УДК 004
DOI https://doi.org/10.32838/2663-5941/2021.5/22

Пасєка Н.М.
ДВНЗ «Прикарпатський національний університет імені Василя Стефаника»

Шекета В.І.
Івано-Франківський національний технічний університет нафти і газу

Пасєка М.С.
Івано-Франківський національний технічний університет нафти і газу

Кулинич М.М.
Українська академія друкарства

РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ З ВИКОРИСТАННЯМ СТАНДАРТІВ GRPD ДЛЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

У статті розглядається та оцінюється вплив інформаційних технологій регуляторних вимог загальних правил захисту даних на процес розробки програмного забезпечення в Європейській економічній зоні й інших регіонах. Описані основні зміни, які зазнає цей процес, та як підготуватися до цих змін. Особиста інформація користувача поділяється на загальні й спеціальні категорії. Пояснюються методи й причини, які необхідно використовувати для збору даних, обробки й публікації. Визначено, що обробка персональної інформації відповідно до вимог Загального регламенту захисту даних повинна відповідати таким умовам: законність, обмежена мета, точність використання даних, мінімізація обсягів зберігання та кількості й принципи конфіденційності. Крім того, необхідно забезпечити зберігання даних, щоб запобігти їх витоку за межі організації, яка їх зберігає. На основі досліджень була розроблена й скоригована модель відповідно до потреб індустрії інформаційних технологій для впровадження загальних положень щодо захисту даних у циклі розробки програмного забезпечення. Отриманий перелік рішень, що дозволить розробку програмного забезпечення відповідно до всіх вимог загальних правил захисту даних, і надано бачення необхідних змін у проєкті на етапах збору вимог і розвитку архітектури системи. Це значно зменшує обсяг коштів, необхідних для редагування на наступному етапі розробки. Були виділені спеціальні засоби, які дозволяють шифруванню даних відповідати рівню, передбаченому національним законодавством Європи, і розроблено перелік додаткових інструментів, що повністю відповідають системним вимогам.

Ключові слова: *захист даних, персональні дані, програмне забезпечення, вимоги регуляції, інформаційні технології.*

Постановка проблеми. Процес захисту персональних даних користувачів у наш час набув як ніколи важливо значення, і кожен спеціаліст у сфері інформаційних технологій (далі – IT) уже не може обходитись без відповідних навичок. Недотримання чи порушення захисту особистих даних завжди було причиною неймовірно великої кількості випадків, коли вони потрапляли у відкритий доступ. Цим самим порушували права та свободи людей з якими вони були пов'язані. Через це уже постраждали такі компанії: Adobe, eBay, LinkedIn, H&M, Google, Microsoft та Facebook і понесли за це колосальні матеріальні та, що найбільш відчутно репутаційні збитки. А за деяких випадків, такий як при витоку даних з сайту знайомств, ладні викликати суспільний резонанс. Більше того, зараз через покращення хмарних обчислень та стрімкий розвиток квантових комп'ютерів, що здатні обходити колись надійні механізми захисту даних, питання про забезпечення конфіденційності інформації користувачів, стоїть як ніколи актуально. З цієї причини було вирішено створити спеціальну регуляцію, яка покликана урівноважити права та свободи людей з потребами організацій у їх персональних даних – GDPR (General Data Protection Regulation). Вона представляє собою відносно нову регуляція із захисту персональних даних у межах Європейської Економічної Зони (далі – ЄЕЗ), яка була розроблена, як заміна для попередньої «Директиви про захист персональних даних» у державах-членах ЄС та організаціях які надають там свої послуги. У будь-якому

випадку, бізнес тепер здійснюється переважно у електронному режимі з використанням програмних засобів. Цей фактор, як ніщо інше демонструє необхідність даної регуляції і водночас пришвидшує процес її адаптації у цикл розробки програмного забезпечення (далі – ПЗ).

