МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Одеська національна академія харчових технологій
Університет Інформатики і прикладних знань, м.Лодзь, Польща
Національний технічний університет України «Київський політехнічний інститут»
Навчально-науковий інститут комп'ютерних систем і технологій «Індустрія 4.0» ім. П.М. Платонова

XXI Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

«СТАН, ДОСЯГНЕННЯ ТА ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ»

Матеріали конференції

Одеса

22-23 квітня 2021 р.

Стан, досягнення та перспективи інформаційних систем і технологій / Матеріали XXI Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Одеса, 22-23 квітня 2021 р**.** - Одеса, Видавництво ОНАХТ, 2021 р. – 229 с.

Збірник включає матеріали доповідей учасників конференції, які об'єднані за тематичними напрямками конференції.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Матеріали подано українською, російською та англійською мовами.
Редактор збірника Котлик С.В.

УДК 004.056.53

ОЦІНКА ПРОБЛЕМ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФРАСТРУКТУРІ “РОЗУМНИЙ БУДИНОК”

ЄРЕЩЕНКО О. Д., (*lenaereschenko0928@gmail.com*),
Харківський національний університет імені Семена Кузнеця

Сьогодні система «Розумний будинок» виходить на новий рівень у нашому житті та є досить перспективним напрямком у розвитку. Система використовується від організації рутинних хатніх справ до систем на заводах. У цю систему входять пристрої, що відповідають за захист від пожеж, а також охоронна сигналізація. Апарати, які контролюють газо- і водопостачання. Пристрої, що відповідають за охолодження та вентиляцію повітря. Обладнання, що контролює подачу електричної енергії та опалення. Пристрої, які контролюють побутову техніку. Все об’єднується в єдину систему управління будинком. Розглянемо деякі, найбільш характерні уразливості, проблеми та як їх вирішити.

1. Проблема неправильно налаштованого віддаленого підключення. Використовується VPN-підключення зі стандартним налаштуванням. Хто завгодно зможе підключитися до керування системою. Вирішується використанням нестандартних портів або SSL-сертифікатів, або 2 факторної автентифікації.

2. Підміна DHCP сервера. Цим зловмисник може змусити клієнта використовувати нелегітимний вузол в якості шлюза за замовчуванням. Захист від цього можливий за допомогою коректного налаштування мережі: увімкнути DHCP Snooping, визначити довірені порти та вказати адресу довіреного DHCP сервера який доступний через довірений порт.[1]

3. Порушення електропостачання. Часто відбуваються перебої з електропостачанням. Вони можуть призвести до виходу зі строю елементів системи, порушенню роботи програми автоматизації. Вирішити це можна встановленням пристрою гарантованого електропостачання або генератора.

4. Атака на відмову в обслуговуванні. Намір зловмисника зробити комп'ютерні ресурси недоступними користувачам. Одним із методів нападу є насичення великою кількістю зовнішніх запитів та тоді устаткування не може відповісти користувачам, або відповідає настільки повільно, що стає фактично недоступним. Фактично примушують устаткування зупинити роботу.

Загальні поради для роботи з системою розумного будинку включають:

Часте і регулярне оновлення IoT-пристроїв. Важливо, що багатьом з цих пристроїв не вистачає фізичної пам'яті для забезпечення оновлень безпеки. Це може поставити під загрозу всю мережу. Оновлення прошивки вашого пристрою IoT на постійній і регулярній основі, коли це можливо, допоможе уникнути багатьох порушень в мережі. [2]

Зміна паролів і протоколів на пристроях за замовчуванням на більш надійні.

Використання багатофакторної автентифікації.

Перевірка на працездатність і технічний стан всіх пристроїв, підключених до вашої мережі, абсолютно необхідна для визначення атаки до її розвитку і є одним з найбільш важливих аспектів ефективного реагування на інциденти. Чим більш всеосяжний аудит проводиться, тим краще. Важливо перевіряти не тільки обладнання, яке раніше не контролювалося (наприклад, камери, монітори, датчики), але і фізично перевіряти всі пристрої на всі вразливості.[3]

