Додаток №5 до наказу № 03-ПДн від _ _ _ листопада 2018

ПОЛОЖЕННЯ
ПРО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ
ПЕРСОНАЛЬНИХ ДАНИХ

м. Київ, 2020 р.

зміст

* Терміни та скорочення

* Персональні дані (ПДн) – будь-яка інформація, що відноситься до прямо або побічно визначеному або визначається фізичній особі (суб'єкту персональних даних).

* Оператор-державний орган, муніципальний орган, юридична або фізична особа, самостійно або спільно з іншими особами організуючі і (або) здійснюють обробку персональних даних, а також визначають цілі обробки персональних даних, склад персональних даних, що підлягають обробці, дії (операції), що здійснюються з персональними даними.

* Обробка персональних даних - будь-яка дія (операція) або сукупність дій (операцій), що здійснюються з використанням засобів автоматизації або без використання таких засобів з персональними даними, включаючи збір, запис, систематизацію, накопичення, зберігання, уточнення (оновлення, зміна), Витяг, використання, передачу (поширення, надання, доступ), знеособлення, блокування, видалення, знищення персональних даних.

* Автоматизована обробка персональних даних-обробка персональних даних за допомогою засобів обчислювальної техніки.

* Поширення персональних даних-дії, спрямовані на розкриття персональних даних невизначеному колу осіб.

* Надання персональних даних-дії, спрямовані на розкриття персональних даних певній особі або певному колу осіб.

* Блокування персональних даних-тимчасове припинення обробки персональних даних (за винятком випадків, якщо обробка необхідна для уточнення персональних даних).

* Знищення персональних даних-дії, в результаті яких стає неможливим відновити зміст персональних даних в інформаційній системі персональних даних і (або) в результаті яких знищуються матеріальні носії персональних даних.

* Знеособлення персональних даних-дії, в результаті яких стає неможливим без використання додаткової інформації визначити приналежність персональних даних конкретному суб'єкту персональних даних.

* Інформаційна система персональних даних (Іспдн) – сукупність містяться в базах даних персональних даних і забезпечують їх обробку інформаційних технологій і технічних засобів.

* Транскордонна передача персональних даних-передача персональних даних на територію іноземної держави органу влади іноземної держави, іноземній фізичній особі або іноземній юридичній особі.

- Галузь застосування

* Положення про забезпечення безпеки персональних даних (далі – Положення) розроблено з метою виконання вимог законодавства України в галузі захисту персональних даних.

* Це Положення визначає порядок і правила організації та проведення робіт із забезпечення безпеки персональних даних (далі – Оператор).

* Цей документ враховує положення основних нормативних правових актів у галузі захисту персональних даних, перелічених у Положенні про Комісію з приведення у відповідність до вимог законодавства в галузі персональних даних.

* Це положення призначене для всіх працівників Оператора, а також третіх осіб, які отримують тимчасовий або постійний доступ до оброблюваних у нього ПДн на законній підставі.

* Це положення діє з моменту його затвердження керівником Оператора.

* Актуалізація цього Положення проводиться не рідше, ніж два рази на рік відповідно до регламенту з проведення контрольних заходів та реагування на інциденти інформаційної безпеки

* Внесення змін до цього Положення або затвердження його нової редакції проводиться на підставі відповідного наказу керівника Оператора.

* Загальні положення

* ПДн, оброблювані у Оператора, цілі, підстава і терміни їх обробки вказані в переліку оброблюваних персональних даних.

* Обробка ПДн здійснюється Оператором з використанням засобів автоматизації і без їх використання.

* Строки зберігання ПДн встановлюються у письмовій згоді суб'єкта ПДн на обробку його персональних даних, а також вимогами законодавства України, що встановлюють строки зберігання документів.

* Організація робіт із забезпечення безпеки персональних даних

* Під організацією робіт із забезпечення безпеки ПДн розуміється формування і всебічне забезпечення реалізації сукупності узгоджених за метою, завданням, місцем і часом організаційних і технічних заходів, спрямованих на мінімізацію як безпосереднього, так і опосередкованого збитку від реалізації загроз безпеки ПДн, і здійснюваних з метою:

* запобігання можливих (потенційних) загроз безпеці ПДн;

* нейтралізації та / або парирування реалізованих загроз безпеки ПДн;

* ліквідації наслідків реалізації загроз безпеці ПДн.

* Організація робіт із забезпечення безпеки ПДн у Оператора повинна здійснюватися відповідно до чинних нормативних правових актів і розроблених для цих цілей організаційно-розпорядчими документами щодо забезпечення безпеки ПДн Оператором.

