проектування структури програмного комплексу;

3. побудову системи правил для перекладу української жестової мови з використанням граматично доповненої онтології;

4. розроблення методів інформаційної технології для перекладу української жестової мови із застосуванням граматично доповненої онтології;

5. проведення експериментальних досліджень та виконання порівняльного аналізу отриманих результатів [2].

Ключовими завданнями у процесі створення інформаційної технології перекладу української жестової мови є розроблення методів та засобів для ефективного перекладу, оптимізація процесу наповнення граматично доповненої онтології, розроблення системи правил перетворення української словесної мови на жестову та навпаки.

Список використаних джерел

1. Кульбіда С. В. Українська жестова мова як природна знакова система. Жестова мова й сучасність: збірник наукових праць / С. В. Кульбіда // К.: Центродрук. – 2009. – С. 218-239.

2. Фрадкина Р. Н. Говорящие руки: Тематический словарь жестового языка глухих. – М.: Знание, 2001. – 62 с.

Поліщук Володимир Володимирович
кандидат технічних наук, доцент, доцент кафедри програмного забезпечення систем, факультету інформаційних технологій, ДВНЗ «Ужгородський національний університет»
Гелетей Михайло Михайлович
магістр факультету інформаційних технологій, ДВНЗ «Ужгородський національний університет», м. Ужгород, Україна

ЕКСПЕРТНА МОДЕЛЬ ОЦІНЮВАННЯ РИЗИКІВ МЕРЕЖЕВИХ ТА ІНФОРМАЦІЙНИХ СИСТЕМ АЕРОПОРТУ

Сучасний повітряний транспорт, його управління та забезпечення безпекою створюють не тільки комерційні успіхи, але й різного роду ризики, що несуть потенційну небезпеку для людей, майна та інших юридично захищених інтересів. Небезпека проявляється у вигляді інцидентів безпеки чи інших антисоціальних явищ, які також можуть мати кримінальний характер. Інцидент (щодо кібербезпеки) – означає будь-яку подію, що негативно впливає на безпеку мережевих та інформаційних систем (МІС) [1]. Привабливим і потенційним об’єктом кіберзлочинності є величезна кількість даних в мережевій роботі інформаційних систем цивільної авіації та роботи аеропортів.

У більшості випадків для вирішення проблем із захистом МІС аеропортів використовують часткові підходи, що зумовлено поточним рівнем доступних ресурсів. Експерти з безпеки мають тенденцію реагувати лише на

зрозумілі їм ризики безпеки. Тому тільки комплексний підхід, що забезпечить єдину політику безпеки дасть змогу знизити ризики безпеки [2]. Адаптивна безпека мережі, що дає можливість контролювати, виявляти ризики та реагувати на них, складається з трьох компонентів: технологія управління ризиками, технологія аналізу захищеності та технологія виявлення атак [1]. Модель адаптивної безпеки мережі не відкидає вже використовувані механізми захисту, а розширює їх завдяки новим технологіям. Підприємствам необхідно доповнити наявні рішення компонентами, що відповідають за аналіз захищеності, виявлення атак і управління ризиками в рамках запобігання кіберзлочинності та для приведення систем інформаційної безпеки у відповідність до сучасних вимог. Дослідження орієнтується на створення технологій управління ризиками з залученням інтелектуального аналізу знань експертів у адаптивному підході до безпеки роботи аеропортів.

Нехай маємо множину активів інформаційної безпеки аеропорту, для яких визначено множину загроз безпеки персональних даних мережевих та інформаційних систем. Кожна загроза безпеки для деякого активу буде оцінюватись експертом з безпеки по вхідним експертним даним: T – наслідки реалізації загроз безпеки персональних даних МІС аеропорту; μ – степінь можливості реалізації загрози МІС аеропорту; L – тяжкість наслідків інциденту по активу.

На основі вхідних експертних даних потрібно вивести оцінку ризику безпеки персональних даних МІС аеропорту окремо по активах, розрахувати фінансові збитки інцидентів (ймовірність реалізації ризику) для активів та вивести одну агреговану оцінку для прийняття подальших рішень у рамках запобігання кіберзлочинності.

Розроблена модель та її програмна підтримка буде корисним інструментом для експертів з безпеки авіації та роботи аеропортів в рамках запобігання кіберзлочинності [3].

Список використаних джерел

1. *Бобало Ю.Я. Інформаційна безпека: навчальний посібник / Ю.Я. Бобало, І.В. Горбатий, М.Д. Кіселичник, А.П. Бондарєв, С.С. Войтусік, А.Я. Горпенюк, О.А. Нємкова, І.М. Журавель, Б.М. Березюк, Є.І. Яковенко, В.І. Отенко, І.Я. Тишик. Львів: Видавництво Львівської політехніки, 2019. – 580 с.*

2. *Казарин О.В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для вузов / О.В. Казарин, А.С. Забабурин. – М.: Издательство Юрайт, 2017. – 312 с.*

3. *Polishchuk V. Technology Improving Safety of Crowdfunding Platforms Functioning in the Context of the Protection of the Start-up Investors in the Financial and Transport Sectors/ V. Polishchuk, M. Kelemen, J. Kozuba // The Journal of Air Force Institute of Technology (Journal of KONBiN), 2019. – Volume 49: Issue 1. – P. 313-330.*