УДК 004.9

Юр'єв Д.А., Тимошенко Л.М.

Національний університет «Одеська політехніка»

КІБЕРСИТУАЦІЙНА ОБІЗНАНІСТЬ СПІВРОБІТНИКІВ ОБ'ЄКТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Вступ. В Україні в умовах воєнного стану питання людського фактору є особливо актуальним, оскільки об'єкти критичної інфраструктури постійно перебувають під загрозою кібератак. Необізнаність або помилки співробітників можуть проявлятись у різних формах, серед яких відзначають використання слабких паролів, нехтування правилами кібергігієни, наприклад, перехід за фішинговими посиланнями або встановлення вірусного програмного забезпечення. Відсутність знань або навичок у реагуванні на кіберзагрози, зокрема, фішинг, DDoS-атаки, втрата пристроїв, що містять конфіденційну інформацію, або їх неналежне зберігання призводять до отримання зловмисниками доступу до систем, що за інших обставин було б неможливим.

Одеська обласна державна (військова) адміністрація (ОВА) – ключова державна інституція виконавчої влади і важлива ланка в системі державного управління, особливо в умовах воєнного стану. ОВА виступає координатором роботи органів влади, органів місцевого самоврядування, критичних підприємств державного і приватного сектора в регіоні.

Перехід війни в кіберпростір сприяє зростанню кількості практичних розробок і наукових праць з проблематики кіберситуаційної обізнаності, визначає актуальність досліджень з оцінки й моніторингу ситуаційної обізнаності та інформаційної безпеки для усіх сфер державного управління та держави в цілому.

Мета: Дослідження кіберситуаційної обізнаності співробітників об'єкту критичної інфраструктури, інструментів для опису стану ситуаційної обізнаності, та розробка програмної системи моніторингу кіберситуаційної обізнаності.

Основна частина

Особливу роль ОВА відіграє у підтримці обороноздатності регіону [1], зокрема через мобілізацію ресурсів, активну взаємодію з військовими підрозділами, військовим командуванням, Радою національної безпеки і оборони України, Кабінетом Міністрів України.

Серед основних задач ОВА під час воєнного стану визначають забезпечення безперебійного і стабільного функціонування об'єктів критичної інфраструктури, зокрема, залізничних вузлів, портів, медичних закладів, об'єктів енергетичної інфраструктури вищих навчальних закладів, базових станцій операторів стільникового зв'язку. Таким чином ОВА виступає стратегічним центром управління та захисту, поєднуючи адміністративні, оборонні та координаційні функції для підтримки регіональної стабільності.

Завдання системи із ситуаційною обізнаністю полягає у забезпеченні повністю автономного прийняття рішення інтелектуальною системою у динамічному середовищі. Зі стрімким розвитком інформаційних технологій термін «ситуаційна обізнаність», що з'явився у військовій галузі, набуває

подальшого розвитку. Це означає можливість отримання досить повного і точного набору необхідної для прийняття рішення інформації про ситуації в реальному часі [2]. Такий комплексний підхід у володінні ситуацією актуальний в різних областях, де є великий обсяг інформаційних потоків і високий ступінь ризику, зокрема, в кіберпросторі. Побудова автоматизованого механізму виявлення загроз створить картину ситуаційної обізнаності в кіберпросторі для керівників різних рівнів управління критичної інфраструктури.

Вимоги до кіберзахисту державних електронних інформаційних ресурсів та інформаційної інфраструктури, критичної інфраструктури, до якої належать органи державного управління, встановлені законом. Вони передбачають, насамперед, підвищення обізнаності працівників держорганів у сфері інформаційної безпеки та кібербезпеки шляхом проведення різних тренінгів і навчань, та проведення моніторингу їх результатів. Для оцінки кіберситуаційної обізнаності у цій роботі використано метод тестування. Для визначення експертних оцінок, що є вагами кожної відповіді, використано метод аналізу ієрархій (MAI) - математичний інструмент системного підходу до різних складних проблем прийняття рішень [3]. Згідно MAI складено матрицю порівняння критеріїв, матриці порівняння альтернатив за кожним критерієм, матриці ваги альтернатив і ваги критеріїв, з'ясовано та узгоджено експертні оцінки кіберситуаційної обізнаності співробітників. Враховуючи одержані ваги відповідей у тестах, використовуючи шкалу Лайкерта рівнів обізнаності, розраховано рівень кіберситуаційної обізнаності.

Для реалізації системи використано Python та Michrosoft Excel. Виконано експериментальне дослідження тестування ситуаційної обізнаності та аналіз одержаних результатів моніторингу.