Аналіз останніх досліджень і публікацій. На тему захисту персональних даних існує дуже багато робіт, які розкривають ті чи інші аспекти цього процесу. Однак не для аналізу безпосереднього чи опосередкованого впливу регуляції GDPR на процес розробки ПЗ, порівняння його з аналогічними законами, на кшталт HIPAA чи CCPA та побудови на основі цього рішень для відповідності процесу розробки програмного забезпечення до даної регуляції наразі немає. Однак, на даний момент, не існує настільки потужного та впливового інструменту на процес розробки програмного забезпечення як GDPR, оскільки він тягне за собою гігантські штрафи та поширюється на дію цілої ЄЕС. Користуючись поточними даними, існує збірка інструкцій та прикладів від Європейської ради захисту даних, раніше відомої як WP29, однак вони не мають моделі впливу на розробку.

Постановка завдання. Є проведення дослідження та аналізу змін які зазнав процес розробки програмного забезпечення після впровадження регуляції GDPR визначених в яких саме ролях може виступати програмний продукт та яке відношення це буде мати до зміненої відповідальності за обробку персональних даних. На основі цього, було створено модель, що забезпечує полегшене та економічно обґрунтоване впровадження дій регуляції у процес розробки ПЗ.

Об'єктом дослідження є виплив який привнесли правила та обмеження регуляції GDPR відносно обробки персональних даних в процесі розробки ПЗ.

Предметом дослідження є вплив регуляції захисту персональних даних GDPR на процес розробки програмних рішень в організаціях до яких вона застосована.

Методи дослідження Для виокремлення нововведень дії регуляції на процес розробки ПЗ було застосовано ізолююче абстрагування, порівняння існуючих рішень в предметній області регуляції захисту даних, використано системний підхід до побудови моделі впровадження цих змін у процес розробки та проведення експерименту його використання на прикладі створення застосунку міжрегіонального рівня для пошуку роботи.

Виклад основного матеріалу дослідження. Регуляція щодо захисту персональних даних включає в себе безліч інформації, щоб врегулювати процеси поводження з конфіденційними даними та забезпечити виконання усіх прав суб'єктів даних. Відповідно, внаслідок введених обмежень процеси поведінки з даними мають змінитись, що потягне за собою зміни у роботі готових програмних рішень цих компаній та, навіть, зміни у самому процесі розробки програмного забезпечення в цілому. У загальних рисах описується процес розробки програмного забезпечення і корективи які дана регуляція внесла у це, включені такі поняття як: складання оцінки впливу на конфіденційність даних (DPIA), внесення у процес розробки заходів планування приведення процесу обробки до GDPR, створення реєстру інцидентів з даними, оповіщення суб'єкта про них чи втрату доступу до даних не пізніше ніж за 72 години. На закінчення тут визначаються процеси погодження користувачів на обробку своїх даних, і які саме зміни вони за собою потягнули у сфері ринку IT. Приклад, сповіщення про використання їх у куках, створення нової позиції DPO, зобов'язання відносно застосування шифрування, використання псевдоанонімізації, забезпечення функціоналу поінформованості користувача.

Головна інформація щодо регуляції GDPR. Регуляція захисту персональних даних була розроблена як еволюцію Директиви із захисту даних, прийнятої ще у 1995 році та представляє його оновлену та адаптовану до сучасних вимог версію. GDPR – складається з 99 статей, які визначають структуру регламенту та покликані покрити головні процеси управління та взаємодії персональної інформацією людей які перебувають у межах Європейської Економічної Зони, а також процесу передачі персональної інформації про них поза її межі. Важливо зазначити, що регламент вступив у законну силу у 2018 році, однак був прийнятий ще у 2016 році. Це пояснюється перш за все, тим що компаніям та організаціям які працюють з персональними даними людей потрібен був час для переходу та адаптацію до нових вимог [1; 2]. Так, наприклад, один лишень процес, збереження інформації в куках зазнав значних змін та покращень, що вилилось у показі спеціальних сповіщень яких, по правилам, має неможливо бути приховати. Також, це було зробленим для того щоб організації могли ідентифікувати шляхи взаємодії та підготуватись до зміни у роботі їх продуктів. Одним з найважливіших та найбільш незрозумілих понять GDPR, а радше сказати сильно відносних, є термін територіального покриття цієї регуляцією. У більшості простих користувачів або ж

