УДК 004.056

О.М. ФАЛЬ
Інститут кібернетики імені В.М. Глушкова НАН України, Київ, Україна,
email: *amfall@bigmir.net*.

ДОКУМЕНТАЦІЯ У СТАНДАРТІ ISO/IEC 27701

Анотація. Запропоновано набір можливих документів, які організація повинна розробити і продемонструвати під час проведення процесу сертифікації її системи менеджменту інформаційного прайвесі на відповідність міжнародному стандарту ISO/IEC 27701: 2019 «Методи захисту. Розширення ISO/IEC 27001 та 27002 для менеджменту інформаційного прайвесі. Вимоги та настанови».

Ключові слова: документація, інформаційна безпека, прайвесі, сертифікація, система менеджменту, стандарт.

ВСТУП

У межах спільного технічного комітету зі стандартизації ISO/IEC JTC1 «Інформаційні технології» (Information technology) функціонує підкомітет SC27 «Безпека інформації, кібербезпека та захист прайвесі» (Information security, cybersecurity and privacy protection). До його складу входять п'ять робочих груп, при цьому перша робоча група (РГ1) займається розробленням стандартів у галузі менеджменту інформаційної безпеки, а п'ята робоча група (РГ5) розробляє стандарти, що стосуються захисту прайвесі. Огляд стандартів, що мають стосунок до менеджменту інформаційної безпеки, опубліковано у журналі «Кібернетика та системний аналіз» [1] і процитовано у 47 наукових статтях.

Найбільш затребуваним стандартом у галузі менеджменту інформаційної безпеки є стандарт ISO/IEC 27001 [2], в якому сформульовано вимоги до систем менеджменту інформаційної безпеки (ISMS). Його цінність пояснюється, зокрема, тим, що він є основою для процесу сертифікації ISMS. Поряд з ним є стандарт ISO/IEC 27002 [3], в якому визначено набір заходів щодо забезпечення інформаційної безпеки.

Дотепер аналогічних стандартів в галузі захисту прайвесі не було. Зазначимо, що паралельно з розробленням стандартів у Європейському Союзі створюють законодавчі та нормативні документи, пов'язані із захистом персональних даних. Найбільш значущим документом у цій серії є чинний з травня 2018 року регламент General Data Protection Regulation (GDPR) [4], який на відміну від рекомендацій, викладених у стандартах, є документом прямої дії, що вимагає обов'язкового виконання його положень. Однак, цей документ не пристосований до процесів створення систем сертифікації, що відповідають його вимогам.

Для заповнення утвореної прогалини було розроблено стандарт ISO/IEC 27701 «Методи захисту. Розширення ISO/IEC 27001 та 27002 для менеджменту інформаційного прайвесі. Вимоги та настанови» (Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines) [5].

Стандарт ISO/IEC 27701 складається з двох логічно пов'язаних між собою частин. Перша частина присвячена питанням забезпечення інформаційної безпеки і є адаптацією стандарту ISO/IEC 27001 до систем, які містять і обробляють інформацію, що ідентифікує особу (Personally Identifiable Information — PII).

У цьому стандарті дотримано термінологію, наведену в GDPR. Зокрема, в ньому визначені сторони, дотичні до захисту PII. Ними є PII-контролери, що відповідають перед PII-принципалом, якому належить інформація, за її захист. При цьому PII-процесори обробляють PII за правилами, що визначаються контролером.

Друга частина стандарту значною мірою відображає вимоги, наведені у GDPR, хоч вони й сформульовані у вигляді рекомендацій. Можна сказати, що в ній у найбільш загальному вигляді викладено принципи забезпечення прайвесі, які містять, поміж іншим, права PII-принципалів на дотримання їхнього прайвесі. Комбінація цих двох частин надає змогу сформувати вимоги до узагальненої системи менеджменту, названої у стандарті Privacy Information Management System (PIMS).

