, що його база зламана, і з неї іде витік інформації. Ця теза стосується питання про те, як закон про захист даних повинен реагувати на проблеми, що виникають у зв'язку з постійно зростаючою поширеністю великих даних.

Розслідування проводиться на прикладі вивчення поведінкової реклами в Інтернеті (ОВА) і в рамках нормативно-правової бази ЄС про захист даних, особливо Загального регламенту захисту даних (GDPR). Стверджується, що закон про захист даних повинен відповідати на проблеми з великими даними, використовуючи можливості регулювання, які вже існують в поточному правовий режим або потенційно доступні для політиків. З дуже складною, потужною і непрозорою мережею ОВА, як в технічному, так і в економічному плані, використання великих даних може представляти фундаментальну загрозу певним індивідуалістичної, колективним або суспільним цінностям. Незважаючи на обмежене число економічних вигод, таких як безкоштовний доступ до онлайн-сервісів і зростання цифрового ринку, приховані ризики ОВА вимагають ефективного режиму регулювання великих даних. Росс Андерсон часто казав, що по своїй природі більша кількість баз даних ніколи не буде свободна від зловживань в результаті порушень безпеки. Якщо велика система предназначена для полегшення доступу, вона стає небезпечною. Якщо зроблена водонепроникна, стає неможливо використовувати.

Хоча GDPR ЄС являє собою новітню і найбільш всеосяжну правову базу, яка регулює використання персональних даних, він все ще не досяг певних важливих аспектів. Нормативна модель, яка характеризується індивідуальним згодою і перевіркою необхідності, залишається недостатньою для повного захисту суб'єктів даних як автономних осіб, споживачів і громадян в контексті ОВА.

Таким чином, існує нагальна необхідність для політиків переглянути свої інструменти регулювання в світлі потенційних загроз. З одного боку, необхідно переглянути можливості внесення в чорний список або внесення в білий список певних видів використання даних за допомогою механізмів, які або існують в правовій базі, або можуть бути введені додатково. З іншого боку, також необхідно реалізувати весь спектр варіантів політики, які можуть бути прийняті, щоб допомогти людям в прийнятті обґрунтованих рішень в епоху великих даних.

Список використаних джерел

1. Wikipedia Database security [Електронний ресурс]. Режим доступу: URL: https://ru.wikipedia.org/wiki/Database_security – Назва з екрану.
2. Data protection in the age of Big Data [Електронний ресурс]. Режим доступу: URL: https://era.ed

---