людей які не взаємодіють з GDPR на регулярній основі виникає велика кількість питань та непорозумінь пов'язаних саме з територіальною відповідністю певних організацій до вимог регуляції [3; 4]. Справді, будь-яка організація яка фізично або ж через якесь представництво розташована на території ЄЕЗ підпадає під дію регуляції, однак, якщо вона надає свої послуги натуральним особам, про яких буде написано згодом, які на момент використання їх продукту перебували на цій території – то така організація також повинна підпадати під цю регуляцію. Що це означає на практиці? Насамперед те, що компанії мають не обов'язково фізично розташовуватись в Європейському Союзі, а достатньо просто надавати послуги людям які там знаходяться для того щоб у них застосовувати усі обмеження та вимоги регуляції щодо захисту даних.

Головні терміни та поняття регуляції. Для того, щоб добре зрозуміти суть регуляції та її потенційний вплив, необхідно в першу чергу, зрозуміти її ключові поняття та оперування ними. Оскільки, ця регуляції містить безліч юридичних термінів та незрозумілих на перший погляд понять, тут представлені частково пояснені та адаптовані під розуміння IT – спеціалізації поняття, а саме: «Персональні дані», «Натуральна особа», «Процес обробки персональних даних», «Обмеження обробки», «Контролер даних», «Обробник персональних даних» [5; 6].

Згідно з регуляцією GDPR, контролер або обробник персональних даних може передати своє представництво іншим юридичним чи фізичним особам, як показано на рис 1.

Це може статися тільки у письмовій формі та за умови створення організації яка буде здійснювати представництво у межах Європейського Союзу чи громадянства фізичної особи-представника у якійсь із цих країн.

Важливим аспектом у регуляції із захисту даних є саме поняття головного закладу організації, який містить:

1. Щодо контролера персональних даних з установами в більш ніж одній державі-члені, місце його центральної адміністрації на території Європейського Союзу, якщо рішення про цілі та способи обробки персональних даних не приймаються в іншому представництві контролера в цій же зоні а також, та остання установа має повноваження реалізовувати такі рішення.

2. Щодо обробки персональних даних з установами в більш ніж одній державі-члені, місця його центральної адміністрації на території Європейського Союзу, або, якщо процесор не має центральної адміністрації в цій же зоні, установи процесора, де основна діяльність з обробки в контекст діяльності установи, що займається обробкою, відбувається в тій мірі, в якій на обробника поширюються конкретні зобов'язання згідно з цим регламентом GDPR.

3. «Підприємство» означає фізичну або юридичну особу, яка здійснює господарську діяльність, незалежно від її юридичної форми, включаючи товариства або асоціації, які регулярно здійснюють господарську діяльність;

4. «Група підприємств» означає контролюючу компанію та її контрольовані підприємства;

5. «Зобов'язуючі корпоративні правила» означають політику захисту персональних даних, якої дотримується контролер або обробник, створений на території держави-члена для передачі або набору передач персональних даних контролеру або обробнику в одній або декількох третіх країнах в межах групи підприємств, що здійснюють спільну господарську діяльність.

Розібравшись із головними поняттями регуляції GDPR, можна рухатись до більш детальних пояснення та глибокого аналізу детальних її аспектів та процесу впливу на розробку програмного забезпечення.

