Державна служба статистики України

ЗАТВЕРДЖЕНО

Наказ Державної служби
статистики України
15.02.2017 № 41

МЕТОДОЛОГІЧНІ ПОЛОЖЕННЯ ЩОДО ЗАБЕЗПЕЧЕННЯ СТАТИСТИЧНОЇ КОНФІДЕНЦІЙНОСТІ В ОРГАНАХ ДЕРЖАВНОЇ СТАТИСТИКИ

Київ – 2017

Державна служба статистики України

Методологічні положення щодо забезпечення статистичної конфіденційності в органах державної статистики (далі – Методологічні положення) визначають основні принципи та методи забезпечення статистичної конфіденційності в органах державної статистики та призначені для використання працівниками органів державної статистики.

Методологічні положення схвалені Комісією з питань забезпечення конфіденційності статистичної інформації Держстату (протокол від 24.01.2017 № 1) та Комісією з питань удосконалення методології та звітної документації Держстату (протокол від 15.02.2017 № 2).

Державна служба статистики України
- адреса: вул. Шота Руставелі, 3, м. Київ, 01601
- телефон: (044) 287-24-22
- факс: (044) 235-37-39
- електронна пошта: office@ukrstat.gov.ua
- веб-сайт: www.ukrstat.gov.ua

Зміст

Перелік скорочень

ІТС – інформаційно-телекомунікаційна система органів державної статистики.
СЗІ – служба захисту інформації органів державної статистики.

І. Загальні положення

1. Ці методологічні положення:

розроблені відповідно до законів України "Про державну статистику", "Про інформацію", "Про захист персональних даних", "Про доступ до публічної інформації", "Про захист інформації в інформаційно-телекомунікаційних системах", постанови Кабінету Міністрів України від 29.03.2006 № 373 "Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах" та інших нормативно-правових актів, які регулюють питання конфіденційності, і з урахуванням визначень, понять, термінів, наведених у глосарії до плану статистичного спостереження, затвердженому наказом Держкомстату від 29.12.2009 № 498;

спрямовані на дотримання Принципів діяльності органів державної статистики, затверджених наказом Держкомстату України від 14.06.2010 № 216, та виконання Концепції забезпечення статистичної конфіденційності, затвердженої наказом Держстату від 28.07.2015 № 180;

базуються на Основних принципах офіційної статистики, схвалених Генеральною Асамблеєю ООН 23.01.2014, принципах Кодексу норм європейської статистики, прийнятих Комітетом статистичних програм 28.09.2011, положеннях Регламенту (ЄС) № 223/2009 Європейського парламенту та Ради від 11.03.2009, Регламенту Комісії (ЄС) № 557/2013 від 17.06.2013, Рішенні Комісії (ЄС) С(2006) 3602 від 16.08.2006.

2. Захист даних відіграє дуже важливу роль у виробництві статистичної інформації. Забезпечення статистичної конфіденційності є одним із основних принципів діяльності органів державної статистики.

3. Методологічні положення розроблені з метою визначення основних принципів та методів забезпечення статистичної конфіденційності в органах державної статистики згідно з нормами законодавства.

4. Методологічні положення призначені для внутрішнього використання працівниками органів державної статистики, які на постійній або тимчасовій основі беруть участь у проведенні державних статистичних спостережень.

ІІ. Основні поняття та терміни

Для цілей цих Методологічних положень використовуються такі визначення понять і термінів:

виробництво статистичної інформації – усі заходи, що стосуються збирання, зберігання, оброблення та аналізу, необхідні для складання статистичної інформації;

доступ до інформації – можливість одержання, оброблення, блокування

та/чи порушення цілісності інформації;

доступність – властивість інформації бути захищеною від несанкціонованого блокування (інформація зберігає доступність, якщо підтримується можливість отримати її упродовж будь-якого задовільного проміжку часу);

забезпечення статистичної конфіденційності – комплекс заходів, спрямованих на захист конфіденційних статистичних даних;

захист інформації в інформаційно-телекомунікаційній системі – діяльність, спрямована на запобігання або ускладнення реалізації несанкціонованих дій щодо інформації, що міститься в ІТС;

зовнішній користувач – фізична або юридична особа, яка в установленому законодавством порядку отримала право тимчасового доступу на певний проміжок часу до інформації, що міститься в ІТС;

