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.

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].

Процедура ранжування альтернатив зводиться до розрахунку загальної оцінки кожної альтернативи з використанням різних операторів агрегування. При цьому важливо враховувати важливість (вагу) кожного з критеріїв та ставлення ОПР до ризику.

Для врахування крайніх випадків ставлення до ризику в ГІС можуть бути використані оператори *MIN* і *MAX*:

$$MIN = \min(a_{i1}, a_{i2}, a_{i3}, ...);$$

$$MAX = \max(a_{i1}, a_{i2}, a_{i3}, ...).$$

Оператор агрегування *MIN* дозволяє ухилитися від ризику, та оцінити альтернативу (придатність ділянки території) з точки зору її гіршої якості. Оператор *MAX* протилежний, і тому його можна вважати дуже оптимістичним оператором агрегування: ділянка буде оцінена за своєю найкращою якістю.

Зрозуміло, що для врахування різного рівня прийнятності ризику треба мати оператор агрегування, результат виконання якого потрапляє в діапазон між операторами *MIN* і *MAX,* тобто відображає певну ступень компромісу між оцінками критеріїв. Для цього може бути використаний оператор зважена сума, в якому компроміс задається за допомогою набору ваг:

$$A_i = \sum_{j=1}^{n} a_{ij} w_j, \quad (1)$$

де A_i – загальна оцінка *i*-ої альтернативи; a_{ij} – оцінка *i*-ої альтернативи за *j*-им критерієм; w_j – вага критерію *j*; *n* – кількість критеріїв [2].

Але найбільшими можливостями володіє оператор впорядкованого зваженого усереднення OWA, який побудований за логікою Ягера [3]. Він може бути використаний в ГІС і забезпечує безперервні операції агрегування між оператором *MIN* і *MAX* за рахунок наявності двох наборів ваг – ваг критеріїв $\sum_{j=1}^{n} w_j = 1$ та ваг порядку $\sum_{j=1}^{n} \lambda_j = 1$. Останні керують положенням оператора агрегування в континуумі між крайніми випадками *MIN* і *MAX*, таким чином забезпечуючи певну ступінь компромісу.

Формалізований запис OWA оператора Ягера має наступний вигляд [4]:

$$A_i = \sum_{j=1}^{n} \left(\frac{\lambda_j w_j^b}{\sum_{j=1}^{n} \lambda_j w_j^b} \right) b_{ij},$$

де A_i – загальна оцінка *i*-ої альтернативи; $b_{i1} \geq b_{i2} \geq \ldots \geq b_{in}$ – елементи вектора $A=(a_1,a_2,\ldots,a_n)$ впорядковані за зменшенням; w^b_j – ваги критеріїв, впорядковані у відповідності зі значенням атрибуту b_{ij}.

Оператор OWA має здатність реалізовувати широкий спектр комбінування шарів критеріїв: від *MIN* (у випадку, коли $\lambda_1=\lambda_2=\ldots=\lambda_{n-1}=0$, $\lambda_n=1$), до *MAX* (у випадку, коли $\lambda_1=1$, $\lambda_2=\ldots=\lambda_n=0$). При $\lambda_1=\lambda_2=\ldots=\lambda_n=1/n$ оператор OWA ідентичний оператору (1).

Висновки. Для врахування ставлення ОПР до ризику найбільш обґрунтованим є використання оператора впорядкованого зваженого усереднення OWA, який може бути реалізований в ГІС і забезпечує безперервні операції агрегування між крайніми випадками ставлення до ризику, тобто від готовності до ризику до повної відмови від нього. Оператори *MIN*, *MAX* та зважена сума є окремими випадками оператора OWA.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Кузніченко С.Д., Гунченко Ю.О., Бучинська І.В. (2018) Нечітка модель обробки геопросторових даних в мультикритеріальному аналізі придатності територій. Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. К.: ВІКНУ, 61:90–103

2. Кузніченко С.Д., Бучинська І.В. (2019) Вибір операторів агрегування для багатокритеріальної оцінки придатності територій. Кібербезпека: освіта, наука, техніка, 2019. – Том 2 № 6. – С.46–56.
3. Yager R (1988) "On ordered weighted averaging aggregation operators in multicriteria decision making", IEEE Transactions on System, Man, and Cybernetics 18:183–190.
4. Кузніченко С.Д., Бучинська І.В., Коваленко Л.Б. (2019) Використання OWA-оператора Ягера з нечіткими квантифікаторами в ГІС-орієнтованих багатокритеріальних моделях прийняття рішень. Матеріали 8-ї Міжнародної науково-технічної конференції "Інформаційні системи та технології", КоблевеХарків, 9–14 вересня 2019 р. с 113–116.

КЛАСИФІКАЦІЯ ЗАГРОЗ ВЕБ-ЗАСТОСУНКІВ

ЛАВРЄНОВ В.А., ст. 551 гр.
СІРЕНКО О.І., науковий керівник, ст. викл. кафедра КІ
Одеська національна академія харчових технологій

Безпека веб-застосунків, є одним з найбільш важливих питань інформаційної безпеки. Велика частина веб-сайтів і веб-застосунків в Інтернеті, мають різного роду уразливості, а також схильні до постійних атак.

Мета даної роботи, розібрати основні вразливості веб-застосунків і класифікувати їх за певними ознаками. Розглянемо основні загрози веб-застосунків. Загрози інформаційної безпеки веб-додатки поділяються на три основні типи:

1. Загрози конфіденційності (несанкціонований доступ до даних).
2. Загрози цілісності (несанкціоноване спотворення або знищення даних).
3. Загрози доступності (обмеження або блокування доступу до даних).

Головним джерелом усіх загроз інформаційній безпеці веб-застосунків, є зовнішні порушники – люди, які мають несанкціонований доступ до веб-застосунку. Зовнішній порушник, може виявляти максимально можливу кількість векторів атаки для складання та реалізації потенційно успішних сценаріїв злому, або ж масово атакувати, зазвичай використовує кілька поверхневих вразливостей.

Загрози безпеці, найчастіше пов'язані з наступними п'ятьма параметрами:

1. Вразливості веб-застосунків або їх компонентів.
2. Використання механізмів перевірки ідентифікації.
3. Клієнт-сайд атаки, атаки на користувачів.
4. Витік або розголошення критичної інформації.
5. Логічні атаки.

Вразливості веб-застосунків, працюють за рахунок виконання коду на віддаленому сервері. На сервер надходять дані у вигляді оброблених користувачем запитів, подібні дані використовуються при складанні команд, що застосовуються для генерації динамічного контенту. При відсутності певних вимог безпеки при розробці веб-застосунків, зовнішній порушник може отримати доступ до модифікації виконуваних команд, прикладом можна вважати SQL-ін'єкції.

Атаки, спрямовані на використовувані веб-застосунком методи перевірки ідентифікатора користувача, або спрямовані на методи, які використовуються веб-сервером для визначення вчинення дій дозволу користувача. Один з найбільш частих і простих видів атак, прикладами можуть бути методи перебору паролів або обходи авторизації.

Клієнт-сайд, передбачає, що при відвідуванні веб-ресурсу, між користувачем і сервером встановлюються довірчі відносини, тим самим не чекаючи атак з боку сайту. Цим користується зовнішній порушник, використовуючи властиві для цього методи проведення атак на клієнтів, наприклад, такі як міжсайтовий скриптинг.

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.