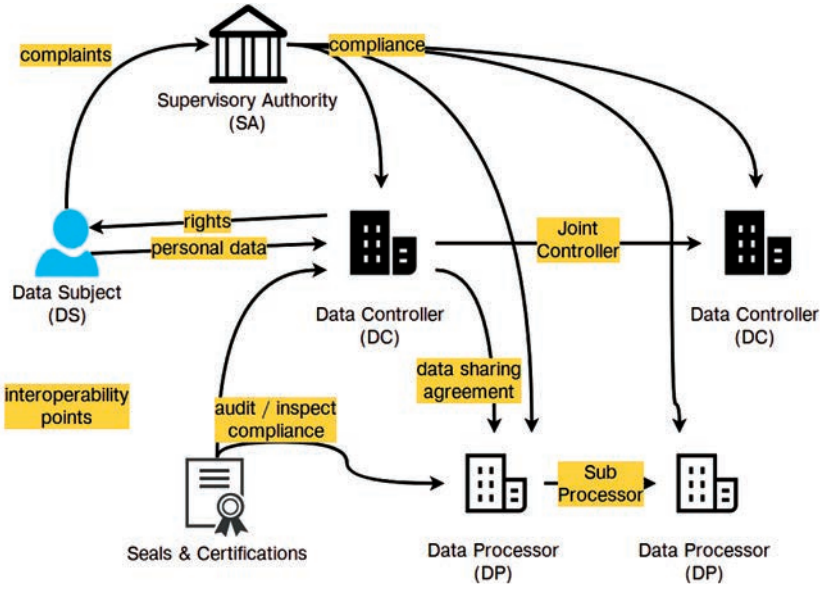

Рис. 1. Зображення позиції контролера даних у процесі їх обробки

Поділ даних системи на спеціальні категорії. Відповідно до обмежень по збору звичайних даних, що саме по собі вимагає згоди особи яку ці дані стосуються, GDPR визначає необхідність визначення ще декілька категорій спеціальних категорій даних і пояснює це тим, що для їх обробки та збір необхідно мати особливий дозвіл. Це пояснюється тим, що існують дані для роботу з якими має бути спеціальна вагома причина. До них відносяться: дані про расове чи етнічне походження, політичні погляди, релігійні чи філософські переконання оскільки саме вони найчастіше стають причиною дискримінації та нерівного поводження у суспільстві [7; 8]. Також сюди відноситься, дані про членство в профспілках, дані що стосуються здоров'я, статеве життя людини, обробка генетичних чи біометричних даних з метою однозначної ідентифікації фізичної особи. Розглянувши та знайшовши більш чіткі визначення про те що саме являють собою біометричні, генетичні чи дані про здоров'я суб'єкта, стає зрозуміло що навіть проста обробка даних трекінгової системи для рейтингової системи з імовірністю уже майже 100% процентів підпадає під це визначення. Цим самим приводячи ці категорії даних до особливої уваги з боку розробників програмного забезпечення під час самостійного аналізу чи виконання вимог від замовника. Оскільки, питання про захист даних стає проблемою усієї організації і вимагає зібраної роботи всіх її підрозділів. Важливо також є розуміти обставини коли з ними чітко та однозначно заборонено працювати, а коли існують виключення цьому процесі для кожного з цих типів: генетичні дані; біометричні дані; дані щодо здоров'я [9].

Проте, існують виключення коли ці дані можуть бути оброблені програмним продуктом без дозволу користувача:

– суб'єкт даних надав явну згоду на обробку його персональних даних для однієї або декількох визначених цілей, за винятком випадків, коли законодавство Європейського Союзу або держави-члена передбачає, що заборона не може бути скасована суб'єктом;

– обробка необхідна для виконання зобов'язань угоди та здійснення конкретних прав контролера або суб'єкта даних у сфері зайнятості або для забезпечення соціально визначених цілей, наскільки це дозволено законодавством ЄС чи держави-члена. Або ж колективний договір відповідно до законодавства держави-члена, передбачає належні гарантії;

– обробка необхідна для захисту життєвих інтересів суб'єкта даних або іншої фізичної особи, коли суб'єкт даних не може дати згоду;

– організація займається тим про що йдеться у цих даних, наприклад: це політична партія або застосунок для визначення серцевої активності протягом дня. Однак тут повинні бути представлені певні гарантійні зобов'язання про нерозголошення цієї інформації;