інформаційна (автоматизована) система – організаційно-технічна система, що реалізує певну технологію обробки статистичних даних із використанням відповідних технічних і програмних засобів;

інформаційно-телекомунікаційна система – сукупність інформаційних (автоматизованих) і телекомунікаційних систем, які у процесі обробки статистичних даних діють як єдине ціле та поєднують у собі обчислювальну систему, фізичне середовище, користувачів і оброблювану інформацію;

конфіденційні статистичні дані – дані, що дозволяють установити конкретну статистичну одиницю та визначити первинні дані щодо неї;

комплексна система захисту інформації – сукупність організаційних і технічних заходів, засобів і методів, які забезпечують захист інформації в інформаційно-телекомунікаційній системі;

конфіденційність – властивість інформації бути захищеною від несанкціонованого ознайомлення (інформація зберігає конфіденційність, якщо дотримуються встановлені правила ознайомлення з нею);

користувач ІТС – працівники органів державної статистики (в тому числі фізичні особи на підставі цивільно-правових угод), які на постійній або тимчасовій основі беруть участь у проведенні статистичних спостережень та допущені в установленому порядку до робіт в ІТС;

несанкціонований доступ – дії з метою одержання доступу до інформації незаконним протиправним шляхом з порушенням установленого порядку та/або правових норм;

первинні статистичні показники визначаються шляхом зведення та групування даних і подаються у формі абсолютних величин;

похідні статистичні показники обчислюються на базі первинних показників і мають форму середніх чи відносних показників;

статистична конфіденційність – це гарантія захисту конфіденційних статистичних даних, унеможливлення їх використання у нестатистичних цілях та ідентифікації зовнішніми суб'єктами при її поширенні, крім випадків, передбачених законодавством;

статистична одиниця – одиниця, щодо якої отримують інформацію в ході

статистичного спостереження;

статистичні дані – інформація, отримана на підставі проведених статистичних спостережень, що опрацьована і подана у формалізованому вигляді відповідно до загальноприйнятих принципів та методології;

телекомунікаційна система – сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб;

цілісність – властивість інформації бути захищеною від несанкціонованого або випадкового спотворення, руйнування або знищення та бути незмінною в процесі її передавання або зберігання (інформація зберігає цілісність, якщо дотримуються встановлені правила її модифікації та знищення).

III. Типологія даних у процесі виробництва статистичної інформації

Дані, що їх використовують органи державної статистики у процесі виробництва статистичної інформації, поділяються на три види: вхідні дані; дані, що обробляються; та дані, що поширюються (оприлюднюються), і для цілей цих Методологічних положень вони вживаються в наведених нижче значеннях.

1. Вхідні дані

До вхідних даних належать первинні дані, адміністративні дані та інші дані.

1. Первинні дані – інформація щодо кількісної та якісної характеристики явищ і процесів, яку подали респонденти під час статистичних спостережень. До первинних даних може належати інформація, яка міститься в заповненій формі звітності, анкеті, переписному (опитувальному) листі, інших статистичних формулярах, необхідних для проведення статистичних спостережень.

2. Адміністративні дані – дані, отримані на підставі спостережень, проведених державними органами (за винятком органів державної статистики), органами місцевого самоврядування та іншими юридичними особами відповідно до законодавства та з метою виконання адміністративних обов'язків та завдань, віднесених до їх повноважень. До адміністративних даних належить інформація, що надходить до органів державної статистики відповідно до угод щодо взаємообміну інформаційними ресурсами між Держстатом та іншими державними органами, установами, організаціями.

3. Іншими даними може бути інформація щодо кількісної та якісної

характеристики явищ і процесів, що офіційно надходить до органів державної статистики від міжнародних організацій, інших юридичних або фізичних осіб або взята з інших офіційних джерел.

4. Органи державної статистики після отримання вхідних даних забезпечують їхню статистичну конфіденційність.

2. Дані, що обробляються (статистичні дані)

1. Вхідні дані, які надійшли до органів державної статистики, завантажуються до ІТС, піддаються арифметичному та логічному контролю відповідно до технології обробки та приймають вигляд даних, що обробляються, для подальшого виробництва статистичної інформації органами державної статистики.

2. До даних, що обробляються, можуть належати мікродані й агреговані дані.

