УДК 004.632

Аналіз програмних засобів захисту персональних даних

Білан В.П., студент 5-го курсу
Науковий керівник – Мандрона М.М., старший викладач кафедри управління інформаційною безпекою, канд. техн. наук,
Львівський державний університет безпеки життєдіяльності, м. Львів

Потребу та необхідність захисту особистих даних про особу чітко визначено на законодавчому рівні України [1-3].

Персональні дані – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [1]. Персональні дані – це вид конфіденційної інформації, що належить до інформації з обмеженим доступом. Отже, система захисту повинна відповідати всім вимогам.

Основною вимогою під час обробки конфіденційної інформації є забезпечення її захисту від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання, поширення [2-4].

Головною вимогою для захисту персональних даних, що обробляються в інформаційно-телекомунікаційній системі є наявність комплексної система захисту інформації. Комплексна система захисту інформації – це сукупність організаційних та інженерних заходів, програмно-апаратних засобів, які спрямовані на забезпечення захисту інформації від розголошення, витоку і несанкціонованого доступу [5]. Така система захисту призначена для забезпечення захисту від витоку технічними каналами, для захисту від несанкціонованого ознайомлення та від спеціальних впливів шляхом формування полів і сигналів з метою порушення цілісності інформації або руйнування системи захисту.

Організаційні заходи є обов'язковою складовою для побудови будь-якої системи. Інженерно-технічні заходи здійснюються в міру необхідності.

Основною вимогою до системи захисту персональних даних є забезпечення захисту від несанкціонованого доступу та від комп'ютерних вірусів. Для цього встановлюють комплекси засобів захисту від несанкціонованого доступу (КЗЗ від НСД) [6, 7]. Ці комплекси повинні бути ліцензійні та сертифіковані. Детальний перелік засобів технічного захисту інформації, дозволених для забезпечення технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, – можна ознайомитись на головній електронній сторінці Держспецзв'язку [8].

Для захисту персональних даних в інформаційно-телекомунікаційній системі потрібно використовувати комплекс із переліку нижче:

- Комплекс засобів захисту інформації від несанкціонованого доступу „Гриф" версії 3;
- Комплекс засобів захисту захищеного носія даних електронних ідентифікаційних та реєстраційних документів на базі чипа InfineonSLE78CLFX4000P;
- Комплекс засобів захисту інформації від несанкціонованого доступу на базі операційної системи Open BSD, шифр "BBOS™" виробництва ТОВ "АТМНІС";
- Захищений від несанкціонованого доступу компонент "Мережевий криптомодуль "Гряда-301" та"Гряда-61";
- Захищений від несанкціонованого доступу компонент "Електронний ключ "Кристал-1Д" та Кристал-1";
- Комплекс засобів захисту інформації від несанкціонованого доступу програмного продукту Symantec Data Loss Prevention11.X виробництва "Symantec", США;
- Захищений від несанкціонованого доступу компонент "Система електронного документообігу АСКОД. Програмне забезпечення АСКОД Корпоративний"
- Пристрої мережевої безпеки FortiGate (20C, 30D, 40C, 50B,60C, 60D, 70D, 80C, 80D, 90D, 92D, 94D, 98D, 110C, 111C, 100D, 140D, 200A, 200B, 224B, 200D, 240D, 280D, 300A,

310B, 300C, 300D, 500D, 700D, 900D, 620B, 600C, 800, 800F, 800C, 1000C, 1000D, 1240B, 1500D, 3016B, 3040B, 3140B, 3240C, 3200D, 3600C, 3700D, 3800D, 3810A, 3180D, 3950B, 5020, 5060, 5140B, 5001C, 5001C, 5001B, 5001D, 5101C) виробництва компанії Hewlett Packard, США;

- Програмний комплекс захисту інформаційних ресурсів “Bitdefender Security for Endpoints” версії 5.x (для платформи віртуалізації Microsoft Hyper-V) виробництва компанії Bitdefender SRL, Румунія.

Перелік сертифікованого антивірусного програмного забезпечення:

- Програмне забезпечення антивірусного захисту “Zillya! Антивірус для Бізнесу” версії 1.1.xxxx.y, Україна;
- Програмний продукт антивірусного захисту інформації ESET File Security для Microsoft Windows Server версії 6.0.X (EFSW) та інші версії виробництва компанії "ESET", Словаччина;
- Комплекс засобів захисту програмного забезпечення антивірусного захисту інформації Symantec Endpoint Protection 12.X, виробництва компанії “Symantec”, США;
- Сервіси безпеки програмного комплексу антивірусного захисту “McAfee Complete Endpoint Protection Enterprise Suite” виробництва компанії McAfee Inc., США.

Висновки. У роботі проаналізовано комплекси засобів захисту від несанкціонованого доступу, які входять до складу системи захисту персональних даних. Варто зазначити, що порушення вимог законодавства щодо захисту персональних даних, тягне за собою накладення штрафу від 5100 до 17 000 грн., відповідно до Кодексу України про адміністративні правопорушення.

Список літератури

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.

5. НД ТЗІ 3.7-003-2005. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі, затверджений наказом ДСТСЗІ СБ України від 08.11.2005 № 125 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806.

6. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені постановою Кабінету Міністрів України від 29.03.2006 № 373 з останніми змінами згідно ПКМУ № 938 від 07.09.2011.

7. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБ України від 28.04.99 № 22.

8. Перелік засобів технічного захисту інформації, дозволених для забезпечення технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом. [Електронний ресурс]. – Режим доступу: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=234237&cat_id=39181.