1. Одне централізоване сховище ключів, доступ до якого можливий лише при наявності інтернет-підключення.
2. Відповідальність за збереження і захист ключів приймає на себе АЦСК.
3. Відпадає необхідність використання бібліотек (драйверів).
4. Можливість інтеграції комплексу зі сторонніми сервісами.
5. Низька ціна аренди місця в криптомодулі.
6. Спрощення процедури отримання КЕП.

**ПЕРЕЛІК ПОСИЛАНЬ:**

1. https://zakon.rada.gov.ua/laws/show/2155-19#n534
2. https://www.pfu.gov.ua/kr/327258-pro-kvalifikovanyj-elektronnyj-pidpys/
3. Семь безопасных информационных технологий / под ред. А. С. Маркова. - М.: ДМК Пресс, 2017. — 224 с.: ил
4. https://medoc.ua/uk/blog/kep-na-zahishhenih-nosijah-roztlumachumo-shho-do-chogo

УДК 004.056

## РОЗРОБКА ІНФОРМАЦІЙНОЇ СИСТЕМИ РИЗИК-БЕЗПЕКИ ПЕРСОНАЛЬНИХ ДАНИХ

В.В. Гнатушенко, В.О. Бура, Т.М. Фененко
(Україна, Дніпро, Національна металургійна академія України)

**Постановка проблеми**. Створення інформаційної системи (ІС) ризик-безпеки персональних даних, яка б дозволила знизити невизначеність при виборі альтернатив, тим самим зменшити можливість прийняття неефективного рішення.

Сучасні інформаційні системи найчастіше представляють собою складні комплекси взаємопов'язаних компонентів. Завдання аналізу безпеки, оцінки ризиків у таких системах ускладнюється тим, що експерту невідомі точні значення характеристик системи яка аналізується. Більшість існуючих методик припускають завдання наближених точкових оцінок, що знижує достовірність отриманих, також точкових, результуючих показників.

При експертному оцінюванні, ми стикаємося з різними видами невизначеності, і основним завданням є її спільне моделювання. Аналогічна проблема виникає і при виборі найбільш ефективного комплексу засобів протидії загрозам інформаційної безпеки. Для її вирішення використовується методика рандомізації оцінок факторів з подальшим відбором результатів, що задовольняють вихідними даними.

В умовах реального світу інформація слабо визначена - має нечислової характер, неточна, погано структурована. Фактично, первинні дані являють собою випадкові величини. Поряд з невизначеністю оцінок можлива і

структурна невизначеність, тобто неповнота знань про наявність чи відсутність відносин між факторами. З урахуванням структурної невизначеності, а також узгодження думки кількох експертів, завдання моделювання факторів ризику ускладнюється, а час рандомізації значно зростає. Для вирішення завдань оцінки і аналізу ризиків застосовуються експертні системи, які, на жаль, мають не дуже велику методологічну різноманітність.

Виходячи з означених вище параметрів інформаційних систем та їх недоліків, була розроблена система ризик-аналізу, в якої оцінки факторів ризику представляють не точкові значення показників, а розподіл їх ймовірностей. Розроблена методика стохастичного ризик-аналізу, дозволяє більш достовірно оцінити загрози для конкретної ІС і розробити ефективну систему захисту. При необхідності можливе додавання факторів, або їх угруповання (об'єднання). Оскільки методика працює не з числовими значеннями, а з розподілами, то вона дозволяє описати різноманітні типи інформації, які одержані в результаті експертного оцінювання.

В рамках роботи розроблено модуль системи ризик-аналізу, що дозволяє вирішити задачу статистичної обробки даних, які отримані на етапі стохастичного моделювання, і подальшого їх відображення у вигляді профілів ризиків. В якості інформаційного об'єкта для аналізу та оцінки ризиків було використано ІСПД медичного закладу.

**Висновки**. Розроблена ризик-модель містить відмінності від вихідної базової моделі безпеки інформаційної системиа персональних даних (ІСПД). Перш за все, фактори ризику в ній об'єднані в зв'язну причинно-обумовлену структуру. Однак, для збереження несуперечності з базовою моделлю, в набір чинників ризик-моделі були включені всі загрози базової моделі. Створено перелік ризик-факторів, який містить джерела загроз, загрози, події ризику, інформаційні компоненти об'єкта захисту. Для дотримання методологічної строгості і логічної повноти ризик-моделі деякі вихідні чинники зазнали змін: змінено формулювання, вироблено розбиття на кілька факторів для зниження складності. Крім того, додані фактори, які явно не вказуються в базовій моделі, але включені в неї контекстуально. Подібні модифікації не створюють протиріч з базовою моделлю.

**ПЕРЕЛІК ПОСИЛАНЬ:**

1. Вишняков Я.Д., Радаев Н.Н. Общая теория рисков Учеб. пособие для студ. высш. учеб. заведений. - 2-е изд., испр. - М. : Академия, 2008. - 368 с

2. Малкин В.С. Надежность технических систем и техногенный риск Учебное пособие. - Ростов-на-Дону: Феникс, 2010. - 432 с.

3. Хованов Н.В. Анализ и синтез показателей при информационном дефиците - СПб.: Изд-во СПб ун-та, 1996. - 196 с.