3. Мікродані – масив даних, що має певну кількість записів, де кожний запис має свої кількісно-якісні характеристики, ідентифікатори та показники на рівні статистичної одиниці, які можна розділити на чотири основні категорії:

1) прямі ідентифікатори – кількісно-якісні характеристики, які однозначно ідентифікують статистичну одиницю (наприклад, ідентифікаційний код ЄДРПОУ, код і номер паспорта фізичної особи тощо);

2) похідні ідентифікатори – кількісно-якісні характеристики, які ідентифікують статистичну одиницю з певним ступенем однозначності. Однак комбінація похідних ідентифікаторів може визначити статистичну одиницю однозначно (наприклад, назва, адреса, номер телефону тощо);

3) конфіденційні показники – кількісно-якісні характеристики, що містять первинні дані щодо статистичної одиниці, які визначені як конфіденційні у методологічних положеннях відповідних державних статистичних спостережень (наприклад, кількість працівників, професія, етнічне походження (національність) тощо);

4) неконфіденційні показники – усі інші кількісно-якісні характеристики, які не належать до вищезазначених категорій.

Персоніфіковані мікродані поряд із конфіденційними та/або неконфіденційними показниками містять прямі ідентифікатори та/або похідні ідентифікатори.

Знеособлені мікродані не містять прямих та/або похідних

ідентифікаторів.

Анонімні мікродані – знеособлені мікродані, до яких були застосовані окремі методи захисту знеособлених мікроданих відповідно до розділу 4 цих Методологічних положень, з метою мінімізації ризику опосередкованого встановлення конкретної статистичної одиниці.

Кількісні та якісні характеристики щодо статистичної одиниці представляються у вигляді статистичних показників (первинних і похідних) та/або ознак.

4. Агреговані дані – масив даних, що має певну кількість записів, де кожний запис має свої кількісно-якісні характеристики на рівні групи статистичних одиниць.

5. Для кожного державного статистичного спостереження у відповідних методологічних положеннях мають бути визначені:

перелік статистичних показників, які можуть бути конфіденційними і підлягають захисту;

методи та критерії захисту конфіденційних статистичних даних, уключаючи правила визначення загрози розкриття конфіденційних статистичних даних.

6. Органи державної статистики забезпечують статистичну конфіденційність даних, що обробляються.

3. Дані, що поширюються (оприлюднюються)

1. Даними, що поширюються (оприлюднюються), можна вважати дані, що були оброблені та підготовлені для оприлюднення у вигляді:

статистичних публікацій: експрес-випусків, доповідей, бюлетенів, збірників, прес-релізів;

статистичної інформації на офіційних веб-сайтах органів державної статистики;

інформації, яку органи державної статистики надають за запитами, у тому числі на платній основі;

інформації, яку органи державної статистики надають відповідно до угод щодо взаємообміну інформаційними ресурсами між Держстатом та іншими державними органами, установами, організаціями;

інформації, яку органи державної статистики надають міжнародним організаціям і статистичним службам інших країн за запитами та в порядку взаємообміну.

2. Вищезазначені дані перед їх оприлюдненням мають проходити контроль загрози розкриття, перевірку на відповідність методам і критеріям конфіденційності статистичних даних. У разі відповідності методам і критеріям

конфіденційності статистичних даних за результатами контролю загрози розкриття дані, що поширюються (оприлюднюються), не є конфіденційними статистичними даними.

Якщо за результатами перевірки встановлено, що дані, що поширюються (оприлюднюються), є конфіденційними, тоді у матеріалах для поширення замість числового значення показника проставляється три крапки з виноскою (…[1]) та подається такий текст виноски: "[1] Дані не оприлюднюються з метою забезпечення виконання вимог Закону України "Про державну статистику" щодо конфіденційності статистичної інформації.".

IV. Методи захисту конфіденційних статистичних даних

1. Загроза розкриття конфіденційних статистичних даних

Для того, щоб працівники органів державної статистики могли визначити, чи можна встановити конкретну статистичну одиницю та первинні дані щодо неї, вони беруть до уваги всі відповідні можливості, що може використати у зв'язку з цим користувач.

1. Конфіденційні статистичні дані можна встановити прямо або опосередковано.