Дане дослідження мотивоване до кіберситуаційної обізнаності співробітників держадміністрації. Співробітники приходять з різних галузей та верств суспільства, володіють різними звичками, досвідом та інтелектом, що в підсумку впливає на їх обізнаність про інформаційну безпеку на робочому місці. З іншого боку, органи державного управління все ще не можуть гарантувати, що у співробітників знання, ставлення і поведінка відповідні і вони автоматично дотримуються правил. Їх кіберситуаційна обізнаність може бути меншою за очікувану або недостатньою настільки, що це загрожуватиме цілісності органу.

Дослідження характеризується кількісною оцінкою індивідуальної обізнаності про інформаційну безпеку. Шляхом її вимірювання можна інтерпретувати, які проблеми чи загрози інформаційної безпеки слід очікувати, використовуючи інформаційні програми обізнаності та кібергігієни в майбутньому. Цей вимір враховує три основні етапи.

1. Побудова кіберситуаційних параметрів обізнаності. Даний етап спрямований на визначення сфери ситуаційного дослідження обізнаності. Він встановлює відповідні критерії вимірювання для контексту співробітника. Критерії охоплюють три виміри моделі AIU (Awareness, Ignorance, Uncertainty), що ґрунтуються на дослідженнях Ханша і Бененсона в [1].

2. Оцінка кіберситуаційної обізнаності. На цьому етапі використовується шкала Лайкерта для вивчення того, як співробітники узгоджуються із твердженнями з кіберситуаційної обізнаності. Цей етап формує середній бал за

відсотковою шкалою. На основі агрегованих оцінок респонденти поділяються на п'ять рівнів обізнаності.

3. Кіберситуаційний аналіз причинно-наслідкових зв'язків. На цьому етапі досліджуються всі активності та можливості, що впливають на результат оцінки кіберситуаційної обізнаності. Це породжує критичні питання співробітників як цілі для поліпшення рівня кіберситуаційної обізнаності в майбутньому.

Відмінним інструментом інформаційної безпеки державної адміністрації є моніторинг. Цей вимір обізнаності співробітників про безпеку використано для спостереження за реагуванням на конкретні питання і ситуації, пов'язані з безпекою. Результати тестування доречно використати для визначення сфер навчання захисту. Згенерований бал і рівень обізнаності можна відстежувати з плином часу як метрику для вимірювання програмних цілей та ініціатив, розробки рекомендацій, для порівняння з колегами по відділу (рисунок1), тощо.

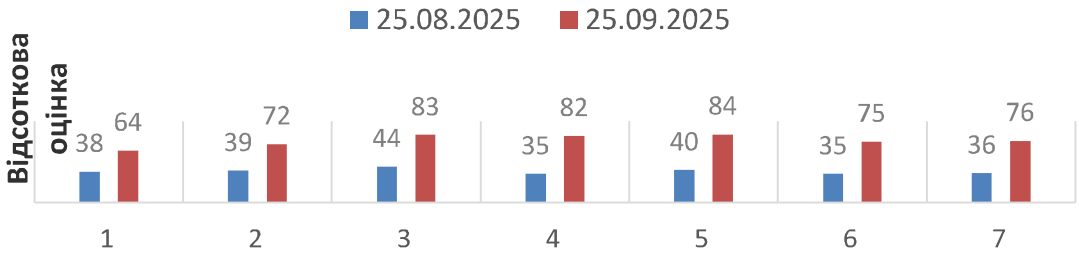

Рисунок 1 - Результати тестування

Висновок. У результаті аналізу існуючого стану захищеності інформаційних ресурсів об'єкту державного управління, зокрема, Одеської державної (військової) адміністрації, вивчили рівень ризику та можливі загрози інформаційній безпеці з боку співробітників. Проведені дослідження методів оцінки ситуаційної обізнаності дозволили обрати комп'ютерне тестування та метод аналізу ієрархій.

Для програмної реалізації моніторингу кіберситуаційної обізнаності обгрунтувано використано середовище Python та Michrosoft Excel. Виконано експериментальне дослідження та проаналізавано одержані результати. Розроблено заходи з підвищення рівня кіберситуаційної обізнаності та рекомендації по їх впровадженню для підвищення захищеності інформаційних ресурсів органу державного управління. За рахунок впровадження заходів з інформаційної безпеки рівень кіберситуаційної обізнаності підвищився на 38%.

Перелік використаних джерел.

1. Микіч Х.І., Буров Є.В. Формальна модель опрацювання знань у системах із ситуаційною обізнаністю. Вісник Національного університету «Львівська політехніка». Інформаційні системи та мережі. 2017. № 872. С. 25-35.

2. Чепурний К., Тимошенко Л. Захист об'єкту критичної інфраструктури в умовах воєнного стану. Інформаційна безпека та інформаційні технології.Зб. матеріалів доп. учасн. V Міжнар. наук.-практ. конф. : Львів, 2024. С. 102-105.

3. Saaty Thomas L. Fundamentals of Decision Making and Priority Theory with the Analytic Hierarchy Process (1994). Pittsburgh: RWS. ISBN 0-9620317-6-3.