УДК 004.42

**ПРОЕКТУВАННЯ ТІ ІНТЕГРАЦІЯ КІБЕРЗАХИСТУ В РОЗУМНОМУ МІСТІ**

*Курило С.О., науковий керівник Лахно В.А.*

Smart City – це набір технологічних інновацій та ініціатив, використання різноманітних датчиків, високошвидкісного підключення до мережі Інтернет, для збільшення ефективності збору та управління даними. Основною метою розумного міста є поліпшення життя громадян більш ефективним використанням даних, дозволивши краще та стійкіше управляти інфраструктурою і послугами.

Стандарти, реалізації і концепції розумних міст побудовані на застосуванні цифрових та інших технологій, що швидко розвиваються і націлені на економічні, соціальні, екологічні та інші позитивні ефекти при їх використанні в містах. Впровадження таких інновацій, фактично, трансформує міський устрій життя неймовірно швидкими темпами і дає величезні переваги жителям міст, але, також, супроводжується абсолютно новими цифровими загрозами і небезпеками [1].

Розумні міста повинні забезпечувати інформаційну безпеку та бути захищеними від кібератак, саме захист має бути головною складовою їх системи. Крім втрати даних, інші потенційні загрози включать в себе зловмисників (кіберзлочинців), які можуть отримувати несанкціонований доступ до інтелектуальної системи міста, змінювати та фальсифікувати дані, порушувати міські послуги задля власних цілей.

Кібербезпека – це реалізація заходів щодо захисту систем, мереж і програмних додатків від цифрових атак. Такі атаки зазвичай спрямовані на отримання доступу до конфіденційної інформації, її зміни і видалення, на вимагання у користувачів грошей або на порушення нормальної роботи системи.

Технології є найважливішим елементом, що надає необхідні інструменти для захисту від кібератак. Основними компонентами, які необхідно захистити, є кінцеві пристрої, наприклад, комп’ютери, датчики, інтелектуальні та мережеві пристрої, комп’ютерні мережі і хмарне середовище. До найбільш поширених технологій, що використовуються для захисту перерахованих компонентів, відносяться міжмережеві екрани нового покоління, фільтрація DNS, захист від шкідливого ПО, антивірусне ПЗ і рішення для захисту електронної пошти.

Основну частку елементів розумних міст складають IoT (Internet of Things). Розумні пристрої, підключені до Інтернету – «Інтернет речей» роблять життя більш зручнішим, покращуючи виробничу ефективність і вже рятують життя. IoT пристрої входять до складу споживчих товарів, таких як центри домашньої автоматизації, відеореєстратори і мережеві маршрутизатори, а також системи автоматизації, які контролюють механізми та системи автоматизації будівель, регулюють клімат будівлі, управляють різними функціями, включаючи енергоспоживання, систему аварійних відмов, подачу води, роботу ліфтів та безпеку контролю доступу [2].

Оскільки ці пристрої підключені до мережі Інтернет, ними можуть незаконно маніпулювати зловмисні суб’єкти. Швидке зростання числа пристроїв IoT ставить підривні завдання для органів інформаційної безпеки, оскільки IoT-пристрої представляють нові типи цілей, а також нову зброю, що загрожує економічній і фізичній безпеці.

Перспективні технології кібербезпеки [3]:

Криптографія. Фахівці з безпеки особливу увагу сьогодні звертають на криптографічне шифрування інформації. Криптографічні методи шифрування діляться на симетричні і асиметричні. У першому випадку для зашифровування і розшифрування даних використовується один і той же ключ. У другому випадку використовуються два різних ключа: один для зашифровування, інший для розшифрування. При цьому вибір того чи іншого рішення залежить від цілей, які ставить перед собою фахівець.

Блокчейн. Розвиток технологій інформаційної безпеки також тісно пов’язаний з можливостями блокчейну і смарт-контрактів. Коли дослідники зрозуміли, що вносити в реєстр можна не тільки дані транзакцій з криптовалютами, але і різні метадані, блокчейн почав активно розширюватися на сферу захисту інформації. Ця технологія може гарантувати не тільки збереження, а й незмінність і автентичність даних, а також робить практично неможливим обман систем ідентифікації.

Токенізація. Одним з найбільш надійних способів захистити платіжні дані є технологія токенізаціі. Її суть полягає в підміні реальних конфіденційних даних іншими значеннями, або токенами. В результаті в торгових компаніях може зникнути необхідність зберігати платіжні дані користувачів, а зловмисники, які отримають доступ до інформації через карти клієнтів компаній, не зможуть ніяк нею скористатися.

Технологія захисту рухомої цілі. Значний внесок в кібербезпеку в майбутньому може внести також технологія захисту рухомої цілі. Зараз ця технологія тільки тестується і не використовується широко на практиці. Нова система захисту вперше була представлена ​​в 2016 році вченими з університету Пенсильванії. За допомогою технології захисту рухомої цілі розробники мають намір вирішити одну з головних проблем захисту даних – позбавити авторів кібератак доступу до коду, який використовується при шифруванні. Експерти кажуть, що наявності одного факту шифрування сьогодні недостатньо. Щоб захистити дані, потрібно безперервно змінювати систему, і тоді зловмисник не зможе отримати актуальну інформацію про її стан, яку можна використовувати в наступний момент часу. В результаті спланувати атаку буде вкрай складно.

Біометрична аутентифікація. До числа перспективних напрямків інформаційної безпеки фахівці відносять також технології біометричної аутентифікації, що дозволяють аутентифікувати користувачів за допомогою зчитування фізіологічних параметрів і характеристик людини і особливостей її поведінки. Швидше за все в цьому сегменті розвиваються технології голосової біометрії і розпізнавання обличь. Ці рішення вже активно застосовуються в галузі криміналістики та соціального контролю і поступово стають стандартною функцією в смартфонах. Однак аналітики вважають, що майбутнє біометрії за використанням «закритих даних», таких як серцевий пульс, малюнок судин які знаходять всередині очного яблука, форма мочок вух та інше.

Штучний інтелект. Нові можливості для фахівців з інформаційної безпеки відкриває штучний інтелект. Технології машинного навчання вже зараз допомагають захищати корпоративні дані в поштовому сервісі Gmail. У червні 2017 року Google представила нову систему виявлення фішингових атак для компаній за допомогою технологій машинного навчання, яка відправляє моментальні попередження про перехід за підозрілими посиланнями, надсилає повідомлення про відправку небажаної відповіді одержувачам за межами домену і пропонує вбудовані функції захисту від нових загроз.

**СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ**

1. Соколов И. А. и др. Умные города, инфраструктуры и их антитеррористическая устойчивость //International Journal of Open Information Technologies. – 2017. – Т. 5. – №. 7.
2. Kupriyanovsky V. et al. Web of Things and Internet of Things in the Digital Economy //International Journal of Open Information Technologies. – 2017. – Т. 5. – №. 5.
3. rb.ru [Електронний ресурс]: «Технологии кибербезопасности: какие решения перспективны и можно ли полностью защититься уже сейчас». Режим доступу: https://rb.ru/longread/cybersecurity-today/ (дата звернення: 28.03.19).