Під прямим установленням розуміється визначення статистичної одиниці з її прямих ідентифікаторів та/або похідних ідентифікаторів. Під опосередкованим установленням розуміється визначення статистичної одиниці за допомогою будь-якого іншого способу, ніж пряме встановлення.

Пряме встановлення здійснюється тільки з персоніфікованих мікроданих.

Опосередковане встановлення застосовується до знеособлених мікроданих і агрегованих даних. Щодо цих даних мають застосовуватися правила визначення загрози розкриття та методи захисту розкриття первинних даних.

2. Статистичні дані щодо статистичних одиниць можуть поділятися на дві групи:

статистичні дані щодо підприємств, їх структурних підрозділів і фізичних осіб-підприємців (далі – статистичні дані щодо підприємств);

статистичні дані щодо фізичних осіб та домогосподарств (далі – статистичні дані щодо фізичних осіб).

3. Статистична інформація в основному представляється у вигляді агрегованих статистичних даних. Агреговані дані знаходяться під ризиком розкриття, якщо існує ризик розкриття первинних даних щодо статистичної одиниці. Загальні правила визначення загрози розкриття використовуються для визначення конкретного ризику розкриття.

Загальні правила визначення працівниками органів державної статистики загрози розкриття, що використовуються для цілей цих Методологічних положень:

правило порогового значення, згідно з яким значення статистичного показника (ознаки) є вразливим, якщо у ньому міститься менше статистичних одиниць, ніж визначено пороговим значенням. Порогове значення для статистичних даних щодо підприємств повинне бути щонайменше три, а для статистичних даних щодо фізичних осіб щонайменше десять;

правило домінанти (правило n, k), згідно з яким значення є вразливим, якщо його n найбільших статистичних одиниць дають більш ніж k% від значення.

Правило порогового значення є обов'язковим. Одночасно може застосовуватися більш ніж одне правило визначення загрози розкриття.

Разом з тим у рамках статистичного спостереження до окремих агрегованих даних можуть бути встановлені інші правила, що базуються на більш глибокому аналізі щодо визначення загрози розкриття. Однак такі правила повинні враховувати вищезазначені правила визначення загрози розкриття.

Водночас, правила визначення загрози розкриття та методи захисту щодо конкретних статистичних даних мають бути визначені у відповідних методологічних положеннях щодо проведення державних статистичних спостережень.

2. Методи захисту розкриття первинних даних для агрегованих даних

1. Основними методами захисту розкриття первинних даних для агрегованих даних є:

1) первинне блокування, що означає неоприлюднення вразливого значення;

2) вторинне блокування, що означає блокування значень, за допомогою яких можна розрахувати вразливі значення, що були заблоковані на етапі первинного блокування;

3) зміни класифікації, що означає агрегацію класифікаційної ознаки, комбінування з іншими класифікаціям тощо;

4) отримання згоди у джерела вхідних даних щодо оприлюднення конфіденційних статистичних даних.

2. При визначенні методу захисту розкриття конфіденційних статистичних даних розглядається таке:

статистичний показник, що включає вразливе значення;

частотність значень показника;

кількість статистичних одиниць у загальній сукупності;

кількість показників, що оприлюднюються за відповідними статистичними одиницями, та інша статистична інформація, яка описує ті ж самі статистичні одиниці;

інша релевантна інформація, за допомогою якої можна визначити конфіденційні статистичні дані.

3. Методи захисту знеособлених мікроданих

1. Знеособлення мікроданих не є достатнім методом захисту конфіденційних статистичних даних. Тому для зниження ризику розкриття первинних даних використовують методи захисту знеособлених мікроданих, необхідних для виготовлення анонімних мікроданих.

2. Основними методами захисту знеособлених мікроданих є:

1) маскування – створення модифікованої версії знеособлених мікроданих. Методи маскування поділяють на дві категорії в залежності від їх впливу на мікродані:

коригувальні методи – мікродані змінюються перед наданням доступу до них, частина первинної комбінації значень видаляється та замінюється та/або доповнюється комбінацією нових значень. Застосування цієї категорії методів повинна бути такою, щоб агреговані дані з первинних даних і агреговані дані зі змінених даних не повинні значно відрізнятися;

некоригувальні методи – не змінюють початкових даних, а здійснюють прикриття певних змінних початкових даних. Глобальне перекодування, локальне закриття, вибірка є прикладами некоригувальних методів;

2) виробництво синтетичних мікроданих – штучні мікродані, що відображають основні характеристики первинних даних.