– обробка стосується персональних даних, які суб'єкт даних явно оприлюднює;

– обробка необхідна для встановлення, здійснення або захисту юридичних вимог або коли суди діють у своєму призначенні;

– обробка необхідна з причин суттєвих суспільних інтересів на основі законодавства ЄС або держави-члена, які повинні бути у відповідності до переслідуваної ними мети, поважати суть права на захист даних та передбачати відповідні та конкретні заходи для захисту основних прав та інтересів суб'єкта цих даних;

– обробка необхідна у медичних цілях для оцінки працездатності працівника, медичного діагнозу, надання медичної чи соціальної допомоги, покращення лікування або управління системами охорони здоров'я, також, так можна робити у зв'язку з договірними зобов'язаннями.

За певних умов обробка спеціальних категорій даних може відбуватись іншою особою, але тільки якщо ця особа є професійним працівником чи дані є під відповідальністю його професійної таємниці. Варто зважати, що держави-члени окрім виконання цих зобов'язань мають, вводити накладати додаткові умови. Тому перед розробкою певного функціоналу варто провести аналіз законодавства у країні використання ПЗ та відредагувати його роботу у відповідність з цими змінами.

Відмінності між даними для ідентифікації та чутливими даними. Дані для ідентифікації персони та персональна інформація суб'єкту даних мають між собою багато спільного, але не є тим самим. Це важливо розуміти у процесі роботи з ними, оскільки відповідно до NIST, дані для ідентифікації особи – це будь-яка інформацію про натуральну живу особу, яка може бути використана для визначення та відслідковування персони цієї особи. До цих даних відноситься : ім'я, номер платника податків, дата або місце роботи, інформація про дівоче ім'я метрі чи біометричні дані а також, будь-яка інша інформація, за допомогою якої можна визначити конкретну особу. У найбільш повному розумінні, тут може виступати будь-що, наприклад : інформація про стан здоров'я, навчання чи фінансовий стан, до якої входять поведінкові звички користувача, переваги під час покупки товарів, дані про расову чи

етнічну приналежність тощо. Регуляція GDPR привносить зміни та доповнення до поняття персональних даних, включаючи до них IP-адресу, дані куків, ідентифікатори пристроїв, та забороняє відслідковування такої інформації без дозволу їх власника. У той самий час у регуляції майже не міститься переліку засобів, якими органи управління організації повинні користуватись для захисту конфіденційних та персональних даних. Відповідно до стандарту ISO 27001, щоб правильно класифікувати інформацію, як просто чутливі дані чи персональну інформацію, необхідно скласти керівні принципи, що пояснюють, як інформація повинна класифікуватися та маркуватися. Ці вказівки повинні описувати, як з ними слід поводитися залежно від їх класифікації, включаючи обмеження доступу, захисту копій, зберігання, розсекречення та знищення. Для більшої ілюстрації усієї важливості цього процесу, відомо що регуляція, навіть, зобов'язує зберігати друковані копії других, у зачиненій під ключ шафці до якої мають мати доступ лишень уповноважений на це персонал. Принцип GDPR щодо обмеження зберігання також вимагає від контролерів або обробників даних встановлення строків обмеження зберігання, а це означає, що конфіденційна особиста інформація не повинна зберігатися довше, ніж це необхідно, і, де це можливо, слід визначати цей періоди зберігання.