* Завдання щодо приведення діяльності Оператора у відповідність до вимог законодавства України в галузі ПДн покладаються на спеціально створювану для цих цілей комісію та осіб, відповідальних за організацію обробки та забезпечення безпеки ПДн, які можуть бути включені до складу даної комісії.

• У випадках, коли Оператор на підставі договору доручає обробку ПДн третій особі, Оператору необхідно укласти з даною особою угоду про дотримання безпеки персональних даних, з покладанням на третю особу обов'язки щодо забезпечення конфіденційності та безпеки переданих Оператором ПДн (або включити дане зобов'язання в укладається/діючий договір).

* Роботи з приведення діяльності Оператора у відповідність до вимог законодавства України ведуться за двома напрямками: забезпечення безпеки ПДн, оброблюваних без використання засобів автоматизації, і забезпечення безпеки ПДн в Іспдн Оператора.

* Роботи із забезпечення безпеки ПДн, оброблюваних без використання засобів автоматизації, ведуться за наступними напрямками:

* визначення переліку осіб, допущених до обробки ПДн;

* визначення приміщень, в яких обробляються персональні дані;

* інформування працівників Оператора про встановлені правила обробки ПДн і вимог щодо їх захисту, підвищення обізнаності в питаннях забезпечення безпеки ПДн;

* облік і захист носіїв ПДн;

* розмежування доступу до носіїв ПДн;

* знищення ПДн.

* Організація і виконання заходів щодо забезпечення безпеки ПДн, оброблюваних в Іспдн Оператора, здійснюються в рамках системи захисту персональних даних Іспдн (далі-СЗПДн), що розгортається в Іспдн в процесі її створення або модернізації.

* СЗПДн являє собою сукупність організаційних заходів і технічних засобів захисту інформації, а також використовуваних в Іспдн інформаційних технологій, що функціонують відповідно до визначених цілей і завдань забезпечення безпеки ПДн.

* СЗПДн повинна бути невід'ємною складовою частиною кожної новоствореної Іспдн Оператора.

* Для існуючих Іспдн, в яких в процесі їх створення не були передбачені заходи щодо забезпечення безпеки ПДн повинен бути проведений комплекс організаційних і технічних заходів з розробки та впровадження СЗПДн.

* Структура, склад і основні функції СЗПДн визначаються відповідно до рівня захищеності персональних даних, оброблюваних в Іспдн і моделлю загроз безпеки персональних даних при їх обробці в Іспдн.

* Проведення робіт із забезпечення безпеки персональних даних

* З метою оцінки рівня захищеності оброблюваних у Оператора ПДн і своєчасного усунення невідповідностей вимогам законодавства України в галузі захисту ПДн у Оператора раз на рік повинен проводитися аналіз змін процесів захисту ПДн.

* Аналіз змін проводиться за такими основними напрямками:

* перелік працівників і третіх осіб, допущених в обробці ПДн, ступінь їх участі в обробці ПДн і характер взаємодії між собою;

* перелік приміщень, в яких обробляються персональні дані;

* перелік і обсяг оброблюваних ПДн;

* цілі обробки ПДн;

* процедури збору, запису, систематизації, накопичення, зберігання ,уточнення(оновлення, зміни), вилучення, використання, передачі (поширення, надання, доступу), знеособлення, блокування, видалення і знищення ПДн;

* способи обробки ПДн (автоматизована, неавтоматизована);

* перелік уповноважених органів, в рамках відносин з якими здійснюється обробка ПДн;

* перелік програмно-технічних засобів, що використовуються для обробки ПДн;

* конфігурація і топологія Іспдн в цілому і її окремих компонент, фізичні, функціональні і технологічні зв'язки як всередині цих систем, так і з іншими системами різного рівня і призначення;

* способи фізичного підключення та логічної взаємодії компонент Іспдн, способи підключення до мереж зв'язку загального користування та міжнародного інформаційного обміну з визначенням пропускної здатності ліній зв'язку;

* режими обробки ПДн в Іспдн в цілому і в окремих компонентах;

* склад використовуваного комплексу засобів захисту ПДн і механізмів ідентифікації, аутентифікації та розмежування прав доступу користувачів Іспдн на рівні операційних систем, баз даних і прикладного програмного забезпечення;

* перелік організаційно-розпорядчої документації, що визначає порядок обробки та захисту ПДн у Оператора;