v – інтенсивність (швидкість) споживання запасу;

s – витрати на зберігання запасу;

K – витрати на здійснення замовлення, що включають оформлення й доставку замовлення.

Для знаходження загальних витрат використовують таку формулу (2):

$$L = K\frac{v}{Q} + s\frac{Q}{2}, \quad (2)$$

де L – загальні витрати на керування запасами в одиницю часу;

Q – розмір замовлення.

Період доставки визначають за наступною формулою (3):

$$\tau = \frac{Q}{v}, \quad (3)$$

де τ – період доставки.

Точку замовлення визначають за формулою (4):

$$h_0 = vt_д. \quad (4)$$

Використання запропонованої моделі управління запасами підприємства в автоматизованих системах управління торгівлею дасть можливість визначати точку замовлення продукції, що є актуальним при великій кількості асортименту продукції, та значно підвищить ефективність використання автоматизованих систем в роздрібній торгівлі.

Список використаних джерел:

1. Реферат «Організація процесу продажу товарів у сфері роздрібної торгівлі та її стимулювання» [Электронный ресурс]. – Режим доступа: http://ukrbukva.net/57065-Organizaciya-processa-prodazhi-tovarov-v-sfere-roznichnoiy-torgovli-i-ee-stimulirovanie.html

2. Автоматизовані системи управління обробки інформації в торгівлі [Электронный ресурс]. – Режим доступа: http://ua-referat.com/Автоматизовані_системи_управління_обробки_інформації_в_торгівлі

3. Автоматизовані системи управління торгівельними підприємствами [Электронный ресурс]. – Режим доступа: http://nauka.kushnir.mk.ua/?p=10048

4. Автоматизація управління запасами торгівельного підприємства [Электронный ресурс]. – Режим доступа: http://works.doklad.ru/view/9ZoptbGRMwI.html

5. Моделі Уілсона управління запасами [Электронный ресурс]. – Режим доступа: http://knowledge.allbest.ru/emodel/3c0b65625a3ad68a5d53b88521206d26_0.html

Щербань В.С.

студент,

Навчально-науковий інститут інформаційної безпеки

Національної академії Служби безпеки України

МОДЕЛЬ ЗАГРОЗ ВЕБ БЕЗПЕКИ: ПІДХІД ДО ВИЗНАЧЕННЯ

Об’єктивний результат моделювання загроз веб безпеки дозволяє оцінити адекватність методів, засобів та заходів захисту веб додатків, оцінити можливі

втрати та імовірність їх реалізації тощо. Оскільки модель загроз та модель порушника є основою для побудови ризикової моделі процесів забезпечення веб безпеки, яка дозволяє також оцінити рівень та економічну ефективність захисту конкретних веб-додатків з урахуванням їх особливостей (призначення, наповнення, затребуваність, технічна реалізація).

Зазначена тематика розглядалася у роботах [1; 2; 4; 6], але є актуальною у сенсі створення та удосконалення ефективних методик оцінювання рівня захищеності сучасних веб розробок.

Загалом, під загрозою веб безпеці можна розуміти сукупність факторів та умов, що можуть призвести до негативних наслідків (збитків) у разі несанкціонованого порушення штатних умов експлуатації веб-додатків.

До найбільш важливих властивостей загроз відносять вибірковість, прогнозованість та шкідливість. Вибірковість характеризує націленість загрози на завдання шкоди конкретним властивостям безпеки веб-додатків. Прогнозованість – наявність ознак виникнення загрози та властивості безпеки веб-додатків, на які вона буде направлена. Натомість, шкідливість характеризує можливість нанесення шкоди з різним рівнем тяжкості.

Загроза завжди породжує небезпеку, яка є імовірнісно-часовою характеристикою загрози відповідно.