Будь-яка система менеджменту містить велику кількість документації, визначеної у тексті відповідного стандарту. Метою цієї статті є викладення у компактному вигляді наведеної у стандарті ISO/IEC 27701 потенційної документації та коротка характеристика її змісту.

У роботах [6, 7] описано різні варіанти документації, передбаченої вимогами стандарту ISO/IEC 27001. Для стандарту ISO/IEC 27701 у мережі Інтернет пропонується на платній основі придбати інструментарій для створення необхідної документації. Згідно з нашим підходом перелік документів, які розробляють для забезпечення процесу сертифікації, є відкритим і його можна адаптувати до контексту організації, для якої здійснюють сертифікацію. В цій статті використано документи [8–12].

ДОКУМЕНТАЦІЯ ДЛЯ PII-КОНТРОЛЕРА

Специфікація цілі

Розділ 7.2.1

Специфікація цілі повинна:

- містити чітке і конкретне формулювання мети, з якою організація збирає PII, і як вона її використовує;
- бути достатньо детальною для того, щоб визначити, який вид оброблення PII передбачений ціллю, а який — ні.
- бути узгодженою з PII-принципалом і відповідати регуляторним вимогам;

Інформація щодо цілі збирання й оброблення PII має бути доведена до відома PII-принципала (наприклад, бути розміщеною у Повідомленні про прайвесі, прийнятому в організації.)

Якщо організація ухвалює нові цілі або змінює початкові, то їх потрібно задокументувати та повідомити зацікавленим сторонам.

Правові підстави для оброблення PII

Розділ 7.2.2

Законність оброблення PII потрібно встановити та підтвердити до початку оброблення PII. Правовими підставами є виконання хоча б однієї зазначеної нижче умови:

- згода PII-принципала;
- виконання контракту;
- відповідність правовим зобов’язанням;
- захист життєвих інтересів PII-принципалів;
- виконання завдання, що здійснюється в суспільних інтересах.

Політика управління згодою

Розділ 7.2.3

Розділ 7.2.4

Розділ 7.2.5

Згідно із законодавством, чинним у сфері захисту прайвесі, в організації може виникнути потреба в отриманні явної згоди PII-принципала на збирання й оброблення PII, що його стосується. Згода вважається наданою лише в тому разі, коли є доказ того, що PII-принципал надав чітке і недвозначне повідомлення про згоду. Згода має бути отримана в результаті самостійної та добровільної дії з боку PII-принципала.

Організація повинна інформувати PII-принципалів про їхні права щодо відкликання згоди. Процес модифікації або відкликання згоди має бути не складнішим, ніж процес її початкового надання. Модифікація згоди може передбачати накладення обмежень на оброблення PII, включаючи заборону на видалення PII (в деяких випадках).

Організація повинна реєструвати будь-який запит на відкликання або модифікацію згоди. Організація має визначити час, потрібний для надання відповіді на запит.

Оцінювання впливу на прайвесі

Розділ 7.2.5

Оброблення PII породжує ризики для PII-принципалів. Ці ризики потрібно проаналізувати шляхом оцінювання їхнього впливу на прайвесі. У деяких юрисдикціях визначені випадки, в яких оцінювання впливу ризиків на прайвесі є обов'язковим (наприклад, використання нових технологій, потенційно високі ризики, великі масиви даних тощо)

Під час оцінювання впливу ризиків на прайвесі слід взяти до уваги такі фактори, як тип оброблюваної PII, місце зберігання PII, місце можливої передачі PII тощо. Результатом проведення аналізу є звіт. Звіт повинен містити такі записи:

- які заходи щодо захисту прайвесі мають бути впроваджені?
- чи кожний ризик є усунутим, зменшеним або прийнятим?
- яким є загальний «залишковий» ризик після впровадження додаткових заходів?

Контракти з PII-процесорами

Розділ 7.2.6

Контролер повинен мати письмовий контракт з кожним використовуваним PII-процесором. Контракти передбачають виконання вимог до PII-процесорів, наведених у додатку B до стандарту.

