Єгор Євсєєв Олексійович,
здобувач (бакалаврського) рівня вищої освіти Вільнюського університет, м. Каунас, Литва
Науковий керівник:
Тарас Гуржій Олександрович,
доктор юридичних наук, професор, завідувач кафедри адміністративного, фінансового та інформаційного права Київського національного торговельно-економічного університету

Витоки даних як порушення права на приватність

Інституціоналізація захисту персональних даних є невід'ємною частиною інформаційного права та одного з основних напрямів національної інформаційної політики, що актуалізує питання вдосконалення її організаційної та законодавчої бази. Передусім стан інформаційної безпеки залежить від її організаційно-правового забезпечення. Розвинена законодавча та адміністративна база оптимізує сферу інформаційних відносин, роблячи її толерантною до внутрішніх і зовнішніх загроз. У свою чергу серйозні законодавчі та організаційні недоліки тягнуть за собою широкий спектр деструктивних наслідків.

Як наголошує професор Т.О.Гуржій: Це підриває інформаційну безпеку, провокує конфлікти, створює передумови для маніпуляцій, зловживань і переслідувань [2, с. 95; 1, с. 16-17]. Очевидно, що ці тенденції зберігатимуться до усунення системних недоліків правового регулювання та організаційного забезпечення захисту персональних даних. Це зумовлює необхідність комплексного вдосконалення законодавчого та організаційного забезпечення захисту персональних даних, що базується на досягненнях сучасної науки, прогресивних тенденціях законотворчості та правозастосування, кращому управлінському досвіді у сфері інформаційної безпеки та захисту персональних даних [3, с. 138].

Щоб запобігти порушенням обмежень щодо конфіденційності, у 2018 році Європейський Союз запровадив жорстке та комплексне регулювання обробки персональних даних – Загальний регламент захисту даних (скорочено GDPR).

Регламент заохочує ефективний захист персональних даних у всьому світі. Сьогодні, щоб відповідати GDPR, будь-яка фірма, яка обробляє дані жителів ЄС, повинна мати чітку стратегію та вживати кількох запобіжних заходів для збереження конфіденційності персональних даних.

Нові правила не лише встановлюють зобов'язання, яких має дотримуватися кожен, але й підтримують компанії, пропонуючи спеціальні угоди про умовне депонування, щоб полегшити перехід до стандартів GDPR.

У GDPR відсутній найпримітивніший засіб безпеки – безпека програмного забезпечення. Компанії з обробки даних не потребують захисту своїх систем від кібератак. Зокрема, речення в розділі «Дизайн конфіденційності» розділу «Ключові питання»: «Законодавство повністю відкрите для того, які засоби захисту повинні бути на місці». Поради GDPR організаціям щодо

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Gurzhii T. Freedom of thought vs. national security interests: the issues of hybrid warfare in Ukraine. Polityka i Społeczeństwo. 2019. №1 (17). P. 94-102.
Гуржій Т. Інформаційне право: виклики гібридної війни. Зовнішня торгівля: економіка, фінанси, право. 2018. № 4. С. 16–26.
Gurzhii T., Gurzhii A., Seliukov V. Public administration of personal data protection in modern Ukraine. Politické vedy. 2018. №2. P.138-158. DOI: http://dx.doi.org/10.24040/politickevedy.2018.21.2.138-158
General Data Protection Regulation(GDPR): REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016. (Дата звернення: 09.11.2022)
IBM "Cost of a data breach 2022" report. Portal of one of biggest technology producing company in the world IBM. URL: https://www.ibm.com/reports/data-breach (Дата звернення: 09.11.2022)
Cyber Security standard ISO/IEC 27001:2022. URL: https://www.iso.org/isoiec-27001-information-security.html (Дата звернення: 09.11.2022)
Cyber Security standard SOC 2 | ISAE 3000. URL: https://www.imperva.com/learn/data-security/soc-2-compliance/ (Дата звернення: 09.11.2022).

захисту даних: Пункт 78 рекомендує, щоб «заходи впровадження, зокрема, відповідали принципам захисту даних за проектом і захисту даних за замовчуванням». Конфіденційність за проектом і конфіденційність за замовчуванням є системним підходом до проектування, який вимагає захисту даних під час розробки системи. Однак, вони не були впроваджені в практичне використання більше 4 років або з моменту прийняття регуляторного підходу і не містять жодних програмних вимог.