V. Захист конфіденційних статистичних даних в ІТС під час їх збирання, зберігання, оброблення та аналізу

1. Головне завдання захисту конфіденційних статистичних даних в ІТС

Інформація під час її збирання, зберігання, оброблення та аналізу в ІТС представляється у певному вигляді, придатному для обробки, та може змінюватися від первинних даних щодо конкретного респондента до статистичної інформації, яка характеризує масові явища та процеси, що відбуваються в економічній, соціальній та інших сферах життя держави та регіонів. Під обробкою можна розуміти як власне обробку з використанням засобів обчислювальної техніки, так і збирання (завантаження інформації в

ІТС), зберігання, аналіз, і т. ін., тобто всі дії над інформацією в ІТС за допомогою відповідних технічних і програмних засобів.

За режимом доступу інформація, що обробляється в ІТС, поділяється на відкриту інформацію та інформацію з обмеженим доступом. У свою чергу інформація з обмеженим доступом за правовим режимом поділяється на конфіденційну, службову і таємну.

У цілях цього документа об'єктом захисту є конфіденційні статистичні дані, які обробляються в ІТС.

Головне завдання захисту конфіденційних статистичних даних, які обробляються в ІТС, полягає у створенні та підтримці у дієздатному стані системи організаційних, технічних та інших заходів, засобів та методів, що дозволяють унеможливити або максимально ускладнити реалізацію несанкціонованих або неконтрольованих дій по відношенню до статистичних даних під час обробки в ІТС та забезпечити дотримання конфіденційності статистичної інформації згідно із вимогами, передбаченими чинним законодавством.

2. Основні види загроз для конфіденційних статистичних даних в ІТС

Основними видами загроз для статистичних даних, уключаючи й конфіденційні статистичні дані, під час обробки в ІТС уважаються будь-які несприятливі обставини чи події, що можуть бути причиною порушення конфіденційності, цілісності або доступності. Відповідно загрози, результат впливу яких на статистичні дані призводить або може призвести до втрати якої-небудь із названих властивостей інформації, розглядаються як загрози конфіденційності, цілісності або доступності.

Загроза конфіденційності полягає в несанкціонованому або неконтрольованому ознайомленні, копіюванні або поширенні конфіденційних статистичних даних особами, які не мають санкціонованого доступу до них. Загроза конфіденційності виникає щоразу, коли отримано несанкціонований доступ до певної інформації з обмеженим доступом, що обробляється в ІТС чи передається між її рівнями.

У зв'язку із загрозою конфіденційності використовується термін виток інформації – це результат дій, унаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї (стаття 1 Закону України "Про захист інформації в інформаційно-телекомунікаційних системах").

Загроза цілісності включає в себе будь-яку несанкціоновану або неконтрольовану модифікацію або знищення конфіденційних статистичних даних, що обробляються в ІТС органів державної статистики та передаються між її рівнями. Цілісність інформації порушена, коли в результаті несанкціонованих дій користувачів навмисно змінюється інформація або якщо до зміни призводить випадкова помилка програмного або апаратного забезпечення. Санкціонованими змінами інформації вважаються ті, які зроблені

користувачами ІТС.

Загроза доступності виникає щоразу, коли в результаті дій, що вживаються користувачем ІТС, або несанкціонованих дій інших користувачів блокується доступ до ресурсів ІТС. Блокування може бути постійним, якщо запитуваний ресурс ніколи не буде отриманий, або воно може викликати тільки затримку запитуваного ресурсу на час, достатній для того, щоб ресурс перестав бути корисним.

Такі види загроз органи державної статистики вважають первинними або безпосередніми, оскільки їх реалізація завдає шкоди ІТС та призводить до безпосередньої несанкціонованої дії на конфіденційні статистичні дані, що підлягають захисту.

3. Основні напрями реалізації захисту конфіденційних статистичних даних в ІТС

1. ІТС включає в себе обчислювальну систему (сукупність програмно-апаратних засобів, призначених для обробки інформації), фізичне середовище, в якому знаходиться і функціонує обчислювальна система, користувачів ІТС, які беруть участь у виробництві статистичної інформації, та інформаційне середовище (оброблювану інформацію, у тому числі й технологію її обробки).