Контракт має містити положення, що стосуються:

- правил оброблення PII-контролера;
- зобов'язань щодо збереження конфіденційності;
- залучення субпідрядників;
- прав PII-принципалів;
- надання допомоги контролерам у виконанні взятих ними на себе зобов'язань перед PII-принципалом;
- аудиту та інспектування.

Угода між спільними контролерами

Розділ 7.2.7

Угода між спільними контролерами може містити:

- ціль спільного використання PII;
- ідентичності спільних контролерів;
- опис відповідних ролей і відповідальностей;
- відповідальність за імплементацію технічних і організаційних заходів щодо гарантування безпеки для захисту PII;
- визначення відповідальності в разі порушення прайвесі;
- спосіб виконання зобов'язань перед PII-принципалами;
- можливий спосіб отримання PII-принципалами іншої призначеної для них інформації;
- контактну інформацію для зв'язку з PII-принципалами.

Записи, що стосуються оброблення PII

Розділ 7.2.8

Записи повинні охоплювати:

- тип оброблення;
- цілі оброблення;

• категорії PII і PII-принципалів;
• категорії одержувачів, яким буде розкрита PII;
• загальний опис технічних та організаційних заходів щодо забезпечення безпеки;
• звіт щодо оцінювання впливу на прайвесі.

Документація щодо виконання зобов'язань перед PII-принципалами
Розділ 7.3.1

Організація повинна визначити і задокументувати свої правові, регуляторні та ділові зобов'язання перед PII-принципалами, що стосуються оброблення їхньої PII, і забезпечити засоби виконання цих зобов'язань.

Інформація для PII-принципалів
Розділ 7.3.2

Цей розділ охоплює:
• інформацію про ціль оброблення;
• контактну інформацію про PII-контролера;
• правові підстави для оброблення;
• інформацію про те, де отримана PII, якщо вона не отримана безпосередньо від PII-принципала;
• інформацію про зобов'язання перед PII-принципалами;
• інформацію про те, як PII-принципал може відкликати свою згоду;
• інформацію про передачу PII;
• інформацію про одержувача або про категорії одержувачів PII;
• інформацію про період збереження PII;
• інформацію про автоматичне прийняття рішення на основі автоматизованого оброблення PII;
• інформацію про право на оскарження;
• інформацію про частоту надання інформації.

Політика доступу PII-принципалів до своєї інформації
Розділ 7.3.6

PII-принципали мають право отримувати від контролера
• підтвердження того, що він обробляє інформацію PII-принципала;
• копію PII;
• іншу додаткову інформацію, включену в Повідомлення про інформацію, яка передається PII-принципалам.

Політика виправлення PII або її видалення
Розділ 7.3.6

Контролери повинні мати змогу реалізовувати право PII-принципала на виправлення своєї інформації.

Потрібно визначити час відповіді на запит про виправлення PII і необхідно неухильно його дотримуватися.

Потрібно описати ситуації, в яких законодавство забороняє видаляти наявну у контролера інформацію PII-принципала.

Під час реалізації запиту на виправлення контролер повинен мати доказ доцільності цієї операції, який можна використовувати в разі виникнення суперечок між контролером і PII-принципалом.

Політика інформування контролером третіх сторін
Розділ 7.3.7

Контролер повинен інформувати треті сторони, з якими він поділяє PII, про будь-які модифікації або відкликання згоди, а також заборони на оброблення спільних PII.

Контролер повинен визначити і підтримувати в робочому стані канали зв'язку з третіми сторонами.

Під час інформування третіх сторін контролер повинен відслідковувати докази отримання цієї інформації.

Процедура для оброблення запитів від PII-принципалів

Розділ 7.3.9

Потрібно виконати такі кроки:

- переконатися в тому, що отримано запит від PII-принципала;
- перевірити ідентичність PII-принципала;
- зібрати всю необхідну для PII-принципала інформацію;
- надати зібрану інформацію у зручному форматі;
- виконати відповідь протягом заданого проміжку часу.

