для скорочення невизначеності або використання альтернативних джерел постачання.

Список використаних джерел

1. Гукалюк А. Ф. Логістичне управління запасами як складова логістичного управління підприємством. *Економічний аналіз.* 2017. Том 27. № 2. С. 130–138.

2. Круш П. В., Орлюк Ю.В. Теоретичні основи управління матеріальними запасами підприємств. *Економічний вісник НТУУ «Київський політехнічний інститут»*. 2017. № 14. DOI: https://doi.org/10.20535/2307-5651.14.2017.108775

3. Логістичне управління запасами на підприємствах: монографія. В. І. Перебийніс, Я. А. Дроботя. Полтава: ПУЕТ, 2012. 279 с.

4. Голіков К. Ю., Шульгіна Л.М. Вдосконалення оцінки ефективності системи управління запасами на підприємстві. *Young*. 2016. Т. 29. №. 2. С. 29–31.

УДК: 331.56

САЧІВКА О.С., СНІЖКО І.В., студенти 1 курсу
Науковий керівник – **БОНДАР О.С.,** канд. екон. наук

БЕЗПЕКА БРАУЗЕРА ЯК ВАЖЛИВИЙ АСПЕКТ ОНЛАЙН-БЕЗПЕКИ

У роботі описано шляхи забезпечення кібербезпеки під час роботи онлайн, вказано, які існують загрози при здійсненні різних операцій в Інтернеті, як вони поширюються і впливають на безпеку інформації. Надано поради для безпечного користування інтернетом.

Ключові слова: безпека, онлайн-безпека, браузер, кібератака.

Безпека браузера є критично важливим аспектом в сучасному світі, де інтернет став необхідним інструментом для спілкування, роботи та розваг. Браузери є програмними засобами, які відображають веб-сторінки та дозволяють користувачам здійснювати різні операції в Інтернеті, такі як пошук інформації, покупки онлайн, спілкування тощо. Однак, як і в будь-якій іншій сфері, збільшення використання браузерів також призвело до збільшення ризиків щодо безпеки. Основні загрози безпеці браузерів полягають у наступному: Фішинг: це атака, при якій зловмисник відправляє електронний лист, що містить посилання на фальшиву веб-сторінку, яка схожа на легітимну веб-сторінку. Користувач, який натискає на посилання та вводить свої дані, може потрапити в руки зловмисників, які використовують ці дані для крадіжки ідентифікаційної інформації. Віруси та інші шкідливі програми можуть бути розповсюджені через веб-сторінки або поштові скриньки. Вони можуть використовувати різні методи, щоб завдати шкоди користувачеві, такі як викрадення інформації, встановлення додаткових програм або знищення файлів.

Крадіжка даних: зловмисники можуть використовувати різні методи, щоб отримати доступ до інформації, що зберігається на комп'ютері користувача. Це може включати викрадення паролів, банківських реквізитів або конфіденційної інформації.

Рекламні програми: деякі рекламні програми можуть включати шкідливі скрипти, які можуть негативно впливати на безпеку браузера та комп'ютера користувача.

Несанкціонований доступ до даних: деякі браузери можуть зберігати деяку інформацію про користувача, таку як історія перегляду веб-сторінок або кукі-файли, які містять інформацію про користувача. Якщо ця інформація потрапить в руки зловмисників, то це може викликати проблеми з безпекою.

Для забезпечення безпеки браузера та захисту від загроз, користувачі можуть вжити наступні заходи:

Оновлювати браузер та програмне забезпечення: більшість виробників браузерів та програмного забезпечення випускають оновлення, які містять патчі безпеки та виправляють відомі уразливості. Користувачі повинні встановлювати ці оновлення якнайшвидше.

Використовувати програми антивірусного захисту: програми антивірусного захисту можуть розпізнавати та блокувати шкідливі програми, віруси та інші загрози.

Не відкривати невідомі посилання та не завантажувати підозрілі файли: користувачі повинні бути обережні, коли отримують електронні листи або переходять на невідомі веб-сторінки. Перед завантаженням файлів, користувачі повинні переконатись, що вони безпечні та надійні.

Використовувати складні паролі та двофакторну автентифікацію: користувачі повинні використовувати складні паролі, які містять букви, цифри та символи. Також вони можуть використовувати двофакторну автентифікацію, яка забезпечує додатковий рівень захисту.

