ж таки користувач може взаємодіяти із вмістом. Релаксуюча музика на фоні, супроводжує процес взаємодії із анімацією та створює медитаційних ефект. При кліку на кнопку вниз – відкривається сторінка з плеєром та загальною інформацією про анімацію. У плеєрі є заздалегідь підібрана музика, що найкраще відображає зміст задумки, юзер може змінювати пісні та таймінг відтворення музики. Нотатки поруч, мають зміст навчального характеру, що показує деякі математичні моделі використані для створення анімацій. Таким чином, користувач отримує базове розуміння моделювання анімацій з використанням математичних бібліотек 3D моделювання.

Підсумовуючи, програма поєднує у собі дві основні цілі, навчальну та пропонує користувачам платформу для покращення свого психічного благополуччя за допомогою керованих вправ і візуальної релаксації. Зручний інтерфейс, настроювані функції та зосередженість на уважності роблять її корисною для тих, хто хоче відпочити та отримати додаткові математичні знання.

Список літератури.

1. Ronald L. Graham Mathematics and Computer Science. Notices of the American Mathematical Society. 1994.

2. Kristin L. Wood. Visualizing Multidimensional Data with 3D Animations. Journal of Computational and Graphical Statistics.

УДК 004.056: [004.6:005] (043.2)

Діденко М.М., студентка 4 курсу спеціальності 125 «Кібербезпека»
Потапова Н. А., к.е.н., доцент, доцент кафедри інформаційних технологій

КІБЕРБЕЗПЕКА В ЛОГІСТИЦІ: ЗАХИСТ ДАНИХ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

Донецький національний університет імені Василя Стуса, м. Вінниця

У сучасному світі логістика грає важливу роль у бізнесі та економіці. Вона включає у себе управління ланцюгами поставок, складську логістику, транспорт та дистрибуцію товарів. Однак, як і багато інших галузей, логістика також стикається з ризиками кібербезпеки. У логістиці обробляється безліч даних, які можуть бути важливими для компаній та їх клієнтів. Ці дані можуть включати інформацію про постачальників, замовлення, склади, транспорт та багато іншого. Хакерські вторгнення або витік даних може призвести до серйозних наслідків для бізнесу та його клієнтів.

Для захисту даних та інформаційних систем у логістиці необхідно приймати заходи з кібербезпеки. Одним з таких заходів є використання

шифрування даних. Шифрування дозволяє захистити дані від несанкціонованого доступу та хакерських вторгнень. Програма чи служба, у якій використовується шифрування, прийматиме повідомлення чи файли та перетворюватиме їх у код, який не дасть змогу прочитати дійсний вміст. Це означає, що навіть якщо в обмін даними втрутиться зловмисник, він нічого не побачить. Шифрування – важливий метод захисту, на який слід звернути увагу під час надсилання файлів за допомогою будь-якої служби [1].

Забезпечення безпеки інформаційних систем може включати в себе: встановлення антивірусних програм та брандмауерів, регулярне оновлення програмного забезпечення та моніторинг системи на наявність загроз. Брандмауер – це програма або пристрій, який перевіряє дані, що надходять з Інтернету або мережі, та на основі поточних параметрів приймає рішення, потрібно їх пропускати чи ні. Таким чином брандмауер блокує доступ до вашого комп'ютера для хакерів і зловмисних програм. Антивірусні програми перевіряють електронну пошту та інші файли комп'ютера на наявність вірусів, хробаків і троянських програм. Якщо такі будуть знайдені, антивірусна програма переміщує їх у карантин (ізолює) або повністю видаляє до того, як буде заподіяно шкоду комп'ютеру та файлам [2].

Одним з найбільш серйозних ризиків є кібератака на системи управління ланцюгами поставок. Кібератака може призвести до перерви в роботі системи та проблем з логістикою. Для захисту від кібератак необхідно приймати заходи з безпеки мережі, а також навчати співробітників компанії основам кібербезпеки та і вчасно оновлювати їх. Також компанія має розробити політику безпеку компанії, в якій буде наведено список правил, яких має працівник дотримуватись. Політика безпеки – попередити велику кількість фішингових листів троянських програм і т.п.