Політика підтримки точності PII протягом її життєвого циклу

Розділ 7.4.3

Контролери повинні вживати заходів до оновлення і видалення неточної PII. Ці заходи передбачають перевірку точності та повноти PII спільно з PII-принципалом у момент збирання даних (якщо це можливо).

PII-принципали мають право на запит щодо видалення або виправлення неточної PII, яка їх стосується. Контролери повинні виконувати ці запити негайно. Вони також повинні розглядати необхідність періодичного оновлення PII.

Політика досягнення цілей мінімізації PII

Розділ 7.4.4

Організація повинна визначити цілі мінімізації PII і механізми їхнього досягнення. Основними механізмами мінімізації PII є:

- уникнення оброблення PII, якщо це є можливим для відповідної цілі;
- релевантність PII заданому обробленню;
- необхідність PII для конкретних цілей;
- обмеження обсягу PII, що збирається, до меж, необхідних для мінімізації;
- агрегування PII;
- псевдонімізація PII;
- анонімізація PII;
- деідентифікація PII.

Механізми деідентифікації PII

Розділ 7.4.4

Розділ 7.4.5

Деідентифікація — це процес видалення PII із запису або сукупності даних. Деідентифікація, що заснована на ризиках, охоплює обчислення прийнятного рівня ризику реідентифікації. У цьому обчисленні потрібно розглянути цілу низку факторів, включаючи використання моделі порушника. Основними методами деідентифікації є маскування, узагальнення, рандомізація, придушення.

Процедура видалення тимчасових файлів

Розділ 7.4.6

Процедура «збирання сміття» є засобом автоматичного керування пам'яттю. Вона намагається використовувати сміття, тобто пам'ять, зайняту об'єктами, які більше не використовуються програмою. «Збирання сміття» є протилежним ручному керуванню пам'яттю, під час якого потрібно, щоб програміст визначив, які об'єкти перерозподілити і повернути в пам'ять. Так само як інші методи керування пам'яттю, «збирання сміття» займає значну частку загального часу процесингу у програмі і, як результат, може мати значний вплив на продуктивність.

Політика збереження PII

Розділ 7.4.7

У політиці збереження зазначають типи записів і PII, якими організація володіє, для чого вони використовуються, як довго вона збирається їх зберігати. PII слід зберігати лише протягом того проміжку часу, в межах якого вона може знадобитися. Його тривалість залежить від цілей зберігання й оброблення PII. Організація повинна періодично аналізувати збережену PII і видаляти або анонімізувати її, якщо в ній більше не буде потреби. Організація повинна встановити і задокументувати стандартні періоди збереження для різних категорій PII.

Політика видалення PII

Розділ 7.4.8

Вибір методів видалення PII залежить від безлічі факторів, оскільки методи видалення є різними за своїми властивостями і результатами. Цими факторами можуть бути природа й обсяг PII, що підлягає видаленню, наявність пов'язаних з PII метаданих, фізичні характеристики носіїв, на яких PII зберігається.

Підстави для передачі PII між юрисдикціями

Розділ 7.5.1

У разі транскордонної передачі PII використовують такі документи:

У випадку передачі PII всередині групи підприємств виконуються обов'язкові корпоративні правила (BCR), які охоплюють усі загальні принципи захисту даних під час їхньої передачі. Вони повинні бути юридично обов'язковими і здійсненними кожним членом групи компаній.

Європейська комісія уповноважена визнавати Типові положення Договору (MCC).

Транскордонні правила прайвесі (CBPR) є добровільною системою, що слугує для міжнародного визнання в межах APEC.

Перелік країн та міжнародних організацій, яким може бути передана PII

Розділ 7.5.2

Політика збереження періоду записів про передачу PII

Розділ 7.5.3

Під час передачі PII контролером третім сторонам або від третіх сторін контролеру, потрібно вести відповідні записи.