2. Захист конфіденційних статистичних даних під час обробки в ІТС від загроз конфіденційності, цілісності й доступності забезпечується шляхом застосування відповідних заходів, засобів та методів безпеки. Вони повинні охоплювати всі зазначені вище компоненти ІТС, ураховувати їх характеристики та умови функціонування, які мають вплив на реалізацію захисту конфіденційних статистичних даних.

3. Заходи, засоби та методи, що вживаються для захисту статистичних даних в ІТС, уключаючи й конфіденційні статистичні дані, поділяють на організаційні, технічні та організаційно-технічні, зокрема:

організаційні (процедурні) заходи з обліку та зберігання паперових та електронних носіїв інформації, що містять конфіденційні статистичні дані;

технічні (програмні, програмно-апаратні) засоби захисту, що реалізуються для контролю забезпечення статистичної конфіденційності під час обробки в ІТС, та засоби захисту, що реалізуються комплексною системою захисту інформації;

організаційно-технічні заходи з фізичного захисту будівель та приміщень, контролю території (кодові замки, організація пропускного режиму, охоронна сигналізація, захист телекомунікаційного обладнання та кабелів зв'язку тощо).

4. Організаційні (процедурні) заходи з обліку та зберігання паперових і електронних носіїв інформації, що містять конфіденційні статистичні дані, реалізуються відповідно до чинних правил ведення діловодства в органах

державної статистики.

5. Технічні (програмні) засоби захисту, що реалізуються для контролю забезпечення статистичної конфіденційності під час обробки інформації в ІТС, спрямовані на застосування методів контролю загрози розкриття конфіденційних статистичних даних (мікродані, агреговані дані).

Вони реалізуються у вигляді програмного забезпечення (модулів безпеки) у складі інформаційних (автоматизованих) систем (прикладних систем обробки статистичної інформації). Їх функціональне призначення полягає у реалізації функцій забезпечення захисту конфіденційних статистичних даних, наприклад:

знеособлення (анонімізація) первинних статистичних даних респондентів;

контроль загрози розкриття конфіденційних статистичних даних, що підлягають подальшому поширенню зовнішнім користувачам інформації;

перетворення (редагування) таблиць статистичних публікацій у вигляд, що забезпечує анонімність даних і унеможливлює ідентифікацію респондентів (наприклад, застосування методу маскування даних) тощо.

Програмні засоби контролю забезпечення статистичної конфіденційності розробляються відповідно до методологічних положень щодо окремих державних статистичних спостережень, де в частині забезпечення статистичної конфіденційності зазначаються, зокрема:

перелік статистичних показників, які є конфіденційними та підлягають захисту;

правила визначення загрози розкриття конфіденційності агрегованих статистичних даних;

кількісні та/або якісні критерії для застосування правил визначення загрози розкриття конфіденційності зведених статистичних даних;

правила (методи) уникнення розкриття конфіденційних статистичних даних під час їх підготовки до поширення тощо.

Технічні (програмні, програмно-апаратні) засоби захисту, що реалізуються комплексною системою захисту інформації, базуються на використанні спеціального програмного забезпечення, що входить до складу інформаційних (автоматизованих) систем, і спрямовані на забезпечення захисту оброблюваної інформації та програмно-апаратних засобів в ІТС органів державної статистики, зокрема:

захист від несанкціонованого доступу системи авторизації користувачів ІТС, управління доступом до ресурсів системи на основі ролей;

реєстрація подій, ведення журналів роботи системи та доступу користувачів ІТС (засоби аудиту);

антивірусний захист, міжмережеві екрани;

системи автентифікації: пароль, фізичний або електронний ключ доступу, сертифікат;

криптографічний захист інформації тощо.

6. Конфіденційні статистичні дані повинні оброблятися в ІТС органів державної статистики, в якій упроваджено комплексну систему захисту

інформації (КСЗІ).

Захист електронних інформаційних ресурсів органів державної статистики, до яких має бути забезпечений вільний доступ користувачів інформації, здійснюється за вимогами, встановленими КСЗІ офіційного веб-сайту Держстату та веб-сайтів його територіальних органів.