Принципи кібербезпеки – Стаття 32 [4] «Безпека обробки» містить основні принципи кібербезпеки, такі як шифрування, мінімізація даних або анонімізація даних, знову ж таки уникаючи будь-яких вимог до програмного забезпечення, які необхідно враховувати. Звичайно, в сучасних умовах широкомасштабної війни в кіберпросторі такий захід є недоречним.

З точки зору GDPR, шифрування є основним заходом кібербезпеки. Однак якщо ви заглибитеся в деталі, то побачите, що GDPR не передбачає конкретних алгоритмів шифрування та їх версій. Тому мені спало на думку риторичне запитання – навіщо компанії впроваджувати сучасне шифрування, якщо немає фінансової вигоди чи юридичного зобов'язання? Однак навіть із сучасним шифруванням дані все ще не захищені без інших програмних механізмів захисту.

Нездатність GDPR запровадити необхідні заходи захисту програмного забезпечення мала серйозні наслідки. Звіт IBM [5, с. 3-7] показує, що середня вартість витоку даних у 2022 році досягла рекордного рівня в 4,3 мільйона доларів, що на 12,7% більше, ніж у звіті 2020 року. Крім того, 83% організацій зазнали принаймні одного порушення безпеки даних. За даними Flashpoint State of Data Breach Intelligence, загальна кількість відкритих записів у першій половині 2022 року сягне 1,4 мільярда, причому принаймні 60% порушень, як повідомляється, пов'язані з несанкціонованим доступом або зломом систем через відсутність безпеки програмного забезпечення.

Нещодавній витік особистої інформації понад 100 мільйонів записів стався з T-Mobile, однією з найбільших телекомунікаційних компаній у світі. 76 мільйонів людей постраждали. Дані були розкриті, навіть в той час як організація відповідала вимогам GDPR.

Щоб зберегти конфіденційність жителів ЄС, важливо обмежити кількість порушень безпеки даних і, як наслідок, кількість витоків особистої інформації. Тому, передусім, GDPR має приділяти фінансування сектору кібербезпеки та приділяти менше уваги правовим питанням.

По-друге, це передбачає впровадження принаймні мінімальних стандартів безпеки програмного забезпечення, яких має дотримуватися закон. Правила не працюватимуть, оскільки, як уже згадувалося, не буде фінансового чи правового стимулу для підприємств забезпечувати належний захист даних. Системи ідентифікації загроз, моніторингу безпеки та виявлення вторгнень можна вважати програмними зобов'язаннями. Будь-яка компанія, яка обробляє персональні дані, повинна мати ці системи. Великі організації слід змусити застосовувати сучасні стандарти безпеки, такі як ISO 27001 [6] або SOC 2 [7], якщо вони обробляють конфіденційні дані в галузі охорони здоров'я, фінансах, освіті чи інших секторах. На цих двох стандартах ґрунтуються два найбільш часто використовувані методи для визначення того, чи створила компанія систему управління інформаційною безпекою (ISMS), здатну захищати конфіденційні дані. Оскільки існують різні стандарти для вибору, давайте залишимо це рішення в повітрі.

Крім того, GDPR впливає на український бізнес. GDPR поширюється на такі операції, якщо компанія зареєстрована в ЄС або збирає персональні дані осіб ЄС. Також, GDPR – це не далеке майбутнє для нашої країни, яка взяла курс на євроінтеграцію, і потребує законодавчої підготовки, оскільки, якщо Україна приєднається до ЄС, це правило одразу почне поширюватися на всі українські фірми. Крім того, GDPR має стати наріжним каменем політики захисту персональних даних, щоб гарантувати безпеку інформації, що належить нашим громадянам, протягом усього гібридного конфлікту, який також вирує в кіберпросторі. З цього випливає, що принципи захисту даних GDPR мають поступово впроваджуватися в українське законодавство.

Оскільки GDPR є основною політикою захисту даних у світі, надзвичайно важливо створити всі відповідні заходи безпеки, щоб захиститися від витоку даних. GDPR не винен у тому, що відповідної стратегії безпеки не було створено, але оскільки метою регламенту є захист персональних даних, він повинен звернути увагу як на правові питання, так і на питання кібербезпеки та надати пріоритет запобіганню витоку даних.