Вимикати автозаповнення та зберігання паролів: автозаповнення та зберігання паролів можуть бути небезпечними, оскільки зловмисники можуть отримати доступ до цієї інформації. Користувачі можуть вимкнути ці функції та вручну вводити свої дані в поля.

Використовувати розширення та додатки для захисту: деякі браузери мають розширення та додатки, які можуть забезпечити додатковий рівень захисту. Наприклад, деякі розширення можуть блокувати рекламу та шпигунські програми, запобігати перенаправленню на шкідливі веб-сторінки, а також дозволяти користувачам контролювати те, яку інформацію надсилають їхні браузери.

Використовувати захищене підключення: коли користувачі входять на веб-сторінки, які вимагають введення особистої інформації, вони повинні переконатись, що вони використовують захищене підключення з шифруванням даних. На сторінках з захищеним підключенням зазвичай є замок у рядку адреси.

Використовувати приватні вікна браузера: більшість браузерів мають функцію приватного перегляду, яка дозволяє користувачам переглядати веб-сторінки без збереження історії браузера та даних форм.

Заблокувати використання плагінів: деякі плагіни можуть бути небезпечними та створювати уразливості в браузері. Користувачі можуть забло-кувати використання плагінів або використовувати лише ті, які є надійними та актуальними.

Бути обережними під час використання громадських мереж Wi-Fi: використання ненадійних мереж Wi-Fi може призвести до зламу браузера та злочинних дій. Користувачі повинні бути обережні під час використання

громадських мереж та не використовувати їх для введення особистої інформації та проведення фінансових транзакцій.

Крім того, спам-фільтри в браузері є важливим інструментом для боротьби з небажаними повідомленнями та шкідливими вмістом, які можуть завдати шкоди комп'ютеру та особистим даним користувача. Вони можуть працювати на основі різних методів. Один з найбільш поширених методів - це фільтрація на основі ключових слів. Фільтр може перевіряти текст повідомлення та порівнювати його з базою даних заборонених слів, фраз та ключових фраз. Якщо повідомлення містить заборонені слова або фрази, воно може бути автоматично відфільтроване.

Іншим методом є аналіз поведінки користувача та виявлення незвичайних дій, які можуть вказувати на спам. Наприклад, якщо користувач отримує велику кількість повідомлень з одного і того ж джерела, або якщо повідомлення містять незвичайні звернення, то це може вказувати на спам.

Деякі спам-фільтри в браузерах можуть також використовувати технології штучного інтелекту та машинного навчання, щоб автоматично визначати спам та інші небажані повідомлення.

Ці заходи допоможуть зменшити ризик атак на браузер та за безпечити особисті дані користувачів. Однак важливо пам'ятати, що навіть при використанні всіх цих заходів, існує певний ризик атак і крадіжки даних. Тому користувачі повинні завжди бути обережними та дотримуватись основних правил безпеки, таких як не введення особистих даних на ненадійних веб-сторінках та завантаження тільки програм і файлів з надійних джерел.

Список використаних джерел

1.Офіційний сайт ЦК Профспілки працівників освіти і науки України https://pon.org.ua/novyny/5427-bezpeka-v-nternet-scho-potrbno-znati.html

2. Інститут інноваційних технологій і змісту освіти Міністерства освіти і науки, молоді та спорту Компанія «Майкрософт Україна» https://elibrary.kubg.edu.ua/id/eprint/1547/1/Internet.pdf

3.Що таке кібератака? https://www.microsoft.com/uk-ua/security/business/security-101/what-is-a-cyberattack

УДК: 658.51/.58

СІВОЗДРАВ Б.І., магістрант
Науковий керівник – **КЕПКО В.М.**, канд. екон. наук
Білоцерківський національний аграрний університет

УДОСКОНАЛЕННЯ УПРАВЛІННЯ ВИРОБНИЧО-ГОСПОДАРСЬКОЮ ДІЯЛЬНІСТЮ НА ПІДПРИЄМСТВІ

Проаналізовано ефективність виробничо-господарської діяльності та процес управління ефективністю ФГ «Добробут-10». Запропоновані заходи, які будуть сприяти підвищенню ефективності управління виробничо-господарською діяльністю у господарстві.

Ключові слова: виробничо-господарська діяльність; організаційна структура; підвищення ефективності; удосконалення управління.

Сутність управління виробничо-господарської діяльності полягає в забезпеченні цілеспрямованого, планомірного впливу суб'єкта управління на об'єкт