Для організаційного забезпечення завдань керування КСЗІ та здійснення контролю за її функціонуванням в органах державної статистики створюється служба захисту інформації (СЗІ) як окремий (самостійний) структурний підрозділ, що діє з урахуванням положень Закону України "Про захист інформації в інформаційно-телекомунікаційних системах", постанови Кабінету Міністрів України від 29.03.2006 № 373 "Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах" та інших законодавчих та підзаконних актів щодо захисту інформації.

4. Загальні правила забезпечення захисту конфіденційних статистичних даних в ІТС

1. Організація захисту конфіденційних статистичних даних в ІТС потребує регламентації дій користувачів ІТС, які беруть участь у виробництві статистичної інформації, з метою унеможливлення або максимального ускладнення здійснення загроз безпеки оброблюваної інформації.

2. Одним із засобів безпеки організаційного характеру, за допомогою якого реалізуються вимоги щодо безпечних дій користувачів ІТС під час роботи з інформаційними ресурсами, програмними й апаратними засобами системи, є виконання правил забезпечення захисту інформації в ІТС, передбачених положеннями постанови Кабінету Міністрів України від 29.03.2006 № 373 "Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах".

Користувачі ІТС мають дотримуватися загальних правил поводження з ІТС, які визначаються окремим документом.

VI. Правила поводження з конфіденційними статистичними даними в органах державної статистики

Зобов'язання щодо забезпечення статистичної конфіденційності визначені статтями 14, 16, 17, 21, 22 Закону України "Про державну статистику" та передбачають, що працівники органів державної статистики, які на постійній або тимчасовій основі беруть участь у проведенні статистичних спостережень (далі – працівники), не мають права розголошувати та використовувати конфіденційні статистичні дані в нестатистичних цілях, які стали їм відомі під час виконання службових обов'язків.

Правила поводження з конфіденційними статистичними даними в органах державної статистики, враховуючи положення статті 23 Закону України "Про державну статистику", визначаються окремим документом.

VII. Надання доступу до мікроданих у дослідницьких цілях

Органи державної статистики, з метою сприяння й розширення доступу до даних в інтересах суспільства, сприяють процесу доступу до мікроданих для наукових досліджень у соціально і політично значущих сферах, підвищуючи таким чином доступність конфіденційних даних, але зберігаючи при цьому конфіденційність респондентів і статистичних одиниць.

Доступ до мікроданих організовується та забезпечується з урахуванням вимог чинного законодавства України, Регламенту Європейського Парламенту та Ради (ЄС) № 223/2009 від 11.03.2009, Регламенту Комісії (ЄС) № 557/2013 від 17.06.2013.

Загальні правила та умови, за яких може бути наданий доступ до мікроданих для забезпечення статистичного аналізу в дослідницьких цілях, визначаються окремим документом.

VIII. Координація робіт щодо забезпечення статистичної конфіденційності

Координацію робіт з питань забезпечення статистичної конфіденційності в органах державної статистики здійснює Комісія з питань забезпечення конфіденційності статистичної інформації та реалізує відповідний структурний підрозділ через:

підготовку пропозицій щодо формування політики органів державної статистики з питань забезпечення статистичної конфіденційності, щодо приведення відповідно до міжнародних норм, стандартів, регламентів і рекомендацій законодавчої та нормативно-правової бази з питань забезпечення статистичної конфіденційності;

підготовку пропозицій щодо захисту інформації в інформаційно-телекомунікаційних системах під час її збирання, зберігання, оброблення та аналізу;

розгляд інцидентів інформаційної безпеки, що виявляються, з метою визначення їх причин, наслідків і засобів захисту в подальшому;

виявлення та розгляд випадків незаконного розкриття конфіденційних статистичних даних або їх використання для нестатистичних цілей сторонніми особами;

здійснення моніторингу забезпечення статистичної конфіденційності органами державної статистики;

сприяння навчанню працівників органів державної статистики встановленим правилам і процедурам з питань статистичної конфіденційності;

прийняття рішення щодо визнання дослідника для надання доступу до мікроданих у дослідницьких цілях;

розгляд окремих випадків щодо запитів на отримання доступу до інформації, яка може містити конфіденційні дані;

прийняття рішення щодо надання доступу до мікроданих у дослідницьких цілях.

Директор департаменту
статистичної інфраструктури Ю. М. Остапчук