Розглянемо декілька ознак класифікації загроз веб безпеці:

– місцезнаходження джерела – внутрішні та зовнішні;

– небезпека – потенційні та реальні з відповідною шкалою градації;

– направленість – порушення доступності, цілісності, автентичності та конфіденційності інформації;

– природа виникнення – вразливості веб-додатків та їх компонентів, недоліки методів, засобів та заходів захисту (на етапах веб розробки, налаштування та управління веб безпекою).

Детальний опис вразливостей для веб-додатків (вразливостей для реалізації загроз – атак на веб-додатки) запропоновано міжнародним консорціумом Web Application Security Consortium [3]: інєкції; порушення автентифікації та управління сеансами; міжсайтовий скриптинг; незахищені прямі посилання на об’єкт; недосконале налаштування функцій безпеки; чутлива експозиція даних; відсутність функції контролю доступу; міжсайтова підробка запиту; використання компонентів з відомими вразливостями; неперевірений перехід та редирект.

З характеристиками інцидентів веб безпеки, методів і засобів пошуку загроз веб-додаткам можна ознайомитись, наприклад, в [5; 7].

У свою чергу, модель загроз веб безпеки – це формальний опис загроз та їх можливих технічних реалізацій (атак) на протязі життєвого циклу веб-додатків, актуальності, імовірності реалізації та можливих наслідків. Модель загроз веб-безпеки уточняється у відповідності з моделлю порушника веб-безпеки, особливо щодо визначення актуальності загроз.

При визначенні підходів до створення моделі загроз веб-безпеки актуалізується завдання з розробки методик оцінювання актуальності та імовірності загроз (атак), оцінювання їх наслідків зокрема. Саме тому

представляє інтерес ризикова модель загроз веб безпеки, оскільки одним із розумінь ризику є поєднання ймовірності та наслідків настання несприятливих подій.

Список використаних джерел:

1. Модель загроз у розподілених мережах [Електронний ресурс]. – Режим доступу: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/7538/09-Matov.pdf?sequence=1
2. НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу.
3. Офіційний сайт Web Application Security Consortium. [Електронний ресурс]. – Режим доступу: http://www.webappsec.org/
4. Створення моделі загроз інформації та механізму її ефективного захисту [Електроний ресурс] – Режим доступу: http://ena.lp.edu.ua:8080/bitstream/ntb/11750/1/11_stvorennya%20modeli.pdf
5. Анализ угроз информационной безопасности [Електронний ресурс]. – Режим доступу: https://www.anti-malware.ru/analytics/Threats_Analysis
6. Методология построения модели угроз безопасности территориально распределённых объектов Интернет-журнал «Технологии техносферной безопасности» (http://ipb.mos.ru/ttb) Выпуск No 2 (48), 2013 г
7 WEB applications security statistics report [Електронний ресурс]. – Режим доступу:https://info.whitehatsec.com/rs/675-YBI-674/images/WH-2016-Stats-Report

Якименко І.З.
кандидат технічних наук, доцент;
Мачуляк М.В.
студент,
Тернопільський національний економічний університет

МЕТОД ГЕНЕРУВАННЯ ПРОСТИХ ЧИСЕЛ НА ОСНОВІ ВИКОРИСТАННЯ СИСТЕМИ ЗАЛИШКОВИХ ФУНКЦІЙ

Сучасні комп’ютерні мережі та системи інтенсивно вдосконалюються на основі нових теоретичних положень опрацювання інформаційних потоків та програмно-апаратних засобів реалізації алгоритмів формування, перетворення, ідентифікація та покращення аутентифікації користувачів інформаційних систем [1]. При цьому, на сучасному етапі розвитку комп’ютерних систем виникає ряд проблем та науково-технічних задач пов’язаних з підвищенням інформаційної стійкості комп’ютерних систем, підвищення швидкодії алгоритмів шифрування/дешифрування а також створення відповідних програмно-апаратних та спецпроцесорних засобів опрацювання інформаційних потоків.

Досвід використання відомих алгоритмів шифрування та розвиток теорії алгоритмів , які широко застосовуються в практиці на основі важко оборотних функцій хешування, факторизації, модулярних та інших операцій вже