Обов'язки системи як контролера чи обробника персональних даних. GDPR приносить нові вимоги які застосовуються напряму до обробника даних, і виділяють його як окремий об'єкт взаємостосунків із зобов'язанням приймати усі заходи щодо її захисту та експорту за межі дії регуляції. Система, яка виступає у ролі обробники даних спільно з їх контролером, мають використовувати усі заходи та міри обережності необхідні для процесу захисту персональних даних відносно до дій GDPR. Обробники також повинні допомагати організаціям, які керують даними з ціллю їх захисту, складання аналізу своїх мір впливу на цілий процес захисту. Наприклад, у випадку виявлення невідповідності процесу система у ролі обробника даних, у відповідності до регуляції GDPR, зобов'язана повідомляти це організацію яка надала їм доступ до даних, відповідно що для цього мають бути присутніми системи аналізу історії змін. Згідно з вимогами дій регуляції, для права обробника на якісь дії з персональними даними необхідно скласти чіткий договір, який буде включати у себе частину яка може містити інструкцію стосовно того як саме ці дані мають бути використаними чи відмову від залучення у цей процес інших обробників. І тут настають вимоги до програмного продукту в плані обліку та аналізу усіх сторонніх сервісів та служб яким надають доступ до отриманих даних. Наприклад, під час логування чи аналізу цієї інформації у стороннього провайдера цих послуг. На відміну від систем-обробників даних, контролери цих даних несуть відповідальність за увесь процес її обробки. Згідно з принципом відповідальності контролери персональних даних (члени процесу які приймають рішення на передачу персональних даних і її причини) повинні не тільки мати у приведені у відповідність до GDPR процеси але і бути готовими це продемонструвати на практиці. Програмні продукти, які виступають у цій ролі, повинні застосувати відповідні технічні та організаційні рішення для захисту персональних даних, включно з впровадження політики цього процесу. У залежності від того яка природа цих даних, їхній контекст та призначення, включно з усіма ризиками, права та свободи їх суб'єктів повинні бути забезпеченими на будь-якому етапі.

Вплив головних принципів GDPR на процес обробки даних. Обробка персональних даних усіма системами загалом, та програмними в особливості, відповідно до регуляції GDPR повинна відбуватись у законній, прозорій, чесній та зрозумілій для користувача формі, яка не порушує права власності суб'єктів даних на їх інформацію. Загалом існує 6 головних принципів у використанні даних: законність; обмеження мети; мінімізація кількості даних; точність їх використання; мінімізація терміну зберігання даних; конфіденційність.

Зміст позиції Data protection officer для розробки ПЗ. Як вказано у попередніх розділах, GDPR має досить чітку та охоплюючу структуру, яка покликана захищати та оберігати права людей відносно їх персональних даних. Однак, просто перерахувати спеціальні пункти та обов'язки організацій є недостатньо для забезпечення виконання цих обов'язків. З цієї та інших причин, включаючи також і складність зміни вимог до ПЗ, було визначено та впровадження нового типу позиції, а саме - службовця з питань захисту даних (Data Protection Officer). Регуляція GDPR визначила особливі випадки коли така позиція є обов'язковою для створення у компанії:

– кількість працівників компанії – понад 50;

– основна діяльність контролера або процесора складається з операцій обробки, які в силу своєї природи, обсягу та цілей вимагають регулярного та систематичного моніторингу. Мають

прямий вплив на життя та діяльність суб'єкта даних;

– компанія в ході своєї роботи займається обробкою персональних даних, що стосуються кримінальних правопорушень суб'єкта даних;

– обробка даних здійснюється державним органом чи іншою компанією, крім суду, яка діє у судовій якості.

Службовець із питань захисту даних призначається на підставі професійних якостей і, зокрема, експертних знань із законодавства та практики захисту даних та здатності виконувати в галузі розробки ПЗ.

Контролер або обробник повинен опублікувати контактні дані працівника з питань захисту даних та повідомити їх контролюючому органу.

Ось головні обов'язки службовця з захисту даних та з описом їх впливу на процес розробки ПЗ:

1. Інформувати та консультувати контролера або обробника та працівників, які здійснюють обробку своїх зобов'язань відповідно до регламенту GDPR чи інших положень про захист персональної інформації, впливати на формування вимог до ПЗ.

