системи. А розвиток накопичувального страхування забезпечить фінансову стійкість системі пенсійного страхування та створить сприятливі умови щодо можливості системи виконати свої коротко-, середньо- і довгострокові зобов'язання перед громадянами, що досягли пенсійного віку.

Список використаних джерел:

1. Про заходи щодо законодавчого забезпечення реформування пенсійної системи: Закон України від 8 липня 2011 року № 3688. URL: http://zakon4.rada.gov.ua/laws/show/3668-17.

Ковальчук Володимир Миколайович
Завідувач сектором реєстрації та роботи з клієнтами з надання кваліфікованих електронних довірчих послуг

РОЗРОБКА ПОЛІТИКИ БЕЗПЕКИ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Перш ніж пропонувати будь-які рішення щодо організації системи захисту інформації, належить розробити політику безпеки. Політика безпеки – набір законів, правил і практичних рекомендацій, на основі яких будується управління, захист і розподіл критичної інформації в системі. Вона повинна охоплювати всі особливості процесу обробки інформації, визначаючи поведінку системи в різних ситуаціях. Політика безпеки реалізується за допомогою організаційних заходів та програмно-технічних засобів, що визначають архітектуру системи захисту, а також за допомогою засобів управління механізмами захисту. Для конкретної організації політика безпеки повинна бути індивідуальною, залежною від конкретної технології обробки інформації, використовуваних програмних і технічних засобів, розташування організації і т. д.

Організаційно політика безпеки визначає порядок подання та використання прав доступу користувачів, а також вимоги звітності користувачів

за свої дії в питаннях безпеки. Система захисту інформації виявиться ефективною, якщо вона буде надійно підтримувати виконання правил політики безпеки, і навпаки. Етапи побудови організаційної політики безпеки – це внесення в опис об'єкта структури цінностей і проведення аналізу ризику, і визначення правил для будь-якого процесу користування даним видом доступу до ресурсів об'єкта автоматизації, які мають даний ступінь цінності.

Розробка політики безпеки організації, як формальної, так і неформальної, – безумовно, нетривіальне завдання. Експерт повинен не тільки знати відповідні стандарти і добре розбиратися в комплексних підходах до забезпечення захисту інформації організації, але й, наприклад, проявляти детективні здібності при виявленні особливостей побудови інформаційної системи та існуючих заходів з організації захисту інформації. Аналогічна проблема виникає в подальшому при необхідності аналізу відповідності рекомендацій політики безпеки реальному стану речей: необхідно за деяким критерієм відібрати свого роду «контрольні точки» і порівняти їх практичну реалізацію з еталоном, що задається політикою безпеки [1].

У загальному випадку можна виділити такі процеси, пов'язані з розробкою і реалізацією політики безпеки.

1. Комплекс заходів, пов'язаних з проведенням аналізу ризиків. До цієї групи можна віднести:

– облік матеріальних або інформаційних цінностей;

– моделювання загроз інформації системи;

– власне аналіз ризиків з використанням того чи іншого підходу – наприклад, вартісний аналіз ризиків.

2. Заходи з оцінювання відповідності заходів щодо забезпечення захисту інформації системи деякого еталонного зразка: стандарт, профіль захисту тощо.

3. Дії, пов'язані з розробкою різного роду документів, зокрема звітів, діаграм, профілів захисту, заданої з безпеки.

4. Дії, пов'язані зі збиранням, зберіганням і обробкою статистики щодо подій безпеки для організації.

Основу політики безпеки складає спосіб керування доступом, що визначає порядок доступу суб'єктів системи до об'єктів системи. Назва цього способу, як правило, визначає назву політики безпеки.

Основою виборчої політики безпеки є виборче керування доступом, що має на увазі, що

• всі суб'єкти і об'єкти системи повинні бути ідентифіковані;

• права доступу суб'єкта до об'єкта системи визначаються на підставі деякого правила (властивість вибірковості).

Для опису властивостей виборчого управління доступом застосовується модель системи на основі матриці доступу, іноді її називають матрицею контролю доступу. Така модель отримала назву матричної. Матриця доступу являє собою прямокутну матрицю, в якій об'єкту системи відповідає рядок, а суб'єкту – стовпець. На перетині рядка і стовпця матриці вказується тип дозволеного доступу суб'єкта до об'єкта. Зазвичай виділяють такі типи доступу суб'єкта до об'єкта, як «доступ на читання», «доступ на запис», «доступ на виконання» та ін.

Безліч об'єктів і типів доступу до них суб'єкта може змінюватися відповідно до деяких правил, що існують в даній системі. Визначення і зміна цих правил також є завданням матриці доступу.

Рішення на доступ суб'єкта до об'єкта приймається відповідно до типу доступу, зазначеного у відповідній клітинці матриці доступу. Зазвичай виборче управління доступом реалізує принцип «що не дозволено, то заборонено», який передбачає явний дозвіл доступу суб'єкта до об'єкта. Матриця доступу – найбільш простий підхід до моделювання систем доступу [3].

Виборча політика безпеки найбільш широко застосовується в комерційному секторі, оскільки її реалізація на практиці відповідає вимогам комерційних організацій щодо розмежування доступу і підзвітності, а також має прийнятну вартість і невеликі накладні витрати [2].

Основу повноважної політики безпеки складає повноважне управління доступом, що має на увазі, що

– всі суб'єкти і об'єкти системи повинні бути однозначно ідентифіковані;

– кожному об'єкту системи привласнена мітка критичності, що визначає цінність, яка міститься в ньому;

– кожному суб'єкту системи привласнений рівень прозорості, що визначає максимальне значення мітки критичності об'єктів, до яких суб'єкт має доступ.

Вибір політики безпеки – це прерогатива керівника системи захисту інформації. Але якою б вона не була, важливо, щоб впроваджена система захисту інформації відповідала ряду вимог, які будуть розглянуті в наступному розділі.

Список використаних джерел:

1. Про захист інформації в інформаційно телекомунікаційних системах: Закон України № 80/94-ВР від 05.07.1994 р. URL : https://zakon.rada.gov.ua/laws/card/80/94-%D0%B2%D1%80.

2. Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України: лист НБУ від 03.03.2011 № 24-112/365. URL : http://zakon4.rada.gov.ua.

3. Степаненко О.П. Моделі, методи, інформаційні технології підтримки процесів діяльності банківської системи Київ : КНЕУ, 2013. 491 с.

Ковальчук Майя Сергіївна
Провідний спеціаліст відділу освіти, молоді та спорту
Чемеровецької селищної ради

ВПЛИВ БЮДЖЕТНОЇ ДЕЦЕНТРАЛІЗАЦІЇ НА ФІНАНСУВАННЯ ОСВІТИ

У контексті реалій сьогодення, варто відзначити зміни у фінансуванні освіти та низку проведених реформ у напрямку проведення децентралізації місцевих органів влади та місцевих бюджетів.