Отже, сьогодні система розумного будинку не є цілком захищеною. Ця технологія прийшла до нас зовсім недавно, тому впроваджуючи систему потрібно дуже уважно та присквпливо підбирати обладнання. Адже, навіть мінімальна помилка може призвести до втрати надзвичайної кількості конфіденційної інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ
1. Rogue DHCP Server (DHCP-spoofing или подмена) [Електронний ресурс] – Режим доступу до ресурсу: https://sites.google.com/site/theocsic/technologies/securitynet/dhcp-spoofing (дата звернення 10.04.21).
2. Подмена MAC: атака и защита, теория и практика [Електронний ресурс] – Режим доступу до ресурсу: https://xakep.ru/2002/01/24/14341/ (дата звернення 10.04.21).
3. "Секьюріті н'юз" [Електронний ресурс] – Режим доступу до ресурсу: https://security-news.today/(дата звернення 10.04.21).

УДК 004.942

ПРО ВРАХУВАННЯ СТАВЛЕННЯ ДО РИЗИКУ В ПРОСТОРОВИХ СИСТЕМАХ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ

КЛЕПАТСЬКА В.В., БУЧИНСЬКА І.В., КУЗНІЧЕНКО С.Д. (victoria.klepatska@gmail.com),
Одеський державний екологічний університет

В роботі розглядається проблема врахування ставлення ОПР до ризику при прийнятті рішень в геоінформаційних системах. Показано, що найбільш обґрунтованим є використання оператора OWA, який забезпечує безперервні операції агрегування між крайніми випадками ставлення до ризику, а саме: від готовності до ризику до повної відмови від нього.

Постановка проблеми. Значні обсяги даних, які сьогодні використовують керівники та особи, що приймають рішення (ОПР), мають географічну природу, тобто є геопросторовимим даними. Для вирішення проблем прийняття рішень, що пов'язані з геопросторовими даними, призначені просторові системи підтримки прийняття рішень (СППР). Часто подібні СППР будуються на базі геоінформаційних системи (ГІС) загального призначення, в яких дані організовані у вигляді окремих тематичних карт або наборів даних, що називаються шарами. Незалежно від організації просторових даних, кінцева мета ГІС – підтримка прийняття просторових рішень, що, як правило, засновано на оцінці великої кількості альтернатив на основі багатьох критеріїв.

Прийняття ризику – це будь-яка свідомо або несвідомо контрольована поведінка з невпевненістю в її результаті та/або можливих вигод або витрат для фізичного, економічного або психосоціального благополуччя себе або інших. Відношення до ризику ОПР може змінюватися від готовності до ризику до повної відмови від ризику. В будь-якому випадку розумним підходом є визначення рівня допустимості (прийнятності) ризику ОПР та врахування цього показника при агрегуванні оцінок альтернатив.

Метою дослідження є аналіз та вибір оператора агрегування, здатного враховувати рівень прийняття ризику ОПР при вирішенні просторових завдань прийняття рішень в ГІС.

Основний матеріал дослідження. У випадку вирішення проблем, що пов'язані з розміщенням геопросторових об'єктів або визначенням придатності територій, альтернативами є земельні ділянки (растри), які треба оцінити за множиною критеріїв. За кожним критерієм створюється окремий шар, кожна комірка растру якого має атрибут, що дорівнює її оцінці за даним критерієм. На цьому етапі застосовують методи нормування даних, суть яких полягають у приведенні діапазону значень атрибутів до деяких необхідних меж (наприклад, від 0 до 1). Для цього можуть бути використані нечіткі множини та фазифікація атрибутів за заданими функціями належності. Множина альтернатив A, що оцінюється за n критеріями буде мати вигляд:

$$A = \left\{ a_{ij} \mid i = \overline{1,m},\ j = \overline{1,n} \right\},$$

де $a_{ij} \in [1,0]$ – оцінка атрибуту за j-им критерієм і за i-ою альтернативою; n – кількість критеріїв; m – кількість альтернатив [1].

XXI Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

«СТАН, ДОСЯГНЕННЯ ТА ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ»

Одеса

22-23 квітня 2021 р.

Збірник включає доповіді учасників конференції. Тези доповідей публікуються у вигляді, в якому вони були подані авторами.

Відповідальність за зміст і форму подачі матеріалу несуть автори статей.

Редакційна колегія: Котлик С.В., Корнієнко Ю.К.

Комп'ютерний набір і верстка: Соколова О.П.

Відповідальний за випуск: Котлик С.В.