Записи розкриття PII третім сторонам

Розділ 7.5.4

Записи повинні містити такі відомості:

- яка PII була розкрита;
- кому PII була розкрита;
- коли PII була розкрита;
- джерело розкриття;
- джерело уповноваженого органу, що санкціонує розкриття.

ДОКУМЕНТАЦІЯ ДЛЯ PII-ПРОЦЕСОРА

Контракт між процесором і клієнтом

Розділ 8.2.1

Контракт повинен містити положення про:

- прайвесі за замовчуванням і проєктування;
- досягнення безпеки оброблення;
- сповіщення наглядовому органу про порушення безпеки PII;
- повідомлення про порушення PII клієнтам і PII-принципалам;
- проведення PIA (Privacy Impact Assessment);
- забезпечення допомоги процесором, якщо буде потрібно попереднє консультування з відповідними органами захисту PII.

Записи, що стосуються оброблення PII

Розділ 8.2.6

Записи можуть містити:

- категорії оброблення, що виконується за дорученням кожного клієнта;
- інформацію про передавання PII третім країнам або міжнародним організаціям;
- загальний опис технічних та організаційних заходів щодо забезпечення безпеки.

Процедура видалення тимчасових файлів

Розділ 8.4.1

Політика повернення, передачі або знищення PII
Розділ 8.4.2

Правила передачі PII між юрисдикціями
Розділ 8.5.1

ВИСНОВКИ

Під час створення системи менеджменту інформаційного прайвесі доводиться розробляти значну кількість документів, пов'язаних із проєктуванням, упровадженням, функціонуванням цих систем. Посилання на необхідне документування у вигляді правил, керівних вказівок, процедур та інших документів містяться в різних розділах стандарту і часто не підкріплені рекомендаціями щодо їхнього змісту. У статті встановлено відповідність між потенційними документами і тими розділами стандарту, в яких сформульовано вимоги до їхнього розроблення. Наведено перелік питань, що містяться в тих чи інших документах.

СПИСОК ЛІТЕРАТУРИ

1. Фаль А.М. Стандартизация в сфере менеджмента информационной безопасности. *Кибернетика и системный анализ.* 2010. Т. 46, № 3. С. 181–184.
2. ISO/IEC 27001:2013. Information technology — Security techniques — Information security management systems — Requirements. URL: https://www.iso.org/standard/54534.html.
3. ISO/IEC 27002:2013. Information technology — Security techniques — Code of practice for information security controls. URL: https://www.iso.org/standard/54533.html.
4. 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). URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj.
5. ISO/IEC 27701:2019. Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines. URL: https://www.iso.org/standard/71670.html.
6. List of mandatory documents required by ISO 27001 (2013 revision). URL: https://advisera.com/27001academy/knowledgebase-category/iso-27001-implementation/list-of-mandatory-documents-required-by-iso-27001-2013-revision.
7. Best Practice ISO 27001 Required Documentation. URL: https://www.riskmanagementstudio.com/best-practice-iso-27001-required-documentation/.
8. UK Information Commissioner's Office. URL: www.ico.org.uk.
9. European Data Protection Board. URL: www.edpb.europa.eu/edpb_en.
10. 17/EN WP 248rev.1 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. URL: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/20171013_wp248_ rev01_enpdf.pdf.
11. EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default adopted on 13 November 2019. URL: https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf.
12. NIST Internal Report (NISTIR), 8053, De-Identification of Personal Information. URL: https:// nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf.

O.M. Fal'

DOCUMENTATION IN ISO/IEC 27701 STANDARD

Abstract. The author proposes a set of possible documents that an organization must develop and demonstrate during the certification of its information privacy management system for compliance with the international standard ISO/IEC 27701: 2019 "Security techniques. Extension to ISO/IEC 27001 and 27002 for privacy information management – Requirements and guidelines."

Keywords: certification, documentation, information security, management system, privacy, standard.

Надійшла до редакції 27.07.2020