Іншим ризиком є соціальний інжиніринг, коли зловмисники використовують людську довіру та недбалість для отримання доступу до системи. Наприклад, можливість отримати доступ до логістичної системи за допомогою краденого пароля від електронної пошти співробітника. В даному випадку також необхідний перелік правил, який може попередити це. Але людський фактор – це найбільша загроза в компанії.

Також важливим є відстеження та аналіз поведінки користувачів системи, щоб вчасно виявляти та запобігати можливим атакам. Компанії повинні регулярно проводити тестування на проникнення та аудит безпеки, щоб виявити можливі слабкі місця в системі та вчасно їх усунути.

Окрім того, у логістичних компаніях велику роль грає безпека транспорту та складів. Наприклад, викрадення товарів з вантажівок або зі складів є серйозною проблемою для логістики. Тут також важливо використовувати заходи з безпеки, такі як контроль доступу, відеоспостереження та захист від крадіжок.

Отже, кібербезпека має велике значення для логістики. Компанії повинні приділяти достатню увагу захисту своїх даних та інформаційних систем. Це може допомогти уникнути серйозних наслідків для бізнесу та його клієнтів.

Список літератури:

1. *Що таке кібербезпека? URL: https://experience.dropbox.com/uk-ua/resources/cyber-security (Дата звернення 27.03.2023)*
2. *Програмні засоби захисту від комп'ютерних вірусів. URL: https://sites.google.com/site/programizahistukomputera/ (Дата звернення 27.03.2023)*
3. *Тимчук О.Г., Потапова Н.А. Принципи забезпечення інформаційної безпеки. Прикладні аспекти сучасних міждисциплінарних досліджень: матеріали І Міжнародної науково-практичної конференції (м. Вінниця, 18 листопада 2022 р.). Вінниця: ДонНУ імені Василя Стуса. 2022. С. 214-215.*

УДК 004.9

Дуріцин В.С., студент 4 курсу
спеціальності 122 «Комп'ютерні науки»
Потапова Н. А., к.е.н., доцент, доцент
кафедри інформаційних технологій

МОБІЛЬНИЙ ЗАСТОСУНОК МОНІТОРИНГУ ВІДКЛЮЧЕНЬ ЕЛЕКТРОМЕРЕЖІ

Донецький національний університет імені Василя Стуса, м. Вінниця

У сучасному світі мобільні пристрої виконують важливу роль комунікації та пошуку інформації, надаючи тим самим доступ до безлічі функцій і можливостей. Однією з таких важливих функцій є сповіщення про аварійні відключення світла у будинках. Функцію моніторингу та ситуаційного оперативного контролю на будь-які аварійні відключення електроенергії мають виконувати спеціально розроблені мобільні застосунки. Застосунки надсилають повідомлення на мобільний пристрій (телефон або планшет), інформуючи про факт відключення світла у будинку. Це надзвичайно важливо, оскільки аварійні відключення світла можуть статися в будь-який час, і ми повинні бути готові до таких ситуацій. Завдяки мобільному застосунку, отримується миттєве повідомлення, внаслідок чого стає можливим прийняти необхідні заходи щодо забезпечення електроенергією, наприклад, переключитися на резервне джерело живлення, або повідомити про проблему відповідним службам.

Основними функціями мобільного застосунку моніторингу відключень електромережі є:

1. Моніторинг відключень електромережі, що сприяє покращенню ефективності управління електропостачанням. Цей застосунок надає оперативне сповіщення про відключення електроенергії, дозволяючи операторам швидко реагувати на проблеми та забезпечувати швидке відновлення постачання. Він також допомагає відстежувати стан електромережі в режимі реального часу, що сприяє швидкому виявленню потенційних проблем та уникненню подальших відключень.

2. Інформаційна підтримка планування дій користувача по забезпеченню електроенергією помешкання. Він забезпечує можливість отримати інформацію