2. Контролювати дотримання цього регламенту, інших положень ЄС або держав-членів про захист даних та політику контролера або обробника стосовно захисту персональних даних. Сюди входить розподіл відповідальності, підвищення обізнаності та навчання персоналу залученого до цієї обробки. Відносно до ПЗ, сюди входить процес атестації та перевірки готових частин продукту на відповідність до вимог по захисту даних GDPR.

3. Надавати консультації щодо запитів оцінки впливу на захисту даних, контролювати її ефективність, включно з аналізом даних та пропозицією змін до процесу розробки.

4. Співпрацювати з контролюючим органом.

5. Зберігати таємницю або конфіденційність щодо виконання своїх завдань відповідно до законодавства Союзу або держави-члена.

Під час виконання своїх завдань службовець з питань захисту даних повинен враховувати ризик, пов'язаний з операціями обробки, беручи до уваги характер, обсяг, контекст та цілі обробки. Під час оприлюднення результатів своєї роботи він має напряму звітувати до найвищого рівня керівництва компанії. Службовець з захисту персональних даних займає найнижчу позицію у складовій структурі наглядових позицій відповідно до регуляції. У свою чергу, контролер чи обробник даних відповідають за невтручання у роботу службовця з захисту персональних даних та зобов'язуються виконувати наступні пункти: надавати йому своєчасний та конструктивний доступ до всіх без виключення справ відносно персональних даних клієнтів організації, у випадку з програмним продуктом – даних користувачів; зобов'язуються надавати будь-яку допомогу у процесі виконання службовцем своїх повноважень, а також надавати безперешкодний доступ до персональних даних суб'єктів даних та можливість виконувати операції над ними;

Контролеру чи обробнику даних зі своєї сторони заборонено давати будь-які вказівки чи розпорядження службовцеві з захисту персональних даних щодо його роботи чи будь-яким чином штрафувати за виконання своїх обов'язків. Часто трапляється що службовець із захисту даних відповідає за декілька завдань одночасно, а тому керівництво обробника чи контролера даних повинно пересвідчитись чи не виникне у нього конфлікту інтересів.

З виходом регуляції постала гостра потреба у відповідності роботи ПЗ на території ЄС до вимог GDPR. Оскільки цей процес був доволі багатофазним та включав залучення спеціалістів із декількох галузей було вирішено де-факто перемістити відповідальність за це на Data Protection Officer.

Вплив прав суб'єкта даних на процес розробки програмного забезпечення. Важливою складової цієї регуляції становить визначення об'єктивних прав суб'єкта щодо своїх даних. Найперше виступає право бути проінформованим у прозорій формі про операції які були проведені над особистими даними суб'єкта. Існують наступні визначені права суб'єкта даних відповідно до GDPR: право бути проінформованим; право доступу до своїх даних; право на зміну своїх даних; право бути забутим; право на припинення обробки; право на портативність персональних даних; право на відношення до процесу автоматизованого прийняття рішень та профілювання.

Висновки. У роботі було оцінено інформаційно-технологічний вплив вимог регуляції GDPR процесу розробки програмного забезпечення на території ЄЕЗ та поза її межами. Описано основні зміни яких зазнає цей процес та яким чином потрібно бути до них готовим. Розподілено персональні дані користувачів на звичайні та спеціальні категорії. Пояснено спосіб та причини які необхідно мати для їх збирання, обробки та оприлюднення. Як було з'ясовано для обробки персональної інформації відповідно до GDPR необхідно задовільнять наступні умови: законності, обмеженої мети, , точності використання даних, мінімізації терміну їх зберігання та кількості, принципу конфіденційності. Щоб краще зрозуміти інформаційно-технічний вплив регуляції був проведений порівняльний аналіз із подібними регулюючими актами про захист

