Секція 5

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ І УПРАВЛІННЯ ПРОЕКТАМИ ТА ПРОГРАМАМИ В БЕЗПЕЦІ ЖИТТЄДІЯЛЬНОСТІ

УДК 004.632

ОРГАНІЗАЦІЙНИЙ ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ, ЩО ОБРОБЛЯЮТЬСЯ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Білан В.П.
Мандрона М.М., канд. техн. наук
Львівський державний університет безпеки життєдіяльності

«Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини" стаття 32 Конституції України [1].

Потребу та необхідність захисту особистих даних про особу чітко визначено на законодавчому рівні України. Питання щодо захисту персональних даних регулює Уповноважений Верховної Ради України з прав людини.

Персональні дані – це дані про особу, що дають змогу її ідентифікувати; це вид інформації, що належить до конфіденційної, яка є інформацією з обмеженим доступом. Вимоги до захисту персональних даних регламентується законодавством України.

Основною вимогою під час обробки конфіденційної інформації є забезпечення її захисту від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання, поширення [2-4]. Отже, для виконання цієї вимоги повинні створюватись комплексні системи захисту інформації, які містять комплекси засобів захисту від несанкціонованого доступу, тобто спеціальне ліцензійне, сертифіковане програмне забезпечення.

Експлуатація інформаційно-телекомунікаційної системи (ІТС) можлива лише за умови наявності затвердженого встановленим порядком Плану захисту інформації в ІТС. Дії користувачів ІТС повинні визначатися відповідними інструкціями. Повинні бути розроблені порядки дій користувачів у разі відмови системи захисту в цілому чи окремого її компоненту, також мають бути розроблені нормативні та розпорядчі документи, що визначають правила режиму доступу у приміщення, в якому розміщена ІТС, та порядок доступу користувачів до неї. Користувачі ІТС, котрі працюють з персональними даними повинні мати дозвіл керівника для виконання цієї роботи.

Проаналізувавши літературні джерела ми можемо виділити такі основі організаційні заходи із захисту інформації, тобто ті дії, які спрямовані на реалізацію захисту інформації шляхом регламентації діяльності персоналу і порядку функціонування засобів і систем забезпечення інформаційної діяльності.

Організаційні заходи щодо керування доступом повинні передбачати:

- визначення порядку доступу користувачів у захищене приміщення, до технічних засобів, носіїв інформації, програмного та інформаційного забезпечення;
- визначення порядку внесення/вилучення даних щодо атрибутів доступу користувача.

Організаційні заходи щодо забезпечення цілісності інформації повинні передбачати:

- резервне копіювання на матеріальних носії інформації еталонних копій операційних систем і функціональних програм;
- контроль цілісності системного програмного забезпечення;
- контроль цілісності комплексу засобів захисту.

Організаційні заходи антивірусного захисту інформації повинні передбачати:

- використання сертифікованого ліцензійного антивірусного програмного забезпечення;
- організацію постійного та своєчасного оновлення антивірусних баз.
- для забезпечення відновлюваності інформації у випадку збоїв системи або помилок користувачів в ІТС повинно здійснюватися періодичне резервне копіювання.

Під час обробки персональних даних в ІТС персонал має право створювати, модифікувати, вилучати, друкувати та копіювати на матеріальні носії файли з текстовими документи, за які вони відповідають, а також працювати із файлами, що створюються спільно з іншими користувачами, відповідно до наданих прав. Проте персонал не повинен виконувати роботи з налаштування конфігурації засобів захисту, загальносистемного та програмного забезпечення, оновленням антивірусних баз, систем управління базами даних, змінювати їх склад та структуру, коригувати права доступу. Усі ці роботи повинні виконуватись службою захисту інформації адміністратором безпеки і системним адміністратором.

Література

1. Конституція України [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/254к /96-вр.

2. Закон України «Про захист персональних даних: від 01.06.2010 р. № 2297-VI // Відомості Верховної Ради України (ВВР). – 2010. – № 34. – С. 481.

3. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах": від 27.03.2014 N 1170-VII.

4. Білан В.П. Вимоги законодавства щодо захисту персональних даних / В.П. Білан, М.М. Мандрона // Захист інформації в сучасному суспільстві: матер. 1 Міжнародної наук.-техні. конференції, 21-22 листопада 2014 р. – Львів: Вид-во ЛДУ БЖД, 2014. – С. 15-16.