даних у медичній сфері. Наведено їх особливості згідно географічного розповсюдження, сфери виливу та обмежень по типу даних відносно до GDPR. Результатом цього стало висвітлення, як переваг так і недоліків. Були знайдені певні недоліки у GDPR у зв'язку з неконкретною позицію щодо питань визначення продажу даних але це пояснюється глобальним охопленням позиції охорони персональних даних. На основі отриманих результатів було складені рішення які покликані полегшити інтеграцію вимог GDPR відповідностей у процес розробки ПЗ на усіх його рівнях. Починаючи зі збору вимог, використовуючи DPIA та data mapping документи, пошук специфікацій щодо доступу до даних у наявних політиках конфіденційності продукту. Представлено також технічні способи досягнення відповідності регуляції, таких як шифрування даних різними алгоритмами, створення псевдоанонімізації та обмеження інформації користувача чи використання надавачів хмарних рішень відповідних до GDPR. Для перевірки та оцінки отриманих методів та алгоритмів у роботі було розроблено тестовий програмний продукт як платформу для пошуку роботи на міжрегіональному рівні. Цей приклад повинний був надати послуги максимально наближені до реальних повсякденних застосунків на ринку але водночас розглянутий із позицій відповідності GDPR.

Список літератури:

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation). OJ 2016 L 119/1. 2016.
2. ISO/IEC 27000 family. Information security management systems. April 2018.
3. Cuevas A., Cabañas J.G., Arrate A., Cuevas R. Does facebook use sensitive data for advertising purposes? W*orldwide analysis and gdpr impact*. 2019.
4. Sourya Joyee De, Abdessamad Imine. On consent in online social networks: Privacy impacts and research directions (short paper). International Conference on Risks and Security of Internet and Systems. 2018. P. 128–135
5. Jayashree Mohan, Melissa Wasserman, Vijay Chidambaram. Analyzing gdpr compliance through the lens of privacy policy. *Heterogeneous Data Management Polystores and Analytics for Healthcare*. 2019. Springer. P. 82–95.
6. Dijana Peras, Renata Mekovec, Ruben Picek. Influence of gdpr on social networks used by omnichannel contact center. *2018 41 st International Convention on Information and Communication Technology Electronics and Microelectronics (MIPRO)*. IEEE. 2018. P. 1132–1137.
7. Yunsen Wang, Alexander Kogan. Designing confidentiality-preserving blockchain-based transaction processing systems. International Journal of Accounting Information Systems. 2018. Vol. 30. P. 1–18.
8. Christopher Millard. Blockchain and law: Incompatible codes? Computer Law & Security Review. 2018. Vol. 34. No. 4. P. 843–846.
9. Dijana Peras, Renata Mekovec, Ruben Picek. Influence of gdpr on social networks used by omnichannel contact center. *2018 41 st International Convention on Information and Communication Technology Electronics and Microelectronics (MIPRO)*. IEEE. 2018. P. 1132–1137.

Pasieka N.M., Sheketa V.I., Pasieka M.S., Kulynych M.M. DEVELOPMENT OF SOFTWARE USING GRPD STANDARDS FOR PERSONAL DATA PROTECTION

This article examines and evaluates the impact of information technology of regulatory requirements of general data protection rules on the process of software development in the European Economic Area and other regions. Describe the main changes that this process entails and how to prepare for these changes. The user's personal information is divided into general and special categories. Explains the methods and reasons that need to be used for their collection, processing and publication. It is stated that the processing of personal information in accordance with the requirements of the General Data Protection Regulation must comply with the following conditions: legality, restricted purpose, accuracy of data use, minimization of storage volumes and quantity, and confidentiality principles. In addition, it is necessary to ensure the preservation of these data to prevent their flow beyond the organization that stores them. On the basis of research was developed and calibrated model in accordance with the needs of the information technology industry for the implementation of general provisions for the protection of data in the software development cycle. Take a list of solutions, allow the software developer to comply with all the requirements of the general data protection rules, and give an idea of the necessary changes in the project during the stages of collecting the requirements and developing the system's architecture. This significantly reduces the amount of costs needed to edit at the next stage of development. Special tools that allow data encryption to meet the level required by the national legislation of Europe were identified and a list of additional tools that fully meet the system requirements was developed.

Key words: *data protection, personal data, software